ISO/IEC 29341-18-13

Edition 1.0 2011-08

INTERNATIONAL STANDARD

colour inside

Information technology – UPnP device architecture – Part 18-13: Remote Access Device Control Protocol – Remote Access Transport Agent Configuration Service

ISO/IEC 29341-18-13:2011(E)

Documents
Document Sharing Hub

Full document details: ISO IEC 29341-18-13-2011

THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2011 ISO/IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about ISO/IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: 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 corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

Documents
Document Sharing Hub

Full document details: ISO IEC 29341-18-13-2011

ISO/IEC 29341-18-13

Edition 1.0 2011-08

INTERNATIONAL STANDARD

colour inside

Information technology – UPnP device architecture – Part 18-13: Remote Access Device Control Protocol – Remote Access Transport Agent Configuration Service

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE S

ICS 35.200

ISBN 978-2-88912-641-5

Documents
Document Sharing Hub

Full document details: ISO IEC 29341-18-13-2011

CONTENTS

1 Overview and Scope 4
1.1 Introduction 4
1.2 Notation 4
1.3 Vendor-defined Extensions 5
1.4 References 5
1.4.1 Normative References 5
1.4.2 Informative References 6
2 Service Modeling Definitions 6
2.1 Service Type 6
2.2 Terms and Abbreviations 7
2.2.1 Abbreviations 7
2.2.2 Terms 7
2.3 *RATAConfig* Service Architecture 8
2.4 State Variables 8
2.4.1 State Variable Overview 8
2.4.2 *SystemInfo* 8
2.4.3 *TransportAgentCapabilities* 9
2.4.4 *CredentialDelivery* 9
2.4.5 *CredentialsList* 9
2.4.6 *ProfileList* 9
2.4.7 *A_ARG_TYPE_ProfileConfigInfo* 10
2.4.8 *A_ARG_TYPE_ProfileID* 10
2.5 Eventing and Moderation 10
2.5.1 Relationships Between State Variables 10
2.6 Actions 10
2.6.1 *GetTransportAgentCapabilities()* 11
2.6.2 *GetSupportedCredentialDelivery()* 11
2.6.3 *GetCredentialsList()* 12
2.6.4 *GetProfileList()* 13
2.6.5 *AddProfile()* 13
2.6.6 *EditProfile()* 14
2.6.7 *DeleteProfile()* 15
2.6.8 *GetProfileConfigInfo()* 16
2.6.9 Error Code Summary 16
2.7 Theory of Operation 17
2.7.1 The Interaction Model 17
2.7.2 Detecting the RATA Role 17
2.7.3 Configuring Remote Access Transport Profile (Server) 17
2.7.4 Configuring Remote Access Transport Profile (Client) 18
2.7.5 Editing a Profile 18
2.7.6 Deleting a Profile 19
3 XML Service Description 19
4 Test 22
Annex A (normative) RATransportAgent Data Structures 23

AVA Documents
Document Sharing Hub

Full document details: ISO IEC 29341-18-13-2011

A.1 ProfileList Template 23
A.2 ProfileConfig Template 23
A.3 TransportAgentCapabilities Template 24
A.4 CredentialDelivery Template 25
A.5 CredentialsList Template 26
A.6 TransportAgent Datastructure Schema 27
Annex B (informative) Addressing Considerations 28
B.1 IPv4 Considerations 28
B.1.1 IPv4 Address Allocation 28
B.1.2 Address Space Collisions 28
Annex C (normative) Using IPsec as Remote Access Transport 30
C.1 IPsec Templates 30
C.1.1 IPsec Options Template 30
C.1.2 IPsec Configuration Template 31
C.2 Sample IPsec Files 34
C.2.1 Sample IPSec based on certificates 34
C.2.2 Sample IPSec based on shared key null policy 37
C.2.3 Sample IPSec based on shared key advanced policy 39
Annex D (normative) Using OpenVPN as Remote Access Transport 42
D.1 OpenVPN Templates 42
D.1.1 OpenVPN Configuration Template 42
D.2 Sample OpenVPN configuration 46
D.2.1 Sample configuration for Server 46
D.2.2 Sample configuration for Client 46

Figure 2-1 — The Interaction Model. 17
Figure 2-2 — Configuring Remote Access Transport Profiles. 18
Figure 2-3 — Editing Remote Access Transport Profiles. 18
Figure 2-4 — Deleting Remote Access Transport Profiles. 19
Figure B.1 — Address Space Collision Problem. 28

Table 2-1 — Abbreviations 7
Table 2-2 — State Variables 8
Table 2-3 — Eventing and Moderation 10
Table 2-4 — Actions 10
Table 2-5 — Arguments for *GetTransportAgentCapabilities()* 11
Table 2-6 — Error Codes for *GetTransportAgentCapabilities()* 11
Table 2-7 — Arguments for *GetSupportedCredentialDelivery()* 11
Table 2-8 — Error Codes for *GetSupportedCredentialDelivery()* 12
Table 2-9 — Arguments for *GetCredentialsList()* 12
Table 2-10 — Error Codes for *GetCredentialsList()* 13
Table 2-11 — Arguments for *GetProfileList()* 13
Table 2-12 — Error Codes for *GetProfileList()* 13
Table 2-13 — Arguments for *AddProfile()* 13
Table 2-14 — Error Codes for *AddProfile()* 14
Table 2-15 — Arguments for *EditProfile()* 14

AVA Documents
Document Sharing Hub

Full document details: ISO IEC 29341-18-13-2011

Table 2-16 — Error Codes for *EditProfile()* 15
Table 2-17 — Arguments for *DeleteProfile()* 15
Table 2-18 — Error Codes for *DeleteProfile()* 16
Table 2-19 — Arguments for *GetProfileConfigInfo()* 16
Table 2-20 — Error Codes for *GetProfileConfigInfo()* 16
Table 2-21 — Error Code Summary 17

Documents
Document Sharing Hub

Full document details: ISO IEC 29341-18-13-2011

INFORMATION TECHNOLOGY – UPNP DEVICE ARCHITECTURE –

Part 18-13: Remote Access Device Control Protocol – Remote Access Transport Agent Configuration Service

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 29341-18-13 was prepared by UPnP Forum Steering committee[1], was adopted, under the fast track procedure, 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 29341 series, under the general title *Information technology – UPnP device 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.

---

1 UPnP Forum Steering committee, UPnP Forum, 3855 SW 153rd Drive, Beaverton, Oregon 97006 USA. See also "Introduction".

AVA Documents
Document Sharing Hub

Full document details: ISO IEC 29341-18-13-2011

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 publication using a colour printer.

Documents
Document Sharing Hub

Full document details: ISO IEC 29341-18-13-2011

1 Overview and Scope

This service definition is compliant with the UPnP Device Architecture version 1.0. It defines a service type referred to herein as *RATAConfig* service.

1.1 Introduction

The *RATAConfig* service is a UPnP service that allows control points to provision and configure the parameters that are required for enabling a Remote Access Server to accept and a Remote Access Client to initiate remote access connections. This service provides control points with the following functionality:

- Determine the Remote Access Transport Agents that can be configured by the service.
- Determine the delivery mechanisms for credentials supported by the service.
- Configure Remote Access Transport Agent profiles
- Management of Remote Access Transport Agent profiles

This service does not address:

- The trust model that will enable secure remote access connections.
- The delivery of credentials.

1.2 Notation

- In this document, features are described as Required, Recommended, or Optional as follows:

  The key words “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” in this specification are to be interpreted as described in [RFC 2119].

  In addition, the following keywords are used in this specification:

  PROHIBITED – The definition or behavior is an absolute prohibition of this specification. Opposite of REQUIRED.

  CONDITIONALLY REQUIRED – The definition or behavior depends on a condition. If the specified condition is met, then the definition or behavior is REQUIRED, otherwise it is PROHIBITED.

  CONDITIONALLY OPTIONAL – The definition or behavior depends on a condition. If the specified condition is met, then the definition or behavior is OPTIONAL, otherwise it is PROHIBITED.

  These keywords are thus capitalized when used to unambiguously specify requirements over protocol and application features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.
- Strings that are to be taken literally are enclosed in “double quotes”.
- Placeholder values that need to be replaced are enclosed in the curly brackets “{” and “}”.
- Words that are emphasized are printed in *italic*.
- Keywords that are defined by the UPnP Working Committee are printed using the *forum* character style.
- Keywords that are defined by the UPnP Device Architecture are printed using the **arch** character style.
- A double colon delimiter, “::”, signifies a hierarchical parent-child (parent::child) relationship between the two objects separated by the double colon. This delimiter is used in multiple contexts, for example: Service::Action(), Action()::Argument, parentProperty::childProperty.

Documents
Document Sharing Hub
Full document details: ISO IEC 29341-18-13-2011

1.3 Vendor-defined Extensions

Whenever vendors create additional vendor-defined state variables, actions or properties, their assigned names and XML representation MUST follow the naming conventions and XML rules as specified in [DEVICE], Clause 2.5, “Description: Non-standard vendor extensions”.

1.4 References

1.4.1 Normative References

This clause lists the normative references used in this specification and includes the tag inside square brackets that is used for each such reference:

[DEVICE] – UPnP Device Architecture, version 1.0. Available at: http://www.upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.0-20080424.pdf. Latest version available at: http://www.upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.0.pdf.

[DEVICE-IPv6] – UPnP Device Architecture, version 1.0., Annex A – IP Version 6 Support. Available at: http://www.upnp.org/resources/documents/AnnexA-IPv6_000.pdf

[RAClient] – RAClient:1, UPnP Forum, Available at: http://www.upnp.org/specs/ra/UPnP-ra-RAClient-v1-Device-20090930.pdf. Latest version available at: http://www.upnp.org/specs/ra/UPnP-ra-RAClient-v1-Device.pdf.

[RAServer] – RAServer:1, UPnP Forum, Available at: http://www.upnp.org/specs/ra/UPnP-ra-RAServer-v1-Device-20090930.pdf. Latest version available at: http://upnp.org/specs/ra/UPnP-ra-RAServer-v1-Device.pdf.

[RADASync] – RADASync:1, UPnP Forum, Available at: http://www.upnp.org/specs/ra/UPnP-ra-RADASync-v1-Service-20090930.pdf. Latest version available at: http://www.upnp.org/specs/ra/UPnP-ra-RADASync-v1-Service.pdf.

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

[DADS-XSD] – XML Schema for UPnP RA Discovery Agent XML Data Structures Available at: http://www.upnp.org/schemas/ra/dads-v1-20090930.xsd. Latest version available at: http://www.upnp.org/schemas/ra/dads-v1.xsd.

[TADS-XSD] – XML Schema for UPnP RA Transport Agent XML Data Structures Available at: http://www.upnp.org/schemas/ra/tads-v1-20090930.xsd. Latest version available at: http://www.upnp.org/schemas/ra/tads-v1.xsd.

[IPSEC-XSD] – XML Schema for IPSec Transport Agent Options and Configuration XML Data Structures Available at: http://www.upnp.org/schemas/ra/tacfg-ipsec-v1-20090930.xsd. Latest version available at: http://www.upnp.org/schemas/ra/tacfg-ipsec-v1.xsd.

[OPENVPN-XSD] – XML Schema for OpenVPN Transport Agent Options and Configuration XML Data Structures Available at: http://www.upnp.org/schemas/ra/tacfg-openvpn-v1-20090930.xsd. Latest version available at: http://www.upnp.org/schemas/ra/tacfg-openvpn-v1.xsd.

[XML] – “Extensible Markup Language (XML) 1.0 (Third Edition)”, François Yergeau, Tim Bray, Jean Paoli, C. M. Sperberg-McQueen, Eve Maler, eds., W3C Recommendation, February 4, 2004. Available at: http://www.w3.org/TR/2004/REC-xml-20040204/.

Documents
Document Sharing Hub

Full document details: ISO IEC 29341-18-13-2011

1.4.2 Informative References

This clause lists the informative references that are provided as information in helping understand this specification:

[IGD] – InternetGatewayDevice:1, UPnP Forum, November, 2001
Available at: http://www.upnp.org/standardizeddcps/documents/UPnP_IGD_1.0.zip

[RAARCH] – RAArchitecture:1, UPnP Forum, Available at: http://www.upnp.org/specs/ra/UPnP-ra-RAArchitecture-v1-20090930.pdf. Latest version available at: http://www.upnp.org/specs/ra/UPnP-ra-RAArchitecture-v1.pdf.

[RADAConfig] – RADAConfig:1, UPnP Forum, Available at: http://www.upnp.org/specs/ra/UPnP-ra-RADAConfig-v1-Service-20090930.pdf. Latest version available at: http://www.upnp.org/specs/ra/UPnP-ra-RADAConfig-v1-Service.pdf.

[RFC 2406] – IETF RFC 2406, IP Encapsulating Security Payload (ESP), S. Kent, R. Atkinson, November 1998
Available at: http://www.ietf.org/rfc/rfc2406.txt

[RFC 3706] – IETF RFC 3706, A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers, G. Huang, et. Al., February 2004
Available at: http://www.ietf.org/rfc/rfc3706.txt

[RFC 3947] – IETF RFC 3947, Negotiation of NAT-Traversal in the IKE, T. Kivinen, B. Swander, A. Huttunen, V. Volpe, January 2005.
Available at: http://www.ietf.org/rfc/rfc3947.txt.

[RFC 4306] – IETF RFC 4306, Internet Key Exchange (IKEv2) Protocol, C. Kaufman, Ed., December 2005
Available at: http://www.ietf.org/rfc/rfc4306.txt

2 Service Modeling Definitions

2.1 Service Type

The following service type identifies a service that is compliant with this specification:

urn:schemas-upnp-org:service:*RATAConfig:1* service is used herein to refer to this service type.

Documents
Document Sharing Hub

Full document details: ISO IEC 29341-18-13-2011

2.2 Terms and Abbreviations

2.2.1 Abbreviations

Table 2-1 — Abbreviations

Definition	Description
DPD	Dead Peer Detection
ESP	Encapsulating Security Payload
IKE	Internet Key Exchange
IPsec	IP security
RAC	Remote Access Client
RADA	Remote Access Discovery Agent
RAS	Remote Access Server
RAT	Remote Access Transport
RATA	Remote Access Transport Agent

2.2.2 Terms

2.2.2.1 Credentials

The term credentials refer to certificates, shared secrets or other means of authentication used in the RATA context.

2.2.2.2 Local Device

A local device is a UPnP device that is attached to the physical network where the RADA is located.

2.2.2.3 Management Console

The collection of Control Points used to configure and monitor Remote Access related services.

2.2.2.4 Remote Access Client

The Remote Access Client (RAC) is the peer physical device that is not part of the physical home network. The RAC is exposing only the UPnP devices and services that are embedded in the physical device.

2.2.2.5 Remote Access Network Interface

The RA network interface is the network interface that is created by the Remote Access Transport Agent. The settings for this interface are contained in a RAT profile.

2.2.2.6 Remote Access Server

The Remote Access Server (RAS) is the peer physical device located in the home network. RAS is exposing to the RAC the UPnP devices and services available in the physical home network as well as any embedded in the physical RAS device.

2.2.2.7 Remote Access Transport Agent Profile

A RATA profile is a configured RATA connection ready to be used by either accepting connections on the RAS side or to initiate connections on the RAC side.

Documents
Document Sharing Hub

Full document details: ISO IEC 29341-18-13-2011

2.2.2.8 Remote Device

A remote device is a UPnP device that is not attached to the physical network where the RADA is located.

2.3 *RATAConfig* Service Architecture

This service is responsible with providing a configuration interface for a secure communication channel that enables a remote UPnP device to interact with the UPnP devices located in the home network.

2.4 State Variables

Reader Note: For a first-time reader, it may be more helpful to read the action definitions before reading the state variable definitions.

2.4.1 State Variable Overview

Table 2-2 — State Variables

Variable Name	R/O [a]	Data Type	Allowed Values	Eng. Units
SystemInfo	*R*	**string**	See Clause 2.4.2	
TransportAgentCapabilities	*R*	**string**	See Clause 2.4.3	
CredentialDelivery	*R*	**string**	See Clause 2.4.4	
CredentialsList	*R*	**string**	See Clause 2.4.5	
ProfileList	*R*	**string**	See Clause 2.4.6	
A_ARG_TYPE_ProfileConfigInfo	*R*	**string**	See Clause 2.4.7	
A_ARG_TYPE_ProfileID	*R*	**ui4**	See Clause 2.4.8	
[a] *R* = Required, *O* = Optional, *X* = Non-standard				

2.4.2 *SystemInfo*

This state variable contains the snapshot of all networks the RATA has a relationship with, the status of the connection and the identity associated with the remote network.

The structure of the *SystemInfo* argument is a DADS XML Document:

- <systemInfo> is the root element.
- See the DADS schema [DADS-XSD] for more details on the structure. The available properties and their names are described in Annex A.1 of [RADASync].

Note that since the value of *SystemInfo* is XML, it needs to be escaped (using the normal XML rules: [XML] Clause 2.4 Character Data and Markup) before embedding in a SOAP response message.

Note: The *SystemInfo* maintained by the RATAConfig service is also shared by the RADASync and RADAConfig services. This state variable MUST be updated by the device and propagated internally to those other services when new remote networks become available or existing remote networks become unavailable, for triggering the RADA synchronization process. Furthermore, invocations of the *AddProfile()*, *DeleteProfile()* and *EditProfile()* actions also result in a modification of this state variable. Each modification in *SystemInfo* MUST be signalled by the device through the *SystemInfoUpdateID* evented state variable of the RADAConfig service (see Clause 2.4.3 of [RADAConfig]).

Documents
Document Sharing Hub
Full document details: ISO IEC 29341-18-13-2011

2.4.3 *TransportAgentCapabilities*

This state variable contains the list of remote access transport agent protocols and their capabilities supported by the RATAConfig.

The structure of the *TransportAgentCapabilities* argument is a TADS XML Document.

- <transportAgentCapability> is the root element.
- See the TADS schema [TADS-XSD] for more details on the structure. The available properties and their names are described in Clause A.3. Examples are provided in Clauses C.2.1.1, C.2.2.1 and C.2.3.1.

Note that since the value of *TransportAgentCapabilities* is XML, it needs to be escaped (using the normal XML rules: [XML] Clause 2.4 Character Data and Markup) before embedding in a SOAP response message.

2.4.4 *CredentialDelivery*

This state variable contains the list of credential delivery mechanisms supported by the RATAConfig.

The structure of the *CredentialDelivery* argument is a TADS XML Document.

- <credentialDelivery> is the root element.
- See the TADS schema [TADS-XSD] for more details on the structure. The available properties and their names are described in Clause A.4.

Note that since the value of *CredentialDelivery* is XML, it needs to be escaped (using the normal XML rules: [XML] Clause 2.4 Character Data and Markup) before embedding in a SOAP response message.

2.4.5 *CredentialsList*

This state variable contains the list of credentials that are present on the RATA.

The structure of the *CredentialsList* argument is a TADS XML Document:

- <credentialsList> is the root element.
- See the TADS schema [TADS-XSD] for more details on the structure. The available properties and their names are described in Clause A.5.

Note that since the value of *CredentialsList* is XML, it needs to be escaped (using the normal XML rules: [XML] Clause 2.4 Character Data and Markup) before embedding in a SOAP response message.

2.4.6 *ProfileList*

This state variable contains the list of configured profiles on the RATA.

The structure of the *ProfileList* argument is a TADS XML Document:

- <profileList> is the root element.
- See the TADS schema [TADS-XSD] for more details on the structure. The available properties and their names are described in Clause A.1.

Note that since the value of *ProfileList* is XML, it needs to be escaped (using the normal XML rules: [XML] Clause 2.4 Character Data and Markup) before embedding in a SOAP response message.

Documents
Document Sharing Hub

Full document details: ISO IEC 29341-18-13-2011

2.4.7 *A_ARG_TYPE_ProfileConfigInfo*

This state variable contains the profile configuration information for particular remote access transport protocol supported by RATA.

The structure of the A_ARG_TYPE_ProfileConfigInfo is a TADS XML Document:

- <profileConfig> is the root element.
- See the TADS schema [TADS-XSD] for more details on the structure. The available properties and their names are described in Clause A.2. Examples are provided in Clauses C.2.1.2, C.2.1.3, C.2.2.2, C.2.2.3, C.2.3.2, C.2.3.3, D.2.1 and D.2.2.

Note that since the value of *A_ARG_TYPE_ProfileConfigInfo* is XML, it needs to be escaped (using the normal XML rules: [XML] Clause 2.4 Character Data and Markup) before embedding in a SOAP response message.

2.4.8 *A_ARG_TYPE_ProfileID*

This state variable contains the unique id for a profile.

2.5 Eventing and Moderation

Table 2-3 — Eventing and Moderation

Variable Name	Evented	Moderated Event	Max Event Rate [a]	Logical Combination	Min Delta per Event [b]
SystemInfo	*NO*	*NO*			
TransportAgentCapabilities	*NO*	*NO*			
CredentialDelivery	*NO*	*NO*			
CredentialsList	*YES*	*NO*			
ProfileList	*NO*	*NO*			
A_ARG_TYPE_ProfileConfigInfo	*NO*	*NO*			
A_ARG_TYPE_ProfileID	*NO*	*NO*			

[a] Determined by N, where Rate = (Event)/(N secs).

[b] (N) * (allowedValueRange Step).

2.5.1 Relationships Between State Variables

None.

2.6 Actions

Table 2-4 — Actions

Name	R/O [a]
GetTransportAgentCapabilities()	*R*
GetSupportedCredentialDelivery()	*R*
GetCredentialsList()	*R*
GetProfileList()	*R*
AddProfile()	*R*
EditProfile()	*R*
DeleteProfile()	*R*
GetProfileConfigInfo()	*R*

AVA Documents
Document Sharing Hub
Full document details: ISO IEC 29341-18-13-2011

Name	R/O [a]
[a] R = REQUIRED, O = OPTIONAL, X = Non-standard	

2.6.1 GetTransportAgentCapabilities()

This action specifies a mechanism to determine the remote access transport agent protocols and their capabilities supported by the RATA.

2.6.1.1 Arguments

Table 2-5 — Arguments for GetTransportAgentCapabilities()

Argument	Direction	relatedStateVariable
TransportAgentCapabilities	OUT	TransportAgentCapabilities

2.6.1.1.1 TransportAgentCapabilities

This argument exposes the capabilities of the transport agent.

2.6.1.2 Dependency on State

None.

2.6.1.3 Effect on State

None.

2.6.1.4 Control Point Requirements

None.

2.6.1.5 Errors

Table 2-6 — Error Codes for GetTransportAgentCapabilities()

ErrorCode	errorDescription	Description
400-499	TBD	See UPnP Device Architecture clause on Control.
500-599	TBD	See UPnP Device Architecture clause on Control.
600-699	TBD	See UPnP Device Architecture clause on Control.

2.6.2 GetSupportedCredentialDelivery()

This action specifies a mechanism to determine what are the mechanisms for delivering credentials that are supported by the RATA.

2.6.2.1 Arguments

Table 2-7 — Arguments for GetSupportedCredentialDelivery()

Argument	Direction	relatedStateVariable
SupportedCredentialDelivery	OUT	CredentialDelivery

2.6.2.1.1 SupportedCredentialDelivery

This argument exposes which credential delivery mechanisms are supported by the device hosting the service.

Documents
Document Sharing Hub
Full document details: ISO IEC 29341-18-13-2011

2.6.2.2 Dependency on State

None.

2.6.2.3 Effect on State

None.

2.6.2.4 Control Point Requirements

None.

2.6.2.5 Errors

Table 2-8 — Error Codes for *GetSupportedCredentialDelivery()*

ErrorCode	errorDescription	Description
400-499	TBD	See UPnP Device Architecture clause on Control.
500-599	TBD	See UPnP Device Architecture clause on Control.
600-699	TBD	See UPnP Device Architecture clause on Control.

2.6.3 *GetCredentialsList()*

This action specifies a mechanism to determine the credentials currently available on the RATA.

2.6.3.1 Arguments

Table 2-9 — Arguments for *GetCredentialsList()*

Argument	Direction	relatedStateVariable
CurrentCredentialsList	*OUT*	*CredentialsList*

2.6.3.1.1 *CurrentCredentialsList*

This argument contains the list of credentials currently available on the RATA. Each entry in the list contains also a pointer to the respective credential.

2.6.3.2 Dependency on State

None.

2.6.3.3 Effect on State

None.

2.6.3.4 Control Point Requirements

Control points MUST select and remember the CredentialID from the list in order to provide this pointer in the *AddProfile()* action.

Documents
Document Sharing Hub

Full document details: ISO IEC 29341-18-13-2011