ISO/IEC 29341-18-11

Edition 1.0 2011-08

INTERNATIONAL STANDARD

colour inside

Information technology – UPnP device architecture – Part 18-11: Remote Access Device Control Protocol – Remote Access Discovery Agent Service

ISO/IEC 29341-18-11:2011(E)

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 It also gives information on projects, withdrawn and replaced publications.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

ISO/IEC 29341-18-11

Edition 1.0 2011-08

INTERNATIONAL STANDARD

Information technology – UPnP device architecture – Part 18-11: Remote Access Device Control Protocol – Remote Access Discovery Agent Service

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE F

ICS 35.200

ISBN 978-2-88912-643-9

CONTENTS

INFORMATION TECHNOLOGY – UPNP DEVICE ARCHITECTURE –

Part 18-11: Remote Access Device Control Protocol – Remote Access Discovery Agent 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 29341-18-11 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”.

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.

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 *RADAConfig* service. This service type enables configuration of the in-band synchronization mechanism between Remote Access Clients and Remote Access Server.

1.1 Introduction

A Remote Access Discovery Agent aggregates information about UPnP devices and services from two primary sources, depending if the devices are located in the local network or they are located in a remote device. For aggregating the devices and services available in the local network, the Remote Access Discovery Agent is constantly monitoring the SSDP traffic, which enables the RADA to have an up-to-date image of the UPnP network. The RADA finds information about remote UPnP devices and services by synchronizing with remote RADAs.

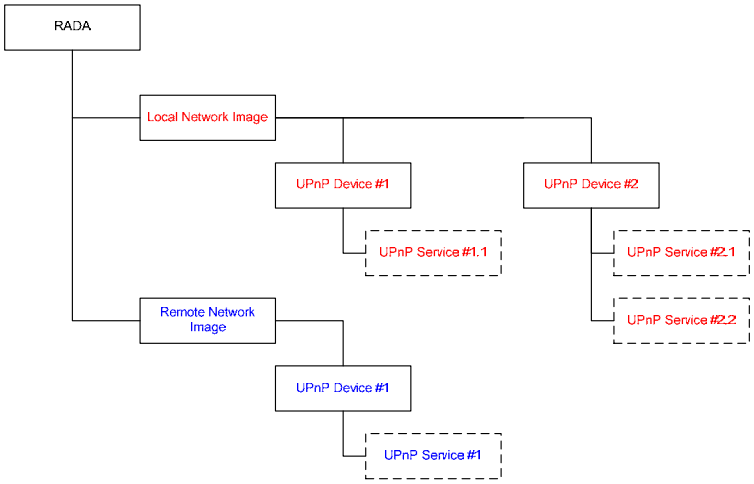

Figure 1-1 — SSDP Aggregation.

The main purpose in maintaining this aggregate view of available devices, is to alleviate the timing dependencies inherent in the UPnP Discovery mechanism. When a UPnP Control Point issues a search request, the request packet contains a parameter that specifies the maximum number of seconds a device can wait before sending the response. In remote scenarios, it is possible that this value will be exceeded with normal network traffic delay.

This aggregate view also serves to minimize the amount of SSDP traffic that needs to flow across the remote transport, as some remote scenarios may be cost-sensitive in regards to the amount of data that is transferred, since SSDP is often described as a “chatty” protocol.

The aggregate view could be used to restrict the visibility of local UPnP devices and services from remote devices and of UPnP devices and services hosted by remote devices to your local network.

This service does not address the actual transport protocol used to facilitate Remote Access.

The *RADAConfig* service is a UPnP service that provides control points with the following functionality:

- Customize which local devices are visible in remote networks
- Customize which remote devices are visible in the local network

This service does not address:

- Aggregation of the the local view of the UPnP network.
- Relaying discovery messages in the local network on behalf of remote devices
- Transport protocol used to facilitate Remote Access or its configurtion.

1.2 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”.

1.3 References

1.3.1 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.

[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.

[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://www.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.

[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/.

1.3.2 Informative References

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

[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.

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:*RADAConfig:1*

RADAConfig service is used herein to refer to this service type.

2.2 Terms and Abbreviations

2.2.1 Abbreviations

Table 2-1 — Abbreviations

Definition	Description
RAC	Remote Access Client
RADA	Remote Access Discovery Agent
RAS	Remote Access Server

2.2.2 Terms

2.2.2.1 Local device

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

2.2.2.2 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.

2.2.2.3 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.

2.2.2.4 Remote device

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

2.2.2.5 SystemInfo Change

The SystemInfo change happens when one of the following occurs:

- A Remote Access connection is established
- A Remote Access connection is ended
- A Remote Access Transport profile is added/modified/deleted
- A device joins a remote network
- A device leaves a remote network
- A filter is added/modified/deleted

2.2.2.6 UpdateID

An unsigned integer associated with *SystemInfo*. The value is incremented each time the *SystemInfo* is modified. Upon reaching the value 2^{32}-1, the next update rolls the value back to zero.

2.3 *RADAConfig* Service Architecture

The Remote Access Architecture defines management interfaces that allow the configuration of the ACLs that will restrict the visibility of the home devices from the remote control points and of remote devices from local control points.

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	
SystemInfoUpdateID	*R*	ui4	See Clause 2.4.3	
A_ARG_TYPE_FilterList	*R*	string	See Clause 2.4.4	
A_ARG_TYPE_UUID	*R*	string	See Clause 2.4.5	
[a] *R* = Required, *O* = Optional, *X* = Non-standard				

2.4.2 *SystemInfo*

This state variable contains the snapshot of all devices that are reachable/visible from the RADA, which are grouped according to the network in which they are present. The state variable contains also the identity of the remote networks, and filters that determine how the synchronization process will be performed.

The structure of the *SystemInfo* state variable 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: implementers must be aware that this state variable is shared with the RADASync service, which updates the information about remote devices, and with the RATAConfig service, which maintains information about Remote Access Transport profiles. This state variable MUST be updated by the device and propagated internally to those other services (if present on the same device). Each modification in *SystemInfo* MUST be signalled by the device through the *SystemInfoUpdateID* evented state variable (see Clause 2.4.3).

2.4.3 *SystemInfoUpdateID*

This state variable contains the value of the *updateID* attribute of the <systemInfo> element in the *SystemInfo* state variable XML Document. Its value is updated each time a SystemInfo Change occurs (see Clause 2.2.2.5). Note that the *SystemInfo* state variable may also be changed by the RADASync and RATAConfig services. Therefore, the RADAConfig service MUST event the *SystemInfoUpdateID* state variable, even if one of the other services (on the same device) is responsible for changing the *SystemInfo*.

2.4.4 *A_ARG_TYPE_FilterList*

The structure of the *A_ARG_TYPE_FilterList* state variable is a DADS XML Document:

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

Note that since the value of *A_ARG_TYPE_FilterList* 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 *A_ARG_TYPE_UUID*

This state variable is introduced to provide type information for action arguments used for identifying a particular local or remote network.

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*			
SystemInfoUpdateID	*YES*	*NO*			
A_ARG_TYPE_FilterList	*NO*	*NO*			
A_ARG_TYPE_UUID	*NO*	*NO*			

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

[b] (N) * (allowedValueRange Step)

2.5.1 Relationships Between State Variables

The *SystemInfoUpdateID* state variable is updated when the *SystemInfo* state variable is changed. Note that the *SystemInfo* state variable may also be changed by the RADASync and RATAConfig services.

2.6 Actions

Table 2-4 — Actions

Name	R/O [a]
GetSystemInfo()	*R*
EditFilter()	*R*

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

2.6.1 *GetSystemInfo()*

This action exposes information about particular device(s) on the local and/or remote networks. A Control Point may invoke this action to determine the list of devices visible for a credential, or to view the list of credentials that have access to a particular device.

2.6.1.1 Arguments

Table 2-5 — Arguments for *GetSystemInfo()*

Argument	Direction	relatedStateVariable
ID	*IN*	*A_ARG_TYPE_UUID*
SystemInfo	*OUT*	*SystemInfo*

2.6.1.1.1 ID

The UUID of the RADA of a network or the UUID of a device for which the *SystemInfo* is requested. If the value is “*” then the full SystemInfo is returned.

2.6.1.1.2 SystemInfo

The entire or a subset of the SystemInfo tree specific to the RADA indicated by the UUID.

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 *GetSystemInfo()*

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.
701	ID Not Found	The UUID corresponding to the ID specified does not match any devices found on the local or remote network.

2.6.2 *EditFilter()*

This action allows a Control Point to modify the accessibility settings for the specified device(s) on the local network. Only those devices which meet the criteria specified by the Filters in the system will be exposed to the Remote Access Client Device (Export) or the Home Network (Import).

2.6.2.1 Arguments

Table 2-7 — Arguments for *EditFilter()*

Argument	Direction	relatedStateVariable
Filter	*IN*	*A_ARG_TYPE_FilterList*

2.6.2.1.1 Filter

The Filter settings for one or more networks, to insert into, remove from, or edit inside the filter table. The type of operation (add, delete, edit) is indicated by the *updateType* attribute in the filterList XML document.

2.6.2.2 Dependency on State

If the *updateType* is “add” or “delete” then if the *controlMode* of the specified filter argument is different from the *exportControlMode* or the *importControlMode* of the corresponding RADA listed in the *SystemInfo* state variable and there is at least one filter defined for that RADA in the *SystemInfo* state variable, then the action MUST fail with an error code 702 (Invalid Filter).

2.6.2.3 Effect on State

The *Filter* is used to modify the appropriate *accessControl* fields on the *SystemInfo* state variable. The modification of the *SystemInfo* state variable results in an update of the *SystemInfoUpdateID* evented state variable.

Note: Since the *SystemInfo* state variable is shared with the RATAConfig and RADASync services, the implementation MUST propagate the modification of its value internally to those services, if present on the same device.

2.6.2.4 Control Point Requirements

Prior to modifying the filters using the *EditFilter()* action, a Control Point SHOULD examine the currently set filters. This can be done by invoking the *GetSystemInfo()* action. A Control Point SHOULD use the *SystemInfoUpdateID* evented state variable to determine whether the *SystemInfo* state variable has changed since the previous time it invoked the *GetSystemInfo()* action.

To modify the *exportControlMode* or the *importControlMode* of a RADA, a Control Point SHOULD first invoke the *EditFilter()* action to delete the corresponding filter and then invoke the *EditFilter()* action again to add the desired filter.

2.6.2.5 Errors

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

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.
702	Invalid Filter	The provided Filter is not valid.

2.6.3 Relationships Between Actions

The *GetSystemInfo* action is used to fetch filter information that can be updated using the *EditFilter* action Complete filter tables can be swapped into and out of the service.

2.6.4 Error Code Summary

The following table lists error codes common to actions for this service type. If an action results in multiple errors, the most specific error should be returned.

Table 2-9 — Error Code Summary

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.
700		Reserved for future extensions.
701	ID Not Found	The UUID corresponding to the ID specified does not match any devices found on the local or remote network.
702	Invalid Filter	The provided Filter is not valid.

Note: 800-899 Error Codes are not permitted for standard actions. See UPnP Device Architecture clause on Control for more details.

2.7 Theory of Operation

2.7.1 Getting Partial SystemInfo

A control point can request the full *SystemInfo* structure by including the "*" as the value of the *ID* argument of the *GetSystemInfo()* action.

A control point may request a subset of the SystemInfo tree by including specific UUID as the value of the ID argument of the *GetSystemInfo()* action. For example if the control point indicates the UUID of a remote RADA then the returned value will be the list of the devices that are visible from the remote network the RADA is attached to. For getting information about a particular device, the control point needs to indicate the UUID of the device itself as the value of the *ID* argument of the *GetSystemInfo()* action. The return value will include the remote network that exposes the device but only the particular device will be listed as available from that network.

2.7.2 Filter Editing

The RADAConfig service's primary role is to configure the filters that are used by the RADASync service, during its synchronization process between Remote Access Servers and Remote Access Clients.

There are two types of filters that the RADAConfig service defines: allowList and denyList filters. When allowlist filtering is specified, without any filters defined by the RADAConfig service, the RADASync would not expose local devices when synchronizing with a remote network, respectively it would not allow discovery of remote devices from a remote network on the local network. If denyList filtering is specified, without any filters defined by the RADAConfig service, the RADASync would expose all the local devices when synchronizing with a remote network, and it would allow the discovery of remote devices from that remote network on the local network.

The default control mode for the export filter is "allowList" and for the import filter is "denyList". A particular implementation may change this behavior.

When a Remote Access Client established a secure tunnel to the Remote Access Server, the RADASync service on the RAS establishes a synchronization session with the RADASync on the RAC. The RADASync service refers to the filter policy defined by the RADAConfig service to determine how devices should be added to the local/remote branches of a synchronization tree.

If one would like to access some of the local devices remotely, all one would need to do is to invoke the *EditFilter* action. The simplest type of filter, is simply a pass-thru filter, where the specified filter allows all devices to be exposed outside the home. Such a filter would look like:

```
<?xml version="1.0" encoding="UTF-8"?>
<dads xmlns="urn:schemas-upnp-org:ra:dads"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="urn:schemas-upnp-org:ra:dads
   http://www.upnp.org/schemas/ra/dads-v1.xsd">
   <filterList>
      <filter
         target="31638B2A-AC78-4766-82D5-D53C6480638A"
         controlMode="denyList"
         updateType="edit">
      </filter>
   </filterList>
</dads>
```

The filter specified above, would allow all the devices on the local network to be discoverable on the remote network, regardless of which transport credential was used to establish the secure tunnel.

A more typical filter would be one that more tightly scopes the devices and credentials that are discoverable on the remote network. Such a filter may look like the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<dads xmlns="urn:schemas-upnp-org:ra:dads"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="urn:schemas-upnp-org:ra:dads
   http://www.upnp.org/schemas/ra/dads-v1.xsd">
   <filterList>
      <filter
         target="31638B2A-AC78-4766-82D5-D53C6480638A"
         controlMode="allowList"
         updateType="add">
         <deviceInfo
            uuid="12338B2A-AC78-4766-82D5-D53C64806ABC"
            <accessControl>
               <access credentialID="David MP3 Player"></access>
            </accessControl>
         </deviceInfo>
      </filter>
   </filterList>
</dads>
```

The filter specified above, only allows the Remote Access Client that uses the credential identified by “David MP3 Player” to discover the media server with the specified UUID.

3 XML Service Description

```
<?xml version="1.0"?>
<scpd xmlns="urn:schemas-upnp-org:service-1-0">

   <specVersion>
      <major>1</major>
      <minor>0</minor>
   </specVersion>

   <actionList>

      <action>
         <name>GetSystemInfo</name>
         <argumentList>
            <argument>
               <name>ID</name>
               <direction>in</direction>
               <relatedStateVariable>
                  A_ARG_TYPE_UUID
```

```
                </relatedStateVariable>
            </argument>
            <argument>
                <name>SystemInfo</name>
                <direction>out</direction>
                <relatedStateVariable>
                    SystemInfo
                </relatedStateVariable>
            </argument>
        </argumentList>
    </action>

    <action>
        <name>EditFilter</name>
        <argumentList>
            <argument>
                <name>Filter</name>
                <direction>in</direction>
                <relatedStateVariable>
                    A_ARG_TYPE_FilterList
                </relatedStateVariable>
            </argument>
        </argumentList>
    </action>

    <!-- Declarations for other actions defined by UPnP vendor
         (if any)go here. -->

</actionList>

<serviceStateTable>

    <stateVariable sendEvents="no">
        <name>SystemInfo</name>
        <dataType>string</dataType>
    </stateVariable>

    <stateVariable sendEvents="yes">
        <name>SystemInfoUpdateID</name>
        <dataType>ui4</dataType>
    </stateVariable>

    <stateVariable sendEvents="no">
        <name>A_ARG_TYPE_FilterList</name>
        <dataType>string</dataType>
    </stateVariable>

    <stateVariable sendEvents="no">
        <name>A_ARG_TYPE_UUID</name>
        <dataType>string</dataType>
    </stateVariable>

    <!-- Declarations for other state variables defined by
         UPnP vendor (if any)go here. -->

</serviceStateTable>
</scpd>
```

4 Test

No semantic tests have been specified for this service.

Annex A RemoteAccessDiscoveryAgent Structures (Normative)

A.1 FilterList Template

The following shows the generalized layout of a FilterList Template. More elements and/or attributes MAY be added in future versions of FilterList templates.

The *forum* character style is used to indicate names defined by the RAWC. Implementations need to fill out the parts that are printed in *vendor* character style.

```
<?xml version="1.0" encoding="UTF-8"?>
<dads xmlns="urn:schemas-upnp-org:ra:dads"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="urn:schemas-upnp-org:ra:dads
   http://www.upnp.org/schemas/ra/dads-v1.xsd">
   <filterList>
      <filter
         target=""
         controlMode=""
         updateType="">
         <deviceInfo
            uuid="">
            <accessControl>
               <access credentialID=""></access>
               <!-- Any other access (if any) go here.-->
            </accessControl>
         </deviceInfo>
         <!--Any other deviceInfo (if any) go here.-->
      </filter>
      <!-- Any other filter (if any) go here.-->
   </filterList>
</dads>
```

xml
REQUIRED for all XML documents. Case sensitive.

RADA
REQUIRED. Must have “urn:schemas-upnp-org:ra:dads” as the value for the xmlns attribute; this references the UPnP Remote Access Working Committee RADA Datastructure Template Schema. As long as the same xmlns is used, the data structure template MUST be backward compatible, i.e. usable by legacy implementations.

filterList
REQUIRED. Contains the list of filters to be added to the SystemInfo. Contains the following sub elements:

filter
REQUIRED. Contains the filter that will be applied to a single network. Contains the following sub elements:

@target
REQUIRED. xs:string. Contains the UUID of the RADA device on which the filter will be applied. This could be the local RADA or a remote RADA.

@controlMode
REQUIRED. xs:token. Contains the access control mode for advertising devices. Possible values are “allowList” or “denyList”.

@updateType
REQUIRED. xs:token. Determines if a filter will be created, edited or deleted. The corresponding values of @updateType are “add”, “edit”, and “delete”.

deviceInfo
OPTIONAL. Contains information about a single device in the network. MUST be omitted when the filter@target represents a remote RADA. When the filter@target represents the local RADA, deviceInfo MUST be present for each device present in the network. Contains the following sub elements:

@uuid

REQUIRED. xs:string. Contains the UUID of the root device.

accessControl

OPTIONAL. Contains the list of remote RADAs that can or cannot see this local device. Contains the following sub elements:

access

OPTIONAL. Describes the remote RADA that can or cannot see the local device. Contains the following attribute:

@credentialID

REQUIRED. xs:string. Contains the identity of the remote RADA that is affected by this entry. If filter@controlMode is “allowList”, the remote RADA has visibility rights on this local device. If filter@controlMode is “denyList”, the remote RADA does not have visibility rights on this local device.

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch