INSO
13285-18-13
1st. Edition
2015

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۱۳۲۸۵-۱۸-۱۳
چاپ اول
۱۳۹۳

فناوری اطلاعات- معماری افزاره‌ی جامع اتصال و اجرا (UPnP)

- قسمت ۱۸-۱۳: پروتکل واپایش (کنترل) افزاره دسترسی از دور-

خدمت پیکربندی عامل کشف دسترسی از دور

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

ICS:35.200

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2 - International Electrotechnical Commission
3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات- معماری افزاره‌ی جامع اتصال و اجرا (UPnP)- قسمت ۱۸-۱۳: پروتکل واپایش (کنترل) افزاره دسترسی از دور- خدمت پیکربندی عامل کشف دسترسی از دور»

رئیس:	**سمت و/ یا نمایندگی**
ماندگاری، مریم (فوق لیسانس مهندسی صنایع-سیستم و بهره وری)	رئیس واحد انفورماتیک اداره کل استاندارد یزد
دبیر:	
ملک زاده، راحله السادات (لیسانس مهندسی کامپیوتر)	کارشناس شرکت پارس معیار سنجش ایساتیس
اعضاء: (اسامی به ترتیب حروف الفبا)	
تقوی، مسعود (لیسانس مهندسی کامپیوتر)	کارشناس انفورماتیک اداره کل استاندارد یزد
تدین تفت، عذرا (لیسانس مهندسی صنایع)	کارشناس صنایع کوچک شرکت شهرکهای صنعتی یزد
تدین تفت، علی اکبر (دکترای مخابرات-سیستم)	عضو هیات علمی دانشگاه یزد
حق شناس، مهدی (فوق لیسانس مهندسی کامپیوتر)	مدیر فنی شرکت پیشگامان کی پاد
حکیمی، سید محمد هاشم (لیسانس مهندسی الکترونیک)	کارشناس شرکت مخابرات استان یزد
زارعی محمود آبادی، محمد حسین (دکترای برق-الکترونیک)	کارشناس استاندارد
طباطبایی، فریده (لیسانس مهندسی کامپیوتر)	کارشناس انفورماتیک برق منطقه‌ای یزد

محمدیان سرچشمه، محمد حسین
(لیسانس علوم کامپیوتر)
مدیر پروژه شرکت پیشگامان کی پاد

فهرست مندرجات

عنوان **صفحه**

پیش گفتار

استاندارد «فناوری اطلاعات- معماری افزاره‌ی جامع اتصال و اجرا (UPnP)- قسمت ۱۸-۱۳: پروتکل واپایش (کنترل) افزاره دسترسی از دور- خدمت پیکربندی عامل کشف دسترسی از دور» که پیش نویس آن در کمیسیون های مربوط، توسط شرکت پارس معیار سنجش ایساتیس تهیه و تدوین شده است و در سیصد و شصت و نهمین اجلاس کمیته ملی استاندارد فناوری اطلاعات مورخ ۹۳/۱۲/۹ مورد تصویب قرار گرفته است ، اینک به استناد بند یک ماده ۳ قانون اصلاح قواعد و مقررات موسسه استاندارد و تحقیقات صنعتی ایران ، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می شود .

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینه صنایع ، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود ، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت . بنابراین، باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد .

منبع و ماخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

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.

فناوری اطلاعات- معماری افزاره‌ی جامع اتصال و اجرا (UPnP)- قسمت ۱۸-۱۳: پروتکل واپایش (کنترل) افزاره دسترسی از دور- خدمت پیکربندی عامل کشف دسترسی از دور

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین و تعریف خدمتی سازگار با معماری افزاره UPnP نگارش ۱٫۰ است و در اینجا به عنوان نوعی از خدمت تحت عنوان *RATAConfig* تعریف می‌شود.

۱-۱ مقدمه

خدمت *RATAConfig*، یک خدمت UpnP است، که به نقاط واپایش اجازه تدارک و پیکربندی پارامترهایی را می‌دهد، که برای قادر ساختن کارساز دسترسی از دور برای پذیرش و کارخواه دسترسی از دور برای راه اندازی اتصال‌ها، ضروری هستند. این خدمت، نقاط واپایشی با کارکردهای زیر را ارائه می‌دهد:

- تعیین عامل‌های کشف دسترسی از دور که می‌توانند توسط خدمت پیکربندی شوند.
- تعیین سازوکارهای تحویل برای اعتبارنامه‌هایی[۱] که توسط خدمت پشتیبانی می‌شوند.
- پیکربندی رخ‌نماهای[۲] عامل انتقال دسترسی از دور.
- مدیریت رخ‌نماهای عامل انتقال دسترسی از دور.

این خدمت موارد زیر را پوشش نمی‌دهد:

- مدل اعتماد[۳] که اتصالات دسترسی از دور امن را امکان پذیر خواهد کرد.
- تحویل اعتبار نامه‌ها.

۱-۲ نمادگذاری

در این استاندارد علاوه بر فعل‌های وجهی که شرح آن در استاندارد ملی شماره ۵ آمده است از کلمات کلیدی زیر نیز استفاده شده است:

ممنوع[۴]- تعریف یا رفتاری که منع مطلق این ویژگی است. متضاد الزام[۵].

به طور مشروط الزامی[۱]- تعریف یا رفتار به شرایط بستگی دارد. اگر شرایط تعیین‌شده برقرار بود، آنگاه تعریف تعریف یا رفتار لازم است، درغیر اینصورت ممنوع است.

1- Credential
2 -Profiles
3- Trust model
4- PROHIBITED
5- REQUIRED

به طور مشروط اختیاری- تعریف یا رفتار به شرایط بستگی دارد. اگر شرایط تعیین‌شده برقرار بود، تعریف یا رفتار اختیاری است، درغیر این صورت ممنوع است.
بنابراین این کلمات کلیدی به صورت پررنگ نوشته می‌شوند تا به طور واضح الزامات پروتکل و مشخصات کاربردی و رفتار تاثیرگذار بر همکاری متقابل[۲] و امنیت پیاده‌سازی‌ها را مشخص کنند. هنگامی که این کلمات به پررنگ نباشند، در معنای اصلی خود به کار می‌روند.

- رشته‌هایی که در معنای تحت اللفظی به کار می‌روند در داخل علامت نقل قول («») قرار می‌گیرند.
- مقادیر نگهدارنده مکان[۳] که لازم است جایگزین شوند در داخل ابرو قرار ({}) می‌گیرند.
- کلمات مورد تاکید به صورت کج (مایل) چاپ می‌شوند.
- کلمات کلیدی تعریف شده توسط کمیته کاری UPnP با استفاده از سبک نویسه‌های کلمه *forum* چاپ می‌شوند.
- کلمات کلیدی تعریف شده توسط معماری افزاره UPnP با استفاده از سبک نویسه‌های کلمه **arch** چاپ می‌شوند.

علامت دو تا دو نقطه حایل (::)به رابطه پدر-فرزندی[۴] (پدر::فرزند) سلسله مراتبی میان دو شیء اشاره دارد که توسط دو تا دو نقطه از هم جدا می شود . این حایل در چندین زمینه استفاده می‌شود، برای مثال:
Service::Action(), Action()::Argument,parentProperty::childProperty

۱-۳ الحاقیه‌های تعریف شده-توسط-عرضه‌کننده

هر موقع عرضه‌کننده‌ها، متغیرهای حالت، اقدامات یا خصوصیات تعریف‌شده-توسط-عرضه‌کننده دیگری را ایجاد کنند، نام‌های اختصاص یافته و نمایش XML آنها، **باید** از قواعد نامگذاری و قوانین XML مشخص شده در بند ۲-۵ [DEVICE] «شرح: الحاقیه‌های غیر استاندارد عرضه‌کننده» تبعیت کند.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آنها ارجاع شده است. به این ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب می‌شود.
در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن موردنظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی آن‌ها موردنظر است.
استفاده از مراجع زیر برای این استاندارد الزامی است:

2-1 [DEVICE] – UPnP Device Architecture, version 1.0. Available at:

1- CONDITIONALLY REQUIRED
2- interoperability
3- Placeholder values
4- parent-child

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.
2-2 [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
2-3 [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.
2-4 [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.
2-5 [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.
2-6 [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.
2-7 [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.
2-8 [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.
2-9 [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.
2-10 [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.
2-11 [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/.

۲ اصطلاحات و تعاریف، نمادها، کوته‌نوشت‌ها و یکاها

در این استاندارد اصطلاحات و تعاریف، نمادها، اختصارات و یکاها زیر به کار می‌رود:

۱-۳

نوع خدمت

نوع خدمت زیر مشخص‌کننده خدمتی است که با این مشخصات سازگار است:

urn:schemas-upnp-org:service: *RATAConfig:1*

در اینجا از خدمت برای اشاره به این نوع خدمت استفاده می‌شود.

۳-۲ اصطلاحات و کوته‌نوشت‌ها

۳-۲-۱ کوته‌نوشت‌ها

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

تشخیص متناظر مرده(از دسترس خارج شده)
پایه‌بار امنیت فشرده سازی
تبادل کلید اینترنت
امنیت IP
کارخواه دسترسی از دور
عامل کشف دسترسی از دور
کارساز دسترسی از دور
انتقال دسترسی از دور
عامل کشف دسترسی از دور

۳-۲-۲ اصطلاحات و تعاریف

۳-۲-۲-۱

اعتبارنامه[1]

اصطلاح اعتبارنامه‌ها به گواهی‌نامه‌ها، اطلاعات محرمانه به اشتراک گذاشته شده، یا سایر ابزارهای اصالت‌سنجی مورد استفاده در مفهوم RATA اشاره دارد.

۳-۲-۲-۲

افزاره محلی

یک افزاره محلی یک افزاره UPnP است که به شبکه فیزیکی‌ای که RADA در آن قرار دارد، وصل می‌شود.

۳-۲-۲-۳

میز فرمان مدیریت[2]

مجموعه‌ای از نقاط واپایش که برای پیکربندی و پایش خدمات مربوط به دسترسی از دور استفاده می‌شوند.

۳-۲-۲-۴

کارخواه دسترسی از دور (RAC)

افزاره فیزیکی متناظر است که جزئی از شبکه فیزیکی خانگی نیست و تنها خدمات و افزاره UPnP تعبیه‌شده در افزاره فیزیکی را آشکار می‌کند.

---

1 - Credentials
2 - Management Console

۳-۲-۲-۵

واسط شبکه دسترسی از دور

واسط شبکه RA یک واسط شبکه‌ای ایجاد شده توسط عامل انتقال دسترسی از دور است. تنظیمات لازم برای استفاده از این واسط در رخنمای RAT موجود است.

۳-۲-۲-۶

کارساز دسترسی از دور (RAS)

افزاره فیزیکی متناظر واقع در شبکه خانگی است. RAS، خدمات و افزاره‌های موجود بر روی شبکه فیزیکی خانگی و همچنین افزاره‌ها و خدمات تعبیه شده در افزاره‌ی RAS فیزیکی را برای RAC افشا می‌کند.

۳-۲-۲-۷

رخنمای عامل انتقال دسترسی از دور[1]

رخنمای RATA اتصال RATA پیکربندی شده است که آماده استفاده برای پذیرش ارتباطات سمت RAS یا شروع کردن ارتباطات سمت RAC است.

۳-۲-۲-۸

افزاره‌ی از دور

افزاره‌ی از دور، یک افزاره‌ی UPnP است که به شبکه فیزیکی‌ای که RADA در آن است، متصل نیست.

۳-۳ معماری خدمت *RATAConfig*

این خدمت مسئول ارائه یک واسط پیکربندی برای یک کانال ارتباطی امن است که یک افزاره UPnP را قادر می‌سازد تا با افزاره‌های UPnP مستقر در شبکه خانگی تعامل کند.

۳-۴ متغیرهای حالت

یادآوری- ممکن است برای خواننده در بار اول خواندن تعاریف اقدام[2] قبل از خواندن تعاریف متغیر حالت مفیدتر باشد.

۳-۴-۱ مروری بر متغیر حالت

جدول ۱- متغیرهای حالت

نام متغیر	R/O[a]	نوع داده	مقادیر مجاز	واحدهای مهندسی
SystemInfo	*R*	رشته	به بند ۲-۴-۲ مراجعه شود.	
TransportAgentCapabilities	*R*	رشته	به بند ۲-۴-۲- ۳ مراجعه شود.	

1- Remote Access Transport Agent Profile
2- Action

جدول ۱- متغیرهای حالت

نام متغیر	R/O[a]	نوع داده	مقادیر مجاز	واحدهای مهندسی
CredentialDelivery	*R*	رشته	به بند ۲-۴-۴ مراجعه شود.	
CredentialsList	*R*	رشته	به بند ۲-۴-۵ مراجعه شود.	
ProfileList	*R*	رشته	به بند ۲-۴-۶ مراجعه شود.	
A_ARG_TYPE_ProfileConfigInfo	*R*	رشته	به بند ۲-۴-۷ مراجعه شود.	
A_ARG_TYPE_ProfileID	*R*	ui4	به بند ۲-۴-۸ مراجعه شود.	
[a] الزامی=R و O= اختیاری و X=غیراستاندارد				

۳-۴-۲ متغیر *SystemInfo*

این متغیر حالت شامل برگرفتی[1] از تمام شبکه‌هایی که RATA با آن ارتباط دارد، وضعیت اتصال و هویت مرتبط با شبکه راه دور است.

ساختار آرگومان *SystemInfo* یک سند DADS XML است:

- <SystemInfo> عنصر ریشه است.
- برای جزئیات بیشتر ساختار به طرح DADS [DADS-XSD] مراجعه شود. ویژگی‌های موجود و اسامی آنها در بند A.1 [RADASync] شرح داده می‌شود.

توجه کنید که از آنجا که مقدار *SystemInfo*، XML است، لازم است که قبل از تعبیه شدن در یک پیغام پاسخ SOAP رها (اسکیپ)[2] شود (استفاده از قواعد XML معمولی: بند ۲-۴ [XML]، نشانه‌گذاری و داده نویسه)

یادآوری- *SystemInfo* نگهداری شده توسط خدمت RATAConfig، توسط خدمات RADASync و RADAConfig نیز به اشتراک گذاشته می‌شود. این متغیر حالت باید برای راه‌اندازی فرآیند همزمان‌سازی RADA هنگامی‌که شبکه‌های راه دور جدید دردسترس می‌شوند یا شبکه‌های راه دور موجود از دسترس خارج می‌شوند، توسط افزاره به روزرسانی و به صورت داخلی به آن خدمات دیگر پخش شود. به علاوه، درخواست‌های اقدامات *AddProfile()*، *DeleteProfile()* و *EditProfile()* هم منجر به اصلاح این متغیر حالت می‌شوند. هر اصلاحی در *SystemInfo* باید توسط افزاره از طریق متغیر حالت رویداد *SystemInfoUpdateID* خدمت *RADAConfig* خبر داده شود (به بند ۲-۴-۳ RADAConfig مراجعه شود).

1- Snapshot
2- Needs to be escaped

۳-۴-۳ متغیر *TransportAgentCapabilities*

این متغیر حالت شامل فهرست پروتکل‌های عامل انتقال دسترسی از دور و توانمندی‌های آنها که توسط RATAConfig پشتیبانی می‌شود، است.

ساختار آرگومان *TransportAgentCapabilities* یک سند TADS XML است.

- <transportAgentCapability> عنصر ریشه است.
- برای جزئیات بیشتر ساختار به طرح TADS، [TADS-XSD] مراجعه شود. ویژگی‌های موجود و اسامی آنها در بند الف-۳ شرح داده شده است. مثال‌های در بندهای پ-۲-۱-۱، پ-۲-۲-۱ و پ-۲-۳-۱ ارائه شده است.

توجه کنید که از آنجا که مقدار *TransportAgentCapabilities*، XML است، لازم است که قبل از تعبیه شدن در یک پیغام پاسخ SOAP رها (اسکیپ) شود (استفاده از قواعد XML معمولی: بند ۲-۴ [XML]، نشانه‌گذاری و داده نویسه)

۴-۴-۳ متغیر *CredentialDelivery*

این متغیر حالت شامل فهرست سازوکارهای تحویل اعتبارنامه مورد پشتیبانی RATAConfig است.

ساختار آرگومان *CredentialDelivery* یک سند TADS XML است.

- <credentialDelivery> عنصر ریشه است.
- برای جزئیات بیشتر ساختار به طرح TADS، [TADS-XSD] مراجعه شود. ویژگی‌های موجود و اسامی آنها در بند الف-۴ شرح داده شده است.

توجه کنید که از آنجا که مقدار *CredentialDelivery*، XML است، لازم است که قبل از تعبیه شدن در یک پیغام پاسخ SOAP رها شود (استفاده از قواعد XML معمولی: بند ۲-۴ [XML]، نشانه‌گذاری و داده نویسه)

۵-۴-۳ متغیر *CredentialsList*

این متغیر حالت شامل فهرست اعتبارنامه‌های موجود در RATA است.

ساختار آرگومان *CredentialsList* یک سند TADS XML است:

- <CredentialsList> عنصر ریشه است.
- برای جزئیات بیشتر ساختار به طرح TADS، [TADS-XSD] مراجعه شود. ویژگی‌های موجود و اسامی آنها در بند الف-۵ شرح داده شده است.

توجه کنید که از آنجا که مقدار *CredentialsList*، XML است، لازم است که قبل از تعبیه شدن در یک پیغام پاسخ SOAP رها شود(استفاده از قواعد XML معمولی: بند ۲-۴ [XML] ، نشانه‌گذاری و داده نویسه)

۲-۴-۶ متغیر *ProfileList*

این متغیر حالت شامل فهرست رخ‌نماهای پیکربندی شده روی RATA است.

ساختار آرگومان *ProfileList* یک سند TADS XML است:

- <profileList> عنصر ریشه است.
- برای جزئیات بیشتر ساختار به طرح TADS، [TADS-XSD] مراجعه شود. ویژگی‌های موجود و اسامی آنها در بند الف-۱ شرح داده شده است.

توجه کنید که از آنجا که مقدار *ProfileList*، XML است، لازم است که قبل از تعبیه شدن در یک پیغام پاسخ SOAP رها شود (استفاده از قواعد XML معمولی: بند ۲-۴ [XML] ، نشانه‌گذاری و داده نویسه)

۳-۴-۷ متغیر *A_ARG_TYPE_ProfileConfigInfo*

این متغیر حالت شامل اطلاعات پیکربندی رخ‌نما برای پروتکل انتقال دسترسی از دور پشتیبانی شده توسط RATA است.

ساختار آرگومان A_ARG_TYPE_ProfileConfigInfo یک سند TADS XML است:

- <profileConfig> عنصر ریشه است.
- برای جزئیات بیشتر ساختار به طرح TADS، [TADS-XSD] مراجعه شود. ویژگی‌های موجود و اسامی آنها در بند الف-۲ شرح داده شده است. مثال‌های در بندهای پ-۲-۱-۲، پ-۲-۱-۳، پ-۲-۲-۲، پ-۲-۲-۳، پ-۲-۳-۲، پ-۲-۳-۳، ت-۲-۱ و ت-۲-۲ ارائه شده است.

توجه کنید که از آنجا که مقدار *A_ARG_TYPE_ProfileConfigInfo*، XML است، لازم است که قبل از تعبیه شدن در یک پیغام پاسخ SOAP رها شود (استفاده از قواعد XML معمولی: بند ۲-۴ [XML] ، نشانه‌گذاری و داده نویسه)

۳-۴-۸ متغیر *A_ARG_TYPE_ProfileID*

این متغیر شامل ID منحصر به فرد برای یک رخ‌نما است.

۳-۵ رویداد و تعدیل[1]

جدول ۲- رویداد و تعدیل

نام	رویداد	رویداد تعدیل شده	بیشینه نرخ رویداد[a]	ترکیب منطقی	کمینه دلتا در هر رویداد[b]
SystemInfo	نه	نه			
TransportAgentCapabilities	نه	نه			
CredentialDelivery	نه	نه			

1- Eventing and Moderation

جدول ۲- رویداد و تعدیل

نام	رویداد	رویداد تعدیل شده	بیشینه نرخ رویداد[a]	ترکیب منطقی	کمینه دلتا در هر رویداد[b]
CredentialsList	بله	نه			
ProfileList	نه	نه			
A_ARG_TYPE_ProfileConfigInfo	نه	نه			
A_ARG_TYPE_ProfileID	نه	نه			

[a] با N مشخص شده، $\text{نرخ} = \frac{\text{رویداد}}{\text{Nثانیه}}$

[b] * (N) (مرحله گستره مقدار مجاز (allowedValueRange Step))

۳-۵-۱ ارتباطات میان متغیرهای حالت

هیچ ارتباطی وجود ندارد.

۳-۶ اقدامات

جدول ۳- اقدامات

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

[a] الزامی=R و اختیاری=O و غیراستاندارد=X

۳-۶-۱ اقدام *GetTransportAgentCapabilities()*

این اقدام سازوکاری را برای تعیین پروتکل‌های عامل انتقال دسترسی از دور و توانمندی‌های آنها که توسط RATA پشتیبانی می‌شود، مشخص می‌کند.

۳-۶-۱-۱ آرگومان‌ها

جدول ۴- آرگومان‌های اقدام *GetTransportAgentCapabilities()*

آرگومان	جهت	متغیر حالت وابسته
TransportAgentCapabilities	خروجی	*TransportAgentCapabilities*

۳-۶-۱-۱-۱ آرگومان *TransportAgentCapabilities*

این آرگومان، توانمندی‌های عامل انتقال را آشکار می‌کند.

۳-۶-۱-۲ وابستگی به حالت

وجود ندارد.

۳-۶-۱-۳ تاثیر روی حالت

وجود ندارد.

۳-۶-۱-۴ الزامات نقاط واپایش

وجود ندارد.

۳-۶-۱-۵ خطاها

جدول ۵- کدهای خطا برای اقدام *GetTransportAgentCapabilities()*

کد خطا	شرح خطا	شرح
۴۹۹-۴۰۰	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.
۵۹۹-۵۰۰	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.
۶۹۹-۶۰۰	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.

۳-۶-۲ اقدام *GetSupportedCredentialDelivery()*

این اقدام سازوکاری برای تعیین این که کدام سازوکارها برای تحویل اعتبارنامه‌های پشتیبانی شده توسط RATA هستند، مشخص می‌کند.

۳-۶-۲-۱ آرگومان‌ها

جدول ۶- آرگومان‌های اقدام *GetSupportedCredentialDelivery()*

آرگومان	جهت	متغیر حالت وابسته
SupportedCredentialDelivery	خروجی	*CredentialDelivery*

۳-۶-۲-۱-۱ آرگومان *SupportedCredentialDelivery*

این آرگومان آشکار می‌کند که کدام سازوکارهای تحویل اعتبارنامه، توسط افزاره میزبان خدمت پشتیبانی می‌شوند.

۳-۶-۲-۲ وابستگی به حالت

وجود ندارد.

۳-۶-۲-۳ تاثیر روی حالت

وجود ندارد.

۳-۶-۲-۴ الزامات نقاط واپایش

وجود ندارد.

۳-۶-۲-۵ خطاها

جدول ۷- کدهای خطا برای اقدام *GetSupportedCredentialDelivery()*

کد خطا	شرح خطا	شرح
۴۰۰-۴۹۹	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.
۵۰۰-۵۹۹	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.
۶۰۰-۶۹۹	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.

۳-۶-۳ اقدام *GetCredentialsList()*

این اقدام سازوکاری برای تعیین اعتبارنامه‌هایی که در حال حاضر بر روی RATA موجود است، مشخص می‌کند.

۳-۶-۳-۱ آرگومان‌ها

جدول ۸- آرگومان‌های اقدام *GetCredentialsList()*

آرگومان	جهت	متغیر حالت وابسته
CurrentCredentialsList	خروجی	*CredentialsList*

۳-۶-۳-۱-۱ آرگومان *CurrentCredentialsList*

این آرگومان شامل فهرست اعتبارنامه‌هایی می‌شود که در حال حاضر بر روی RATA موجود است. هر ورودی در این فهرست شامل یک اشاره‌گر به اعتبارنامه مربوطه هم است.

۳-۶-۳-۲ وابستگی به حالت

هیچ.

۳-۶-۳-۳ تاثیر روی حالت

وجود ندارد.

۳-۶-۳-۴ الزامات نقاط واپایش

نقاط واپایش **باید** به منظور ارائه این اشاره‌گر در اقدام *AddProfile()*، ID اعتبارنامه را از فهرست انتخاب و به خاطر بسپارند.

۳-۶-۳-۵ خطاها

جدول ۹- کدهای خطا برای اقدام *GetCredentialsList()*

کد خطا	شرح خطا	شرح
۴۹۹-۴۰۰	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.
۵۹۹-۵۰۰	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.
۶۹۹-۶۰۰	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.

۳-۶-۴ اقدام *GetProfileList()*

این اقدام سازوکاری به منظور تعیین رخ‌نماهایی که در حال حاضر روی RATA پیکربندی شده‌اند، مشخص می‌کند.

۳-۶-۴-۱ آرگومان‌ها

جدول ۱۰- آرگومان‌های اقدام *GetProfileList()*

آرگومان	جهت	متغیر حالت وابسته
ProfileList	خروجی	*ProfileList*

۳-۶-۴-۱-۱ آرگومان *ProfileList*

این آرگومان شامل فهرستی از رخ‌نماهای پیکربندی شده، است.

۳-۶-۴-۲ وابستگی به حالت

وجود ندارد.

۳-۶-۴-۳ تاثیر روی حالت

وجود ندارد.

۳-۶-۴-۴ الزامات نقاط واپایش

وجود ندارد.

۳-۶-۴-۵ خطاها

جدول ۱۱- کدهای خطا برای اقدام *GetProfileList()*

کد خطا	شرح خطا	شرح
۴۹۹-۴۰۰	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.
۵۹۹-۵۰۰	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.
۶۹۹-۶۰۰	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.

۳-۶-۵ اقدام *AddProfile()*

این اقدام سازوکاری را به منظور پیکربندی رخنما برای RATA تعریف می‌کند.

۳-۶-۵-۱ آرگومان‌ها

جدول ۱۲- آرگومان‌های اقدام *AddProfile()*

آرگومان	جهت	متغیر حالت وابسته
NewProfileConfigInfo	ورودی	*A_ARG_TYPE_ProfileConfigInfo*

۳-۶-۵-۱-۱ آرگومان *NewProfileConfigInfo*

این آرگومان شامل گزینه‌های پیکربندی پروتکل و اعتبارنامه‌های مرتبط برای رخنمای جدید RATA است.

۳-۶-۵-۲ وابستگی به حالت

وجود ندارد.

۳-۶-۵-۳ تاثیر روی حالت

تاثیر این اقدام این است که افزاره باید یک ID منحصر به فرد برای رخنمایی که به تازگی ایجاد شده تولید و متغیر حالت *ProfileList* را به روز رسانی کند. از این گذشته، افزاره باید متغیر حالت *SystemInfo* را با اطلاعات رخنمای تازه ایجاد شده به روز رسانی کند.

یادآوری- از آنجا که متغیر حالت *SystemInfo* با خدمات RADASync و RADAConfig به اشتراک گذاشته می‌شود، پیاده‌سازی باید اصلاح مقدار آن را به صورت داخلی به آن خدمات، در صورت وجود در همان افزاره، پخش کند.

۳-۶-۵-۴ الزامات نقاط واپایش

وجود ندارد.

۳-۶-۵-۵ خطاها

جدول ۱۳- کدهای خطا برای اقدام *AddProfile()*

کد خطا	شرح خطا	شرح
۴۰۰-۴۹۹	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.
۵۰۰-۵۹۹	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.
۶۰۰-۶۹۹	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.
۷۰۱	داده رخنمای نامعتبر	داده رخنمای ارائه شده معتبر نیست.

۳-۶-۶ اقدام *EditProfile()*

این اقدام، سازوکاری برای به روز رسانی گزینه‌ها و پارامترهای رخنمای از قبل پیکربندی شده تعریف می‌کند.

۳-۶-۶-۱ آرگومان‌ها

جدول ۱۴- آرگومان‌های اقدام *EditProfile()*

آرگومان	جهت	متغیر حالت وابسته
ProfileID	ورودی	*A_ARG_TYPE_ProfileID*
UpdatedProfileConfigInfo	ورودی	*A_ARG_TYPE_ProfileConfigInfo*

۳-۶-۶-۱-۱ آرگومان *ProfileID*

این آرگومان ID رخ‌نمای ویرایش شده را نشان می‌دهد.

۳-۶-۶-۱-۲ آرگومان *UpdatedProfileConfigInfo*

این آرگومان شامل گزینه‌های پیکربندی به روز شده پروتکل و اعتبارنامه‌های مربوطه برای یک رخ‌نمای RAT است. اگرچه، **نباید** از آن برای تغییر نوع انتقال استفاده شود. نوع انتقال تنها می‌تواند با ایجاد یک رخ‌نمای جدید تغییر کند.

این آرگومان تنها شامل مقادیر پارامتری که لازم است تغییر کند، است.

حذف پارامترهای خاص می‌تواند با حذف و ایجاد مجدد یک رخ‌نمای کامل به‌دست آید.

۳-۶-۶-۲ وابستگی به حالت

رخ‌نمای نشان داده شده توسط *ProfileID* باید وجود داشته باشد.

۳-۶-۶-۳ تاثیر روی حالت

به روز رسانی رخ‌نما ممکن است بالقوه منجر به اصلاحات متغیر حالت *SystemInfo* (به عنوان مثال، اگر credentialID اصلاح شود) شود. از آنجا که متغیر حالت *SystemInfo* با خدمات RADASync و RADAConfig به اشتراک گذاشته می‌شود، پیاده‌سازی باید اصلاح مقدار آن را به صورت داخلی به آن خدمات، در صورت وجود در همان افزاره، پخش کند.

۳-۶-۶-۴ الزامات نقاط واپایش

وجود ندارد.

۳-۶-۶-۵ خطاها

جدول ۱۵- کدهای خطا برای اقدام *EditProfile()*

کد خطا	شرح خطا	شرح
۴۰۰-۴۹۹	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.
۵۰۰-۵۹۹	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.
۶۰۰-۶۹۹	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.
۷۰۱	داده رخنمای نامعتبر	داده رخنمای ارائه شده معتبر نیست.
۷۰۲	ID رخنمای نامعتبر	رخنمای شناسایی شده توسط profileID وجود ندارد.

۳-۶-۷ اقدام *DeleteProfile()*

این اقدام سازوکاری برای حذف رخنماها از یک RATA تعریف می‌کند.

۳-۶-۷-۱ آرگومان‌ها

جدول ۱۶- آرگومان‌های اقدام *DeleteProfile()*

آرگومان	جهت	متغیر حالت وابسته
ProfileID	ورودی	*A_ARG_TYPE_ProfileID*

۳-۶-۷-۱-۱ آرگومان *ProfileID*

این آرگومان ID رخنمای حذف شده را نشان می‌دهد.

۳-۶-۷-۲ وابستگی به حالت

رخنمای نشان داده شده توسط *ProfileID* باید وجود داشته باشد.

۳-۶-۷-۳ تاثیر روی حالت

تاثیر آن این است که *ProfileList* باید به روز رسانی شود. به علاوه، افزاره **باید** متغیر حالت *SystemInfo* را به‌روزرسانی کند.

یادآوری- از آنجا که متغیر حالت *SystemInfo* با خدمات RADASync و RADAConfig به اشتراک گذاشته می‌شود، پیاده‌سازی باید اصلاح مقدار آن را به صورت داخلی به آن خدمات، در صورت وجود در همان افزاره، پخش کند.

۳-۶-۷-۴ الزامات نقاط واپایش

وجود ندارد.

۳-۶-۷-۵ خطاها

جدول ۱۷- کدهای خطا برای اقدام *DeleteProfile()*

کد خطا	شرح خطا	شرح
۴۰۰-۴۹۹	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.
۵۰۰-۵۹۹	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.

۶۹۹-۶۰۰	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.
۷۰۲	ID رخنمای نامعتبر	رخنمای شناسایی شده توسط profileID وجود ندارد.

۳-۶-۸ اقدام *GetProfileConfigInfo()*

این اقدام سازوکاری برای تعیین گزینه‌ها و پارامترهای یک رخنمای از قبل پیکربندی شده، تعریف می‌کند.

۳-۶-۸-۱ آرگومان‌ها

جدول ۱۸- آرگومان‌های اقدام *GetProfileConfigInfo()*

آرگومان	جهت	متغیر حالت وابسته
ProfileID	ورودی	*A_ARG_TYPE_ProfileID*
ProfileConfigInfo	خروجی	*A_ARG_TYPE_ProfileConfigInfo*

۳-۶-۸-۱-۱ آرگومان *ProfileID*

این آرگومان ID رخنمایی که تاریخ رخنمای آن فرا خوانده شده، را نشان می‌دهد.

۳-۶-۸-۱-۲ آرگومان *ProfileConfigInfo*

این آرگومان شامل گزینه‌های پیکربندی پروتکل و اعتبارنامه‌های مربوطه برای یک رخنمای RAT مرتبط با *ProfileID* است.

۳-۶-۸-۲ وابستگی به حالت

رخنمای نشان داده شده توسط *ProfileID*، باید موجود باشد.

۳-۶-۸-۳ تاثیر روی حالت

وجود ندارد.

۳-۶-۸-۴ الزامات نقاط واپایش

وجود ندارد.

۳-۶-۸-۵ خطاها

جدول۱۹- کدهای خطا برای اقدام *GetProfileConfigInfo()*

کد خطا	شرح خطا	شرح
۴۹۹-۴۰۰	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.
۵۹۹-۵۰۰	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.
۶۹۹-۶۰۰	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.
۷۰۲	ID رخنمای نامعتبر	رخنمای شناسایی شده توسط profileID وجود ندارد.

۳-۶-۹ خلاصه کد خطا

جدول زیر کدهای خطای مشترک اقدامات را برای این نوع خدمت فهرست می‌کند. اگر اقدامی منجر به چندین خطا شود، بهتر است، مشخص‌ترین خطا برگشت داده شود.

جدول ۲۰- خلاصه کد خطا

کد خطا	شرح خطا	شرح
۴۰۰-۴۹۹	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.
۵۰۰-۵۹۹	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.
۶۰۰-۶۹۹	TBD	به بند معماری افزاره UpnP در واپایش مراجعه شود.
۷۰۰		برای گسترش‌های آینده ذخیره شده است.
۷۰۱	داده رخنمای نامعتبر	داده رخنمای ارائه شده معتبر نیست.
۷۰۲	ID رخنمای نامعتبر	رخنمای شناسایی شده توسط profileID وجود ندارد.

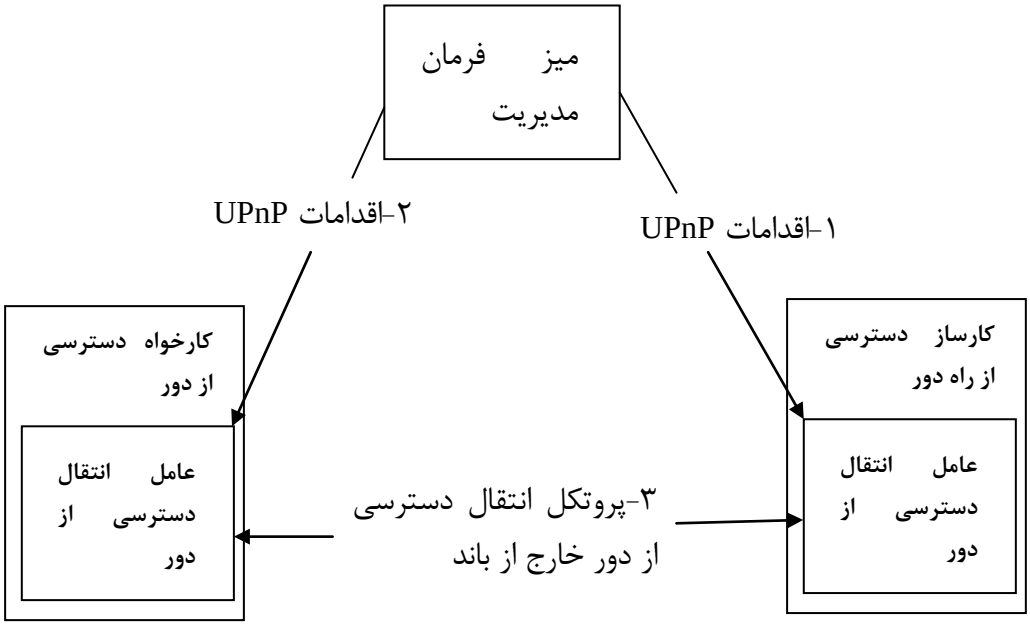
یادآوری- کدهای خطای ۸۰۰-۸۹۹ برای اقدامات استاندارد مجاز نیست. برای مشاهده جزئیات بیشتر به بند معماری افزاره UPnP در واپایش مراجعه شود.

۳-۷ نظریه عملیات

۳-۷-۱ مدل برهمکنش

اتصالات انتقال دسترسی از دور تنها در صورتی می‌تواند برقرار شود که *RAServer* [RAServer] دارای یک رخنمای پیکربندی شده برای پذیرش اتصالات و *RAClient* [RAClient] دارای رخنمای تطبیقی پیکربندی شده برای راه‌اندازی اتصال به کارساز خاص باشد. یک رخنمای کارساز مجاز است که دارای چندین رخنمای کارخواه متناظر باشد.

میز فرمان مدیریت ممکن است هم کارساز و هم کارخواه را در یک زمان پیکربندی کند اما ممکن است هم، پیکربندی را در دو مرحله انجام دهد: اول کارساز و سپس کارخواه. این انعطاف‌پذیری، میز فرمان مدیریت را قادر می‌سازد که یک کارخواه را حتی اگر در شبکه/موقعیت یکسان با کارساز قرار ندارد، پیکربندی کند. در این موارد، میز فرمان مدیریت باید اطلاعات رخنمای کارساز را در حافظه نهان ذخیره کند.



شکل۱- مدل برهمکنش

۳-۷-۲ شناسایی نقش RATA

خدمت RATAConfig می‌تواند در افزاره *RAServer* [RAServer] یا افزاره *RAClient* [RAClient] تعبیه شود. بر اساس این اطلاعات، نقطه واپایش می‌تواند تشخیص دهد که آیا RATA در حالت کارساز کار می‌کند یا کارخواه، بنابراین آن می‌تواند در حین تنظیم رخنماهای RAT، گزینه‌های پیکربندی مناسب را تحویل دهد.

۳-۷-۳ ایجاد پیکربندی رخنمای انتقال دسترسی از دور (کارساز)

قبل از شروع پیکربندی رخنماهای انتقال دسترسی از دور، نقطه واپایش باید نقش عملیاتی ایفا شده توسط RATA برای مثال کارخواه یا کارساز را تعیین کند. رویه دقیق در بند ۳-۷-۲ شرح داده شده است.

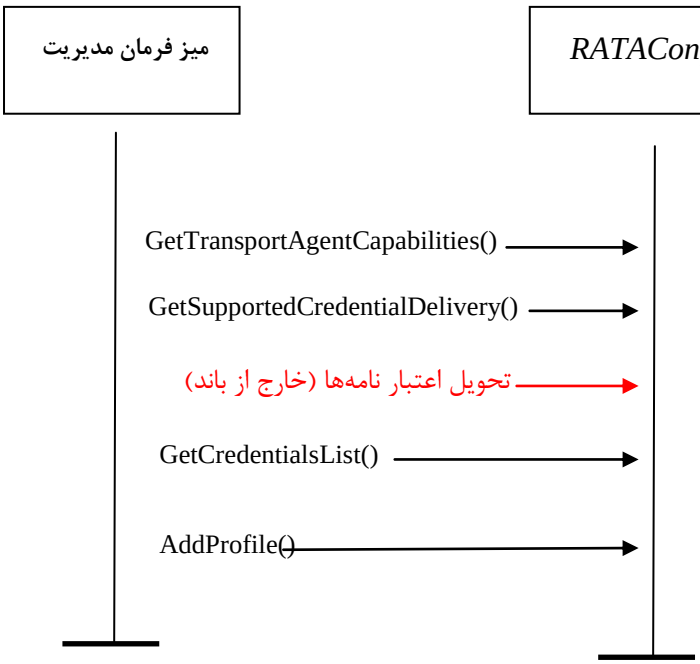
میز فرمان مدیریت رویه پیکربندی را با اولین پرسش از خدمت *RATAConfig* به منظور تشخیص اینکه کدام پروتکل‌های انتقال پشتیبانی می‌شوند (به عنوان مثال، *GetTransportAgentCapabilities()*) و چه سازوکارهایی برای تحویل اعتبارنامه‌ها موجود هستند (به عنوان مثال، *GetSupportedCredentialDelivery()*)، شروع خواهد کرد. با تبعیت از این درخواست، میز فرمان مدیریت و *RATAConfig* تحویل اعتبارنامه متداولی را به اشتراک می‌گذارند، کاربر تحویل را با استفاده از رویه‌های خاص سازوکار خارج از باند راه اندازی می‌کند.

هنگامی‌که فرآیند تحویل به طور موفقیت آمیز کامل می‌شود، میز فرمان مدیریت دوباره از خدمت *RATAConfig* پرسش خواهد کرد تا بفهمد که کدام اعتبارنامه‌ها روی افزاره موجود هستند (به عنوان مثال،

GetCredentialsList()). میز فرمان مدیریت، اعتبار نامه تحویل شده را از فهرست بازیابی انتخاب می‌کند و اشاره‌گر را به آن یادآوری می‌کند.

سپس، میز فرمان مدیریت، گزینه‌های پروتکل انتقال موردنظر برای این اتصال خاص را انتخاب خواهد کرد، که شامل اشاره‌گر به اعتبارنامه‌های انتخابی خواهد بود و تنظیمات رخنما (به عنوان مثال، *AddProfile()*) را به *RATAConfig* تحویل خواهد داد.

در این مرحله کارساز آماده پذیرش اتصال‌های ورودی است.



شکل ۲-پیکربندی رخنماهای انتقال دسترسی از دور

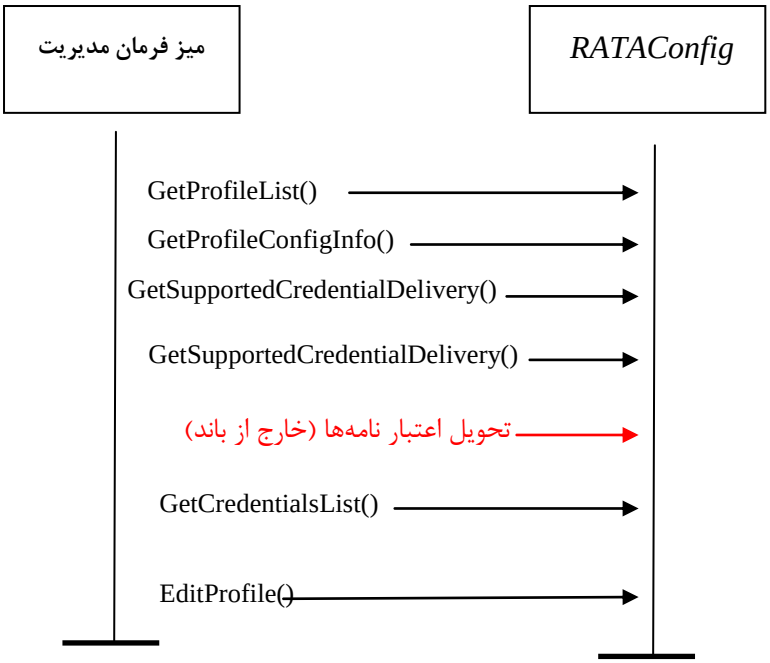
۳-۷-۴ پیکربندی رخنمای دسترسی از دور(کارخواه)

رویه پیکربندی رخنمای دسترسی از دور روی کارخواه، از همان الگوهای مبادله پیغام مشابه برای کارساز تبعیت می‌کند (به بند ۳-۷-۳ مراجعه شود).

یک مرحله دیگر به صورت داخلی توسط میز فرمان مدیریت انجام می‌شود، که باید بررسی کند که پروتکل‌های مورد پشتیبانی گزارش شده توسط کارخواه، با همان‌های کارساز تطبیق دارد یا نه. در مورد تطابق‌های چندگانه، میز فرمان مدیریت، مطابق خط مش‌های از پیش پیکربندی شده، یکی را انتخاب خواهد کرد یا از کاربر خواهد خواست که یکی را انتخاب کند.

۳-۷-۵ ویرایش یک رخنما

قبل از شروع ویرایش رخنماهای انتقال دسترسی از دور، نقطه واپایش باید نقش عملیاتی ایفاشده توسط RATA، به عنوان مثال، کارخواه یا کارساز را تعیین کند. رویه دقیق در بند ۳-۷-۲ شرح داده شده است.



شکل ۳-ویرایش رخ‌نماهای انتقال دسترسی از دور

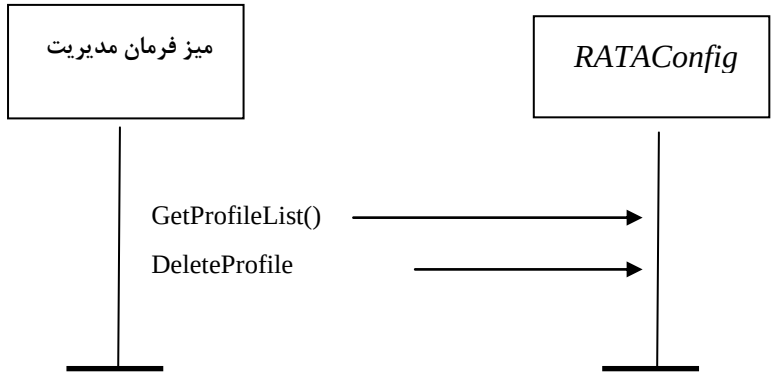
میز فرمان مدیریت، فرآیند ویرایش را با اولین پرسش از خدمت *RATAConfig* به منظور بدست آوردن فهرست رخ‌نماها (به عنوان مثال، *GetProfileList()*) که روی RATA پیکربندی می‌شود، شروع خواهد کرد. به محض اینکه رخ‌نما شناسایی می‌شود، میز فرمان مدیریت جزئیات پیکربندی (به عنوان مثال، *GetProfileConfigInfo()*) را بدست خواهد آورد.

هرگاه لازم باشد اعتبارنامه‌ها اصلاح شود، میز فرمان مدیریت از RATAConfig پرسش خواهد کرد تا بفهمد که کدام اعتبارنامه‌ها روی افزاره موجود است (به عنوان مثال، *GetCredentilasList()*). به صورت اختیاری، میز فرمان مدیریت، اعتبارنامه‌های دیگری را تحویل خواهد داد (به عنوان مثال، *GetSupportedCredentialDelivery()*، تحویل اعتبارنامه خارج از باند و *GetCredentialsList()*).

هنگامی‌که تمام تغییرات قطعی شد، میز فرمان مدیریت می‌تواند تنظیمات جدید را به افزاره تحویل دهد.

۳-۷-۶ حذف رخ نما

میز فرمان مدیریت، فرآیند حذف را با اولین پرسش از خدمت *RATAConfig* به منظور بدست آوردن فهرست رخ‌نماها (به عنوان مثال، *GetProfileList()*) که روی RATA پیکربندی می‌شود، شروع خواهد کرد. به محض اینکه، رخ‌نما شناسایی می‌شود، میز فرمان مدیریت رخ‌نما را حذف خواهد کرد (به عنوان مثال، *DeleteProfile()*).



شکل۴-حذف رخ‌نماهای انتقال دسترسی از دور

۴ شرح خدمت XML

```
<?xml version="1.0"?>
<scpd xmlns="urn:schemas-upnp-org:service-1-0">
<specVersion>
<major>1</major>
<minor>0</minor>
</specVersion>
<actionList>
<action>
<name>GetTransportAgentCapabilities</name>
<argumentList>
<argument>
<name>TransportAgentCapabilities</name>
<direction>out</direction>
<relatedStateVariable>
TransportAgentCapabilities
</relatedStateVariable>
</argument>
</argumentList>
</action>
<action>
<name>GetSupportedCredentialDelivery</name>
<argumentList>
<argument>
<name>SupportedCredentialDelivery</name>
<direction>out</direction>
<relatedStateVariable>
CredentialDelivery
</relatedStateVariable>
</argument>
</argumentList>
</action>
```

<action>
<name>GetCredentialsList</name>
<argumentList>
<argument>
<name>CurrentCredentialsList</name>
<direction>out</direction>
<retval/>
<relatedStateVariable>
CredentialsList
</relatedStateVariable>
</argument>
</argumentList>
</action>
<action>
<name>GetProfileList</name>
<argumentList>
<argument>
<name>ProfileList</name>
<direction>out</direction>
<retval/>
<relatedStateVariable>
ProfileList
</relatedStateVariable>
</argument>
</argumentList>
</action>
<action>
<name>AddProfile</name>
<argumentList>
<argument>
<name>newProfileConfigInfo</name>
<direction>in</direction>
<relatedStateVariable>
A_ARG_TYPE_ProfileConfigInfo
</relatedStateVariable>
</argument>
</argumentList>
</action>
<action>
<name>EditProfile</name>
<argumentList>
<argument>
<name>ProfileID</name>
<direction>in</direction>
<relatedStateVariable>
A_ARG_TYPE_ProfileID
</relatedStateVariable>
</argument>
<argument>

<name>*UpdatedProfileConfigInfo*</name>
<direction>in</direction>
<relatedStateVariable>
A_ARG_TYPE_ProfileConfigInfo
</relatedStateVariable>
</argument>
</argumentList>
</action>
<action>
<name>*DeleteProfile*</name>
<argumentList>
<argument>
<name>*ProfileID*</name>
<direction>in</direction>
<relatedStateVariable>
A_ARG_TYPE_ProfileID
</relatedStateVariable>
</argument>
</argumentList>
</action>
<action>
<name>*GetProfileConfigInfo*</name>
<argumentList>
<argument>
<name>*ProfileID*</name>
<direction>in</direction>
<relatedStateVariable>
A_ARG_TYPE_ProfileID
</relatedStateVariable>
</argument>
<argument>
<name>*ProfileConfigInfo*</name>
<direction>out</direction>
<relatedStateVariable>
A_ARG_TYPE_ProfileConfigInfo
</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="no">
<name>*TransportAgentCapabilities*</name>

```
<dataType>string</dataType>
</stateVariable>
<stateVariable sendEvents="no">
<name>CredentialDelivery</name>
<dataType>string</dataType>
</stateVariable>
<stateVariable sendEvents="yes">
<name>CredentialsList</name>
<dataType>string</dataType>
</stateVariable>
<stateVariable sendEvents="no">
<name>ProfileList</name>
<dataType>string</dataType>
</stateVariable>
<stateVariable sendEvents="no">
<name>A_ARG_TYPE_ProfileConfigInfo</name>
<dataType>string</dataType>
</stateVariable>
<stateVariable sendEvents="no">
<name>A_ARG_TYPE_ProfileID</name>
<dataType>ui4</dataType>
</stateVariable>
<!-- Declarations for other state variables defined by UPnP vendor
(if any)go here. -->
</serviceStateTable>
</scpd>
```

۵ آزمون

هیچ آزمون معناداری برای این خدمت مشخص نشده است.

پیوست الف

(الزامی)

ساختارهای داده RATransportAgent

الف-۱ الگوی ProfileList

شرح زیر چیدمان کلی از یک الگوی ProfileList را نشان می‌دهد. **مجاز است** که به نگارش‌های آتی الگوهای ProfileList عناصر و/یا مشخصه‌های بیشتری اضافه شود.

از سبک نویسه‌های کلمه *forum* برای نمایش اسامی تعریف شده توسط کمیته کاری دسترسی از راه دور (RAWC)[1] استفاده می‌شود. پیاده‌سازی‌ها نیازمند پرکردن قسمت‌هایی هستند که به سبک نویسه‌های کلمه *vendor* چاپ می‌شوند.

```
<?xml version="1.0" encoding="UTF-8"?>
<tads xmlns="urn:schemas-upnp-org:ra:tads"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:schemas-upnp-org:ra:tads
http://www.upnp.org/schemas/ra/tads-v1.xsd">
<profileList dataStructureType="client">
<profileInfo
id="profile unique id"
transportAgentName="transport agent name">
friendly description
</profileInfo>
<!-- Other profiles (if any) go here. -->
</profileList>
</tads>
```

xml

اجباری. برای تمام اسناد xlm. حساس به حروف کوچک.

tads

اجباری. باید "urn:schemas-upnp-org:ra:tads" را به عنوان مقداری برای ویژگی‌های xmlns داشته باشد؛ این به طرح الگوی ساختار داده RADA کمیته کاری دسترسی از دور UpnP ارجاع می‌دهد. تا زمانی که از xmlns یکسان استفاده می‌شود، الگوی ساختار داده **باید** سازگار با قبل باشد، یعنی توسط پیاده‌سازی‌های موروثی قابل استفاده باشد.

profileList

اجباری. مجموعه‌ای از رخ‌نماهای پیکربندی شده، را برمی‌شمارد. **باید** برای هر رخ‌نمای پیکربندی شده روی RATA، عنصر رخ‌نما وجود داشته باشد.

@dataStructureType

اجباری. XS: نشانه[2]. نوع ساختار داده شناسایی می‌شود. مقدار نشانه **باید** کارخواه یا کارساز باشد.

---

1 - Remote Access Working Committee
2- token

profileInfo

اختیاری. XS:رشته. دارای یک نام متناسب با رخنما است. باید شامل ویژگی‌های زیر باشد:

@id

اجباری. XS:صحیح. ID رخنمای منحصر به فرد.

@transportAgentName

اجباری. XS:رشته. شامل نام شناسایی سازوکار انتقال دسترسی از دور است. مقادیر ممکن برابر است با:

“OpenVPN”
“IPSec”

عرضه‌کنندگان ممکن است مقادیر دیگری را تعریف کنند.

الف-۲ الگوی ProfileConfig

شرح زیر چیدمان کلی از یک الگوی ProfileConfig را نشان می‌دهد. **مجاز است** که به نگارش‌های آتی الگوهای ProfileConfig عناصر و/یا ویژگی‌های بیشتری اضافه شود.

از سبک نویسه‌های کلمه *forum* برای نمایش اسامی تعریف شده توسط کمیته کاری دسترسی از دور (RAWC) استفاده می‌شود. پیاده‌سازی‌ها نیازمند پرکردن قسمت‌هایی هستند که به سبک نویسه‌های کلمه *vendor* چاپ می‌شوند.

```
<?xml version="1.0" encoding="UTF-8"?>
<tads
xmlns="urn:schemas-upnp-org:ra:tads"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:schemas-upnp-org:ra:tads
http://www.upnp.org/schemas/ra/tads-v1.xsd">
<profileConfig dataStructureType="client">
<profileInfo
id=" profile unique id"
transportAgentName="transport agent name">
friendly description
</profileInfo>
<profileData>
<!-- Placeholder for defining data specific for each transport
mechanism. Data structures defined in another namespace -->
</profileData>
</profileConfig>
</tads>
```

xml

اجباری. برای تمام اسناد xlm. حساس به حروف کوچک.

tads

اجباری. باید “urn:schemas-upnp-org:ra:tads” را به عنوان مقداری برای ویژگی‌های xmlns داشته باشد؛ این به طرح الگوی ساختار داده RADA کمیته کاری دسترسی از دور UpnP ارجاع می‌دهد. تا زمانی که از xmlns یکسان استفاده می‌شود، الگوی ساختار داده **باید** سازگار با قبل باشد، یعنی توسط پیاده‌سازی‌های موروثی قابل استفاده باشد.

profileList

اجباری. مجموعه‌ای از رخ‌نماهای پیکربندی شده، را برمی‌شمارد. **باید** برای هر رخ‌نمای پیکربندی شده روی RATA، یک عنصر رخ‌نما وجود داشته باشد.

@dataStructureType

اجباری. XS: نشانه. نوع ساختار داده شناسایی می‌شود. مقدار نشانه باید کارخواه یا کارساز باشد.

profileInfo

اختیاری. XS:رشته. دارای یک نام متناسب با رخ‌نما است. باید شامل ویژگی‌های زیر باشد:

@id

اجباری. XS:صحیح. ID رخ‌نمای منحصر به فرد.

@transportAgentName

اجباری. XS:رشته. شامل نام شناسایی سازوکار انتقال دسترسی از دور است. مقادیر ممکن برابر است با:

“OpenVPN”
“IPSec”

عرضه‌کنندگان ممکن است مقادیر دیگری را تعریف کنند.

profileData

اجباری. XS: هر نوع. شامل گزینه‌ها و پارامترهای پیکربندی موردنیاز برای رخ‌نمای دسترسی از دور مربوطه است. محتوا برای هر نوع عامل انتقال مشخص است و در طرحی خاص نوع عامل انتقال مورد استفاده تعریف می‌شود. برای مشاهده یک طرح نمونه تعریف شده برای IPSec به پ-۱-۲ مراجعه شود.

الف-۳ الگوی TransportAgentCapabilities

شرح زیر چیدمان کلی از یک الگوی TransportAgentCapabilities را نشان می‌دهد. **مجاز است** که به نگارش‌های آتی الگوهای TransportAgentCapabilities عناصر و/یا ویژگی‌های بیشتری اضافه شود.

از سبک نویسه‌های کلمه *forum* برای نمایش اسامی تعریف‌شده توسط RAWC استفاده می‌شود. پیاده‌سازی‌ها نیازمند پرکردن قسمت‌هایی هستند که به سبک نویسه‌های کلمه *vendor* چاپ می‌شوند.

```
<?xml version="1.0" encoding="UTF-8"?>
<tads
xmlns="urn:schemas-upnp-org:ra:tads"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:schemas-upnp-org:ra:tads
http://www.upnp.org/schemas/ra/tads-v1.xsd">
<transportAgentCapability
transportAgentName="IPsec">
<transportAgentOptions>
<!-- Placeholder for defining data specific for each transport
mechanism. Data structures defined in another namespace -->
</transportAgentOptions>
<!-- Other transport agent options (if any) go here. -->
</transportAgentCapability>
<!-- Other transport agent capabilities (if any) go here. -->
</tads>
xml
```

اجباری. برای تمام اسناد xlm. حساس به حروف کوچک.

tads

اجباری. باید "urn:schemas-upnp-org:ra:tads" را به عنوان مقداری برای ویژگی‌های xmlns داشته باشد؛ این به طرح الگوی ساختار داده RADA کمیته کاری دسترسی از دور UpnP ارجاع می‌دهد. تا زمانی که از xmlns یکسان استفاده می‌شود، الگوی ساختار داده باید سازگار با قبل باشد، یعنی توسط پیاده‌سازی‌های موروثی قابل استفاده باشد.

transportAgentCapability

اجباری. شامل گزینه‌های موجود برای یک عامل انتقال خاص است. **باید** برای هر عامل انتقال پیکربندی شده روی RATA، یک عنصر transportAgentCapability وجود داشته باشد. باید شامل زیر عنصر زیر باشد:

@transportAgentName

اجباری. XS:رشته. عامل انتقال را شناسایی می‌کند. مقادیر ممکن برابر است با:

"OpenVPN"
"IPSec"

عرضه‌کنندگان ممکن است مقادیر دیگری را تعریف کنند.

transportAgentOptions

اجباری. XS:هر نوع. شامل گزینه‌های پشتیبانی شده توسط عامل انتقال شناسایی شده توسط @transportAgentName است. به طور نوعی، این ساختار داده می‌تواند به عنوان یک الگو برای پیکربندی رخ‌نما درنظر گرفته شود. **مجاز است** که برای یک عامل انتقال خاص چندین عنصر transportAgentOptions وجود داشته باشد، هرکدام یک مجموعه متفاوت از گزینه‌ها را تعریف می‌کند. برای مشاهده یک مثال از طرح تعریف شده برای IPSec به پ-۱-۱ مراجعه شود.

الف-۴ الگوی CredentialDelivery

شرح زیر چیدمان کلی از یک الگوی CredentialDelivery را نشان می‌دهد. **مجاز است** که به نگارش‌های آتی الگوهای CredentialDelivery عناصر و/یا ویژگی‌های بیشتری اضافه شود.

از سبک نویسه‌های کلمه *forum* برای نمایش اسامی تعریف شده توسط RAWC استفاده می‌شود. پیاده‌سازی‌ها نیازمند پرکردن قسمت‌هایی هستند که به سبک نویسه‌های کلمه *vendor* چاپ می‌شوند.

```
<?xml version="1.0" encoding="UTF-8"?>
<tads xmlns="urn:schemas-upnp-org:ra:tads"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:schemas-upnp-org:ra:tads
http://www.upnp.org/schemas/ra/tads-v1.xsd">
<credentialDelivery credentialDeliveryMechanism="mechanism name">
<credentialType credentialEncoding="RSA Raw Key">
RSA
</credentialType>
<!-- Other credential types (if any) go here. -->
</credentialDelivery>
<!-- Other credential delivery (if any) go here. -->
</tads>
```

xml

اجباری. برای تمام اسناد xlm. حساس به حروف کوچک.

tads

اجباری. باید "urn:schemas-upnp-org:ra:tads" را به عنوان مقداری برای ویژگی‌های xmlns داشته باشد؛ این به طرح الگوی ساختار داده RADA کمیته کاری دسترسی از دور UpnP ارجاع می‌دهد. تا زمانی که از xmlns یکسان استفاده می‌شود، الگوی ساختار داده باید سازگار با قبل باشد، یعنی توسط پیاده‌سازی‌های موروثی قابل استفاده باشد.

credentialDelivery

اجباری. شامل گزینه‌های موجود برای یک سازوکار تحویل اعتبارنامه است. **باید** برای هر سازوکار تحویل اعتبارنامه پشتیبانی شده توسط RATA، یک عنصر credentialDelivery وجود داشته باشد. باید شامل زیر عناصر زیر باشد:

@credentialDeliveryMechanism

اجباری. XS: رشته. سازوکار تحویل اعتبارنامه را شناسایی می‌کند. مقادیر ممکن برابر است با:

ارتباط حوزه نزدیک	Near-field communication	*"NFC"*
پروتکل انتقال فایل	File Transfer Protocol	*"FTP"*
پروتکل انتقال فوق متن	Hyper-text Transfer Protocol	*"HTTP"*

عرضه‌کنندگان ممکن است مقادیر دیگری را تعریف کنند.

credentialType

اجباری. XS:رشته. نوع اعتبارنامه که ممکن است توسط سازوکار تحویل اعتبارنامه تحویل داده شود را شناسایی می‌کند. **باید** برای هر نوع اعتبارنامه که می‌تواند تحویل داده شود، یک عنصر credentialType وجود داشته باشد. باید شامل ویژگی زیر باشد:

@credentialEncoding

اجباری. XS: رشته. کدبندی نوع گواهی خاص را شناسایی می‌کند.

الف-۵ الگوی CredentialsList

شرح زیر چیدمان کلی از یک الگوی CredentialsList را نشان می‌دهد. **مجاز است** که به نگارش‌های آتی الگوهای CredentialsList عناصر و/یا ویژگی‌های بیشتری اضافه شود.

از سبک نویسه‌های کلمه *forum* برای نمایش اسامی تعریف شده توسط RAWC استفاده می‌شود. پیاده‌سازی‌ها نیازمند پرکردن قسمت‌هایی هستند که به سبک نویسه‌های کلمه *vendor* چاپ می‌شوند.

```
<?xml version="1.0" encoding="UTF-8"?>
<tads xmlns="urn:schemas-upnp-org:ra:tads"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:schemas-upnp-org:ra:tads
http://www.upnp.org/schemas/ra/tads-v1.xsd">
<credentialsList>
<credential scope="local">
<credentialID>ID</credentialID>
```

<credentialFriendlyName>friendly name</credentialFriendlyName>
<credentialType credentialEncoding="RSA Raw Key">RSA</credentialType>
</credential>
<!-- Other credential (if any) go here. -->
</credentialsList>
</tads>
xml

اجباری. برای تمام اسناد xlm. حساس به حروف کوچک.

tads

اجباری. باید "urn:schemas-upnp-org:ra:tads" را به عنوان مقداری برای ویژگی‌های xmlns داشته باشد؛ این به طرح الگوی ساختار داده RADA کمیته کاری دسترسی از دور UpnP ارجاع می‌دهد. تا زمانی که از xmlns یکسان استفاده می‌شود، الگوی ساختار داده باید سازگار با قبل باشد، یعنی توسط پیاده‌سازی‌های موروثی قابل استفاده باشد.

credentialsList

اجباری. شامل اعتبارنامه‌های موجود روی RATA است. باید شامل زیر عناصر زیر باشد:

Credential

اجباری. شامل اطلاعات اعتبارنامه است. **باید** برای هر اعتبارنامه موجود روی RATA، یک عنصر credential وجود داشته باشد. باید شامل زیر عناصر زیر باشد:

@scope

اجباری. XS:نشانه. نشان می‌دهد که آیا اعتبارنامه با RADA محلی یا راه دور مرتبط است.

credentialed

اجباری. XS:رشته. به صورت منحصر به فردی، اعتبارنامه روی RATA را شناسایی می‌کند.

credentialFriendlyName

اجباری. XS:رشته. نام دوستانه اعتبارنامه. برای شناساندن اعتبارنامه به کاربر استفاده می‌شود.

credentialType

اجباری. XS:رشته. نوع اعتبارنامه را تعیین می‌کند. باید شامل ویژگی زیر باشد:

@credentialEncoding

اجباری. XS:رشته. کدبندی نوع گواهی خاص را شناسایی می‌کند.

الف-۶ طرح ساختار داده TransportAgent

xsi:schemaLocation="
urn:schemas-upnp-org:ra:tads
http://www.upnp.org/schemas/ra/tads-v1.xsd"

در اینجا شماره یک بعد از حرف "V" شماره نگارش است. هر به روز رسانی نگارش طرح TADS، باید با نگارش قبلی سازگار پس‌سو[1] باشد. بویژه، ممکن است عناصر و/یا ویژگی‌های XML ، به آخرین نگارش‌های طرح TADS اضافه شود، اما هرگز نباید حذف شود. در نتیجه، هنگام آزمایش مقدار نگارش طرح،

1- **B**ackward

پیاده‌سازی‌ها به احتمال زیاد می‌خواهند به جای یک بررسی برابری ساده، یک مقایسه بزرگتر مساوی انجام دهند.

پیوست ب
(اطلاعاتی)
ملاحظات نشانی‌دهی

ب-۱ ملاحظه IP4

ب-۱-۱ تخصیص نشانی IP4

به منظور توانایی برهمکنش با افزاره‌های راه دور، اول، باید افزاره‌های UPnP خانگی به طور صحیح برای دسترسی به اینترنت پیکربندی شوند؛ در عمل به این معنا است که افزاره‌های UPnP خانگی باید یک نشانی IP را از کارساز DHCP دریافت کنند.

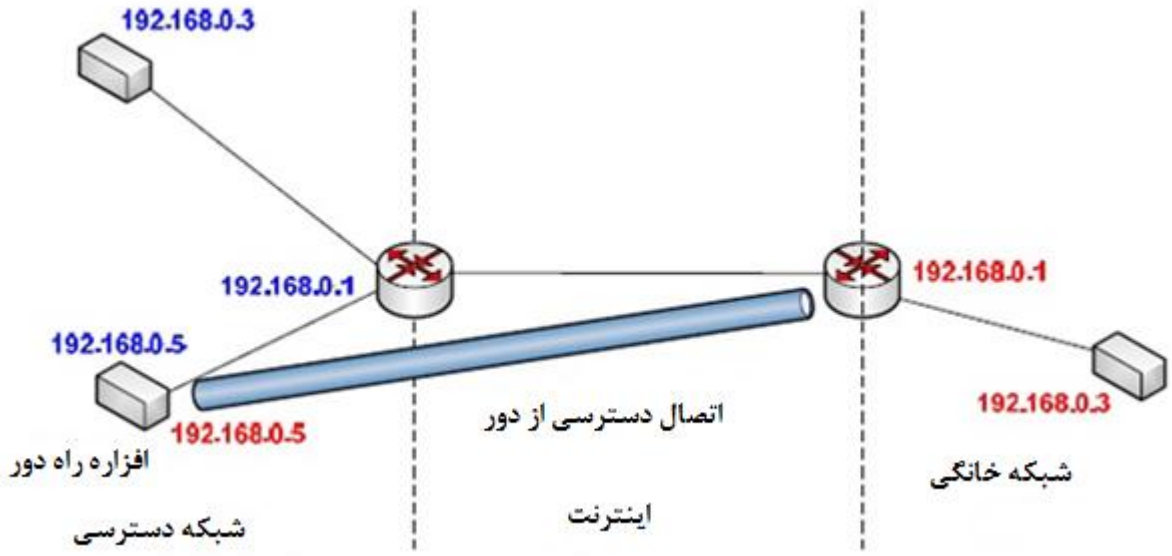
ب-۱-۲ تلاقی‌های فضای نشانی

انتظار می‌رود که افزاره UPnP راه دور بتواند از سایر شبکه‌های خانگی به عنوان شبکه‌های دسترسی استفاده کند، به عنوان مثال، هنگام بازدید از خانه یک دوست. در چنین محیط‌هایی، احتمال زیادی وجود دارد که دروازه مقیم[۱] شبکه دسترسی به گونه‌ای پیکربندی شوند که نشانی‌های IP در فضای نشانی یکسان با دروازه مقیم موجود در شبکه خانگی را اختصاص دهد. مشکل تلاقی فضای نشانی با ممارست ISP برای پیکربندی تمام دروازه‌های مقیم با تنظیمات یکسانی برای واسط LAN تسهیل می‌شود. همچنین، در این موارد هنگامی که دروازه مقیم توسط ISP فراهم نشده است و از یک خرده فروشی خریداری می‌شود، مصرف کننده‌ها آنها را به طور مستقیم با تنظیمات تولیدکننده استفاده خواهند کرد که این تنظیمات نوعا برای تمام افزاره‌ها از یک تولیدکننده خاص یکسان است. این تقریبا دسترسی از دور را هنگامی‌که هردوی شبکه خانگی و شبکه دسترسی از طریق ISP یکسان به اینترنت وصل می‌شوند، یا هنگامی‌که هر دو شبکه دارای یک دروازه مقیم از تولیدکننده یکسان هستند و با تنظیمات پیش فرض استفاده شده‌اند، را غیر ممکن می‌کند.

تلاقی فضای نشانی موجب مشکلات اساسی در مسیریابی می‌شود که مانع رسیدن بستک‌های شروع شده در افزاره راه دور به افزاره‌های موجود در شبکه خانگی خود، خواهد شد، مگر اینکه افزاره راه دور، یک افزاره مالتی هوم هوشمند[۲] باشد.

1- Residential gateway

۲ - multi-home aware: کامپیوتر یا افزاره‌ای که به بیش از یک شبکه کامپیوتری وصل است.



شکل ب-۱-مشکل تلاقی فضای نشانی

به منظور کاهش احتمال تلاقی فضای نشانی، صاحب خانه می‌تواند شبکه خانگی را - در طول یک رویه راه‌اندازی که یکبار اجرا می‌شود- به منظور استفاده از یک فضای نشانی تصادفی دوباره پیکربندی کند.
برای خودکار کردن رویه، توصیه می‌شود که از خدمت LANHostConfigManagement موجود روی IGDv1 [IGD] سازگار با دروازه‌های مقیم استفاده شود.
باید توجه شود که این رویه، امکان تلاقی‌های فضای نشانی را کاملا رفع نمی‌کند، اما به این سمت سوق خواهد داد که، در عمل، خیلی بعید خواهد بود که شبکه دسترسی و شبکه خانگی، فضای نشانی یکسانی را به اشتراک گذارند. انتقال به IPv6، مشکل تلاقی فضای نشانی را برطرف خواهد کرد.

پیوست پ

(اطلاعاتی)

استفاده از IPsec به عنوان انتقال دسترسی از دور

هدف این پیوست شرح چگونگی استفاده از یک زیرمجموعه از دنباله پروتکل IPsec، به عنوان سازوکار انتقال دسترسی از دور در دسترسی از دور UPnP است.

این پیوست ممکن است به عنوان مدلی برای تعریف سازوکار دیگر انتقال دسترسی از دور به کار رود.

پ-۱ الگوهای IPsec

پ-۱-۱ الگوی گزینه‌های IPsec

الگوی گزینه‌های IPsec جاری، به عنوان الگویی برای پیکربندی رخنماهای IPsec دسترسی از دور درنظر گرفته شده است. هر گزینه IPsec شامل مجموعه‌ای از الگوریتم‌ها و پروتکل‌های رمزنگاشتی مرتبط با یک روش اصالت‌سنجی تکی است. اگر IPsec، از روش‌های اصالت‌سنجی چندگانه پشتیبانی کند، **باید** برای هر روش اصالت‌سنجی پشتیبانی شده یک گزینه IPsec، به عنوان مثال، امضاهای رقمی RSA، مورد مخفی مشترک[1]، EAP تعریف شود.

```
<?xml version="1.0" encoding="UTF-8"?>
<ipsecOPT xmlns="urn:schemas-upnp-org:ra:tacfg:ipsec"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:schemas-upnp-org:ra:tacfg:ipsec
http://www.upnp.org/schemas/ra/tacfg-ipsec-v1.xsd"
authenticationMethod="RSA Digital Signature"
credentialEncoding="PKCS #7 wrapped X.509 certificate"
keyExchangeProtocol="IKEv2">
<encryptionAlgorithm>AES_CBC</encryptionAlgorithm>
<authenticationAlgorithm>HMAC_SHA1_96</authenticationAlgorithm>
<integrityAlgorithm>AES_XCBC_96</integrityAlgorithm>
<pseudoRandomFunction>AES128_XCBC</pseudoRandomFunction>
</ipsecOPT>
```

xml

اجباری برای تمام اسناد xlm. حساس به حروف کوچک.

ipsecOPT

اجباری. باید "urn:schemas-upnp-org:ra:tacfg:ipsec" را به عنوان مقداری برای ویژگی‌های xmlns داشته باشد؛ این به طرح الگوی گزینه‌های IPsec RATA کمیته کاری دسترسی از دور UpnP ارجاع می‌دهد. تا زمانی که از xmlns یکسان استفاده می‌شود، الگوی ساختار داده باید سازگار با قبل باشد، یعنی توسط پیاده‌سازی‌های موروثی قابل استفاده باشد. شامل ویژگی‌ها و زیر عناصر زیر است:

@authenticationMethod

اجباری .xs : نشانه[2]. روش اصالت‌سنجی استفاده شده را تعیین می‌کند.

@credentialEncoding

1- shared secret
2- token

اجباری .xs : نشانه. کدبندی مورد استفاده برای اعتبارنامه خاص روش شرح داده شده در authenticationMethod را تعیین می‌کند.

@keyExchangeProtocol

اجباری .xs :نشانه. پروتکل تبادل کلید را برای گزینه IPsec تعیین می‌کند. مقادیر ممکن عبارتند از: "IKEv1" و"IKEv2".

encryptionAlgorithm

اجباری .xs :نشانه. الگوریتم رمز گذاری که باید با این گزینه IPsec استفاده شود را تعیین می‌کند. اگر از چندین الگوریتم رمزگذاری پشتیبانی شود، آنها **باید** در اینجا به ترتیب الویت فهرست شوند.

authenticationAlgorithm

اجباری .xs :نشانه. الگوریتم اصالت‌سنجی که باید با این گزینه IPsec استفاده شود را تعیین می‌کند. اگر از چندین الگوریتم اصالت‌سنجی پشتیبانی شود، آنها **باید** در اینجا به ترتیب الویت فهرست شوند.

integrityAlgorithm

اجباری .xs :نشانه. الگوریتم یکپارچگی که باید با این گزینه IPsec استفاده شود را تعیین می‌کند. اگر از چندین الگوریتم یکپارچگی پشتیبانی شود، آنها **باید** در اینجا به ترتیب الویت فهرست شوند.

pseudoRandomFunction

اجباری .xs :نشانه. تابع شبه تصادفی[1] که باید با این گزینه IPsec استفاده شود را تعیین می‌کند. اگر از چندین تابع شبه تصادفی پشتیبانی شود، آنها **باید** در اینجا به ترتیب الویت فهرست شوند.

پ-۱-۲ الگوی پیکربندی Ipsec

الگوی پیکربندی IPsec رایج که در درجه اول طراحی شده تا با IKEv2 استفاده شود، اما شامل اطلاعات کافی برای این که IKEv1 هم بتواند استفاده شود، است.

```
<?xml version="1.0" encoding="UTF-8"?>
<ipsecCFG xmlns="urn:schemas-upnp-org:ra:tacfg:ipsec"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:schemas-upnp-org:ra:tacfg:ipsec
http://www.upnp.org/schemas/ra/tacfg-ipsec-v1.xsd"
configurationType="client">
<policy>
<perfectForwardSecrecy>true</perfectForwardSecrecy>
<replayWindowLength>10</replayWindowLength>
<remoteIdentity>MyIdentity</remoteIdentity>
<proposal protocol="ESP">
<encryptionAlgorithm keyLength="256">
AES_CBC
</encryptionAlgorithm>
<integrityAlgorithm> </integrityAlgorithm>
<lifetime>
<seconds>28800</seconds>
<kBytes>5000</kBytes>
</lifetime>
```

1- the pseudo random function

```
</proposal>
</policy>
<ike version="IKEv2">
<remoteAddress>X.X.X.X</remoteAddress>
<sendNotification>true</sendNotification>
<idType>ID_DER_ASN1_DN</idType>
<useIPsecExpire>true</useIPsecExpire>
<useReplayDetection>true</useReplayDetection>
<useInternalAddress>true</useInternalAddress>
<dpdHeartbeat>600</dpdHeartbeat>
<natKeepalive>100</natKeepalive>
<rekeyingThreshold>90</rekeyingThreshold>
<proposal protocol="IKE">
<encryptionAlgorithm keyLength="256">
AES_CBC
</encryptionAlgorithm>
<integrityAlgorithm>AES_XCBC_96</integrityAlgorithm>
<pseudoRandomFunction>AES128_XCBC</pseudoRandomFunction>
<groupDescription>MODP_1536</groupDescription>
<groupType>Group_2</groupType>
<lifetime>
<seconds>28800</seconds>
<kBytes>500</kBytes>
</lifetime>
</proposal>
<authenticationMethod>RSA Digital Signature</authenticationMethod>
<credentialID>100</credentialID>
</ike>
</ipsecCFG>
```

xml

اجباری برای تمام اسناد xlm. حساس به حروف کوچک.

ipsecOPT

اجباری. باید "urn:schemas-upnp-org:ra:tacfg:ipsec" را به عنوان مقداری برای ویژگی‌های xmlns داشته باشد؛ این به طرح الگوی گزینه‌های RATA IPsec کمیته کاری دسترسی از دور UpnP ارجاع می‌دهد. تا زمانی که از xmlns یکسان استفاده می‌شود، الگوی ساختار داده باید سازگار با قبل باشد، یعنی توسط پیاده‌سازی‌های موروثی قابل استفاده باشد. شامل ویژگی‌ها و زیر عناصر زیر است:

@configurationType

اجباری .xs :نشانه. نوع پیکربندی را تعیین می‌کند. مقادیر ممکن "client" یا "server" است.

Policy

اجباری. مجموعه‌ای از پارامترهای مورد نیاز برای پیکربندی IPsec Sas را برمی‌شمارد. شامل زیرعناصر زیر است:

perfectForwardSecrecy

اجباری .xs :نشانه. تعیین می‌کند که آیا IKE، یک تبادل Diffie-Hellman جدید را برای بدست آوردن شاه کلید جدید به منظور کلیدگذاری مواد برای هر کلید نشست[1] جدید موردنیاز SAهای IPsec، آغاز می‌کند.

1- session key

replayWindowLength

اجباری .xs : مقدار صحیح مثبت. تعیین می‌کند که آیا خدمت ضد تکرار[1] برای Ipsec SA استفاده می‌شود یا نه. بیشینه مقدار پشتیبانی شده، ۳۲ است.

remoteIdentity

اجباری .xs : رشته. هویت میزبان راه دور را تعیین می‌کند.

Proposal

اجباری. شامل مجموعه‌ای از ویژگی‌هایی است که هنگام شروع مذاکره IPsec SA استفاده می‌شوند. شامل زیرعناصر زیر است:

@protocol

اجباری .xs :نشانه. نوع پیشنهاد را شرح می‌دهد. مقدار مجاز ESP است.

encryptionAlgorithm

اجباری .xs :نشانه. الگوریتم رمزگذاری پیشنهادی را شرح می‌دهد. مقادیر مجاز در IKEv2، [RFC 4306] تعریف شده است. شامل ویژگی زیر است:

@keyLength

اختیاری. xs: صحیح. طول کلید الگوریتم رمزگذاری پیشنهادی را شرح می‌دهد. ممکن است اگر الگوریتم رمزگذاری ذکر شده در encryptionAlgorithm، طول مختلف کلید را اجازه دهد، در هر نمونه‌ای موجود باشد. مقادیر مجاز در IKEv2 تعریف شده است.

integrityAlgorithm

اجباری .xs :نشانه. الگوریتم اصالت‌سنجی پیشنهاد شده مطابق توصیه RFC 2406، را شرح می‌دهد. مقادیر مجاز در IKEv2 تعریف شده است.

lifetime

اجباری . بیشینه طول عمر SAی IKE، را شرح می‌دهد. شامل زیر عناصر زیر است:

seconds

اجباری. xs: صحیح. بیشینه مدت[2] SAی IKE.

kBytes

اجباری. xs: صحیح. بیشینه مقدار داده (برحسب بایت) که SAی IKE نگهداری می‌کند.

ike

اجباری. مجموعه‌ای از پارامترهای مورد نیاز برای پیکربندی IKE را برمی‌شمارد. شامل زیرعناصر زیر است:

@version

اجباری .xs :نشانه. نگارش پروتکل IKE را تعیین می‌کند. مقادیر مجاز IKEv1 یا IKEv2 است.

remoteAddress

اختیاری. xs: رشته. شامل نشانی IP یا FQDN مربوط به RAS است. باید در هر لحظه اگر مقدار configurationType، کارخواه است، موجود باشد.

sendNotification

1- anti replay
2- duration

اجباری. xs: بولی. تعیین می‌کند که آیا IKE پیام اخطار را در صورت بروز خطا ارسال می‌کند. برای راحت‌تر کردن عیب‌یابی، مقدار را TRUE قرار دهید.

idType

اجباری .xs :نشانه. تعیین می‌کند که چگونه RAC خود را به RAS بشناساند. مقادیر مجاز در IKEv2 مشخص شده است.

useIPsecExpire

اجباری. xs: بولی. تعیین می‌کند که چگونه SA های IPsec منقضی می‌شوند:

TRUE ، هنگامی‌که SAی IKE استفاده شده برای انتقال آنها، منقضی یا حذف شده است،

FALSE، مطابق طول عمر آنها،

useReplayDetection

اجباری. xs: بولی. تعیین می‌کند که آیا پاسخ دهنده تشخیص ضد تکرار را اجرا می‌کند:

TRUE ، تشخیص تکرار فعال است،

FALSE، تشخیص تکرار غیرفعال است.

useInternalAddress

اختیاری. xs: بولی. تعیین می‌کند که آیا RAC نیازمند یک نشانیIP از منبع نشانی شبکه خانگی که آن را عملا قسمتی از شبکه خانگی می‌سازد، است. مقدار پیش فرض TRUE است. در صورتی که مقدار configurationType، کارخواه باشد، باید در هر لحظه وجود داشته باشد.

useNATProbe

اختیاری. xs: بولی. تعیین می‌کند که آیا RAC از تشخیص خودکار NAT استفاده می‌کند. به صورت کارکردی در [RFC 3947] تعریف شده است. مقدار پیش‌فرض TRUE است. در صورتی که مقدار configurationType، کارخواه باشد، باید در هر لحظه وجود داشته باشد.

dpdHeartbeat

اختیاری. xs: صحیح. تعیین می‌کند که هر چند وقت یکبار RAC از ویژگی تشخیص همتای از دسترس خارج شده (DPD)[1] تعریف شده در [RFC 3706] استفاده می‌کند. در صورتی که مقدار configurationType، کارخواه باشد، باید در هر لحظه وجود داشته باشد.

natKeepalive

اختیاری. xs: صحیح. تعیین می‌کند که هر چند وقت یکبار RAC یک بسته UDP خالی به درگاهی ۴۵۰۰ RAS ارسال می‌کند. مقدار پیش‌فرض ۱۲۰ ثانیه است. به صورت کارکردی در [RFC 3947] تعریف شده است. در صورتی که مقدار configurationType، کارخواه باشد، باید در هر لحظه وجود داشته باشد.

rekeyingThreshold

اجباری. xs: صحیح. کلیدگذاری مجدد[2] SAی IKE را هنگامی‌که درصد مشخص شده از مدت زمان انقضای SAی IKE رسیده است، شروع می‌کند. مقادیر درصد قابل قبول در گستره ۷۰ تا ۹۵ قرار دارد.

proposal

1- Dead Peer Detection
2- rekeying

اجباری. شامل مجموعه‌ای از ویژگیهای استفاده شده هنگام شروع یک مذاکره IKE است. شامل زیر عناصر زیر است:

@protocol

اجباری .xs :نشانه. نوع پیشنهاد را توصیف می‌کند. مقدار مجاز IKE است.

encryptionAlgorithm

اجباری .xs :نشانه. الگوریتم رمز گذاری پیشنهاد شده را توصیف می‌کند. مقادیر مجاز در IKE2 تعریف شده است. شامل ویژگی زیر است:

keyLength

اختیاری. xs: صحیح. طول کلید الگوریتم رمزگذاری پیشنهاد شده را شرح می‌دهد. ممکن است اگر الگوریتم رمزگذاری ذکر شده در encryptionAlgorithm، طول مختلف کلید را اجازه دهد، در هر لحظه موجود باشد. مقادیر مجاز در IKEv2 شده است.

integrityAlgorithm

اجباری .xs :نشانه. الگوریتم اصالت‌سنجی پیشنهاد شده، را شرح می‌دهد. مقادیر مجاز در IKEv2 تعریف شده است.

pseudoRandomFunction

اجباری .xs :نشانه. تابع شبه تصادفی[1] پیشنهاد شده را شرح می‌دهد. مقادیر مجاز در IKEv2 تعریف شده است.

groupDescription

اجباری .xs :نشانه. گروه مورد استفاده در طول تبادل Diffie-Hellman (DH) را شرح می‌دهد. مقادیر مجاز در IKEv2 تعریف شده است.

groupType

اجباری .xs :نشانه. نوع گروه DH استفاده شده (به عنوان مثال، modular یا elliptic) را شرح می‌دهد. مقادیر مجاز در IKEv2 تعریف شده است.

lifetime

اجباری . بیشینه طول عمر SAی IKE، را شرح می‌دهد. شامل زیر عناصر زیر است:

seconds

اجباری. xs: صحیح. بیشینه دیرش SAی IKE.

kBytes

اجباری. xs: صحیح. بیشینه مقدار داده (برحسب بایت) که SAی IKE حفاظت می‌کند.

authenticationMethod

اجباری .xs :نشانه. شامل روش اصالت‌سنجی استفاده شده است. مقادیر مجاز در IKEv2 تعریف شده است.

credentialID

اجباری. xs: رشته. شامل ID منحصر به فرد اعتبارنامه ذخیره شده روی RATA است.

پ-۲ پرونده‌های IPsec نمونه

پ-۲-۱ IPsec نمونه برحسب گواهی‌ها

1- the pseudo random function

پ-۲-۱-۱ TransportAgentCapabilities نمونه IPsec

این پرونده TransportAgentCapabilities ساده، توانمندی موتور IPsec را شرح می‌دهد.

```
<?xml version="1.0" encoding="UTF-8"?>
<tads xmlns="urn:schemas-upnp-org:ra:tads"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:cfg="urn:schemas-upnp-org:ra:tacfg:ipsec"
xsi:schemaLocation="urn:schemas-upnp-org:ra:tads
http://www.upnp.org/schemas/ra/tads-v1.xsd
urn:schemas-upnp-org:ra:tacfg:ipsec
http://www.upnp.org/schemas/ra/tacfg-ipsec-v1.xsd">
<transportAgentCapability transportAgentName="IPsec">
<transportAgentOptions>
<cfg:ipsecOPT
authenticationMethod="RSA Digital Signature"
credentialEncoding="PKCS #7 wrapped X.509 certificate"
keyExchangeProtocol="IKEv2">
<cfg:encryptionAlgorithm>AES_CBC</cfg:encryptionAlgorithm>
<cfg:encryptionAlgorithm>AES_CTR</cfg:encryptionAlgorithm>
<cfg:authenticationAlgorithm></cfg:authenticationAlgorithm>
<cfg:integrityAlgorithm>AES_XCBC_96</cfg:integrityAlgorithm>
<cfg:pseudoRandomFunction>
AES128_XCBC
</cfg:pseudoRandomFunction>
</cfg:ipsecOPT>
</transportAgentOptions>
</transportAgentCapability>
</tads>
```

پ-۲-۱-۲ اطلاعات پیکربندی IPsec نمونه جهت کارساز

این پرونده نمونه اطلاعات پیکربندی به کارساز دستور می‌دهد تا برای هر جفت IPsec متناظر که سعی در برقراری اتصال دارد پیشنهادهای IKE ارائه کند و از SAی IKE ایجاد شده برای مبادله کاربرد ESP با توالی رمز AES_CBC با یک طول کلید ۲۵۶ استفاده خواهد شد. ESP SA بعداز ۲۸۸۰۰ ثانیه یا انتقال ۵۰۰۰ کیلوبایت منقضی می‌شود.

```
<?xml version="1.0" encoding="UTF-8"?>
<tads
xmlns="urn:schemas-upnp-org:ra:tads"
xmlns:cfg="urn:schemas-upnp-org:ra:tacfg:ipsec"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:schemas-upnp-org:ra:tads
http://www.upnp.org/schemas/ra/tads-v1.xsd
urn:schemas-upnp-org:ra:tacfg:ipsec
http://www.upnp.org/schemas/ra/tacfg-ipsec-v1.xsd">
<profileConfig dataStructureType="server">
<profileInfo id="12" transportAgentName="IPsec">
IPsec configuration
</profileInfo>
```

<profileData>
<cfg:ipsecCFG configurationType="server">
<cfg:policy>
<cfg:perfectForwardSecrecy>
true
</cfg:perfectForwardSecrecy>
<cfg:replayWindowLength>10</cfg:replayWindowLength>
<cfg:remoteIdentity>bob@home.com</cfg:remoteIdentity>
<cfg:proposal protocol="ESP">
<cfg:encryptionAlgorithm keyLength="256">
AES_CBC
</cfg:encryptionAlgorithm>
<cfg:lifetime>
<cfg:seconds>28800</cfg:seconds>
<cfg:kBytes>5000</cfg:kBytes>
</cfg:lifetime>
</cfg:proposal>
</cfg:policy>
<cfg:ike version="IKEv2">
<cfg:sendNotification>true</cfg:sendNotification>
<cfg:idType>ID_DER_ASN1_DN</cfg:idType>
<cfg:useIPsecExpire>true</cfg:useIPsecExpire>
<cfg:useReplayDetection>true</cfg:useReplayDetection>
<cfg:rekeyingThreshold>90</cfg:rekeyingThreshold>
<cfg:proposal protocol="IKE">
<cfg:encryptionAlgorithm keyLength="256">
AES_CBC
</cfg:encryptionAlgorithm>
<cfg:integrityAlgorithm>
AES_XCBC_96
</cfg:integrityAlgorithm>
<cfg:pseudoRandomFunction>
AES128_XCBC
</cfg:pseudoRandomFunction>
<cfg:groupDescription>MODP_1536</cfg:groupDescription>
<cfg:groupType>MODP</cfg:groupType>
<cfg:lifetime>
<cfg:seconds>28800</cfg:seconds>
<cfg:kBytes>5000</cfg:kBytes>
</cfg:lifetime>
</cfg:proposal>
<cfg:proposal protocol="IKE">
<cfg:encryptionAlgorithm keyLength="128">
AES_CBC
</cfg:encryptionAlgorithm>
<cfg:integrityAlgorithm>
AES_XCBC_96
</cfg:integrityAlgorithm>
<cfg:pseudoRandomFunction>
AES128_XCBC
</cfg:pseudoRandomFunction>
<cfg:groupDescription>MODP_1024</cfg:groupDescription>
<cfg:groupType>MODP</cfg:groupType>
<cfg:lifetime>

<cfg:seconds>28800</cfg:seconds>
<cfg:kBytes>5000</cfg:kBytes>
</cfg:lifetime>
</cfg:proposal>
<cfg:authenticationMethod>
RSA Digital Signature
</cfg:authenticationMethod>
<cfg:credentialID>100</cfg:credentialID>
</cfg:ike>
</cfg:ipsecCFG>
</profileData>
</profileConfig>
</tads>

پ-۲-۱-۳ ConfigInfoی IPsec نمونه برای کارخواه

این پرونده اطلاعات پیکربندی یک کارخواه IPsec را قادر می‌سازد تا اتصال IPsec را با کارساز IPsec پیکربندی شده در بند پ-۲-۱-۲ برقرار کند. پیشنهادهای IKE و ESP با یکی از همان‌ها از کارساز مطابقت خواهد کرد.

<?xml version="1.0" encoding="UTF-8"?>
<tads
xmlns="urn:schemas-upnp-org:ra:tads"
xmlns:cfg="urn:schemas-upnp-org:ra:tacfg:ipsec"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:schemas-upnp-org:ra:tads
http://www.upnp.org/schemas/ra/tads-v1.xsd
urn:schemas-upnp-org:ra:tacfg:ipsec
http://www.upnp.org/schemas/ra/tacfg-ipsec-v1.xsd">
<profileConfig dataStructureType="client">
<profileInfo id="12" transportAgentName="IPsec">
IPsec configuration
</profileInfo>
<profileData>
<cfg:ipsecCFG configurationType="client">
<cfg:policy>
<cfg:perfectForwardSecrecy>
true
</cfg:perfectForwardSecrecy>
<cfg:replayWindowLength>10</cfg:replayWindowLength>
<cfg:remoteIdentity>alice@home.com</cfg:remoteIdentity>
<cfg:proposal protocol="ESP">
<cfg:encryptionAlgorithm keyLength="256">
AES_CBC
</cfg:encryptionAlgorithm>
<cfg:lifetime>
<cfg:seconds>28800</cfg:seconds>
<cfg:kBytes>5000</cfg:kBytes>
</cfg:lifetime>
</cfg:proposal>
</cfg:policy>
<cfg:ike version="IKEv2">
<cfg:remoteAddress>129.178.89.81</cfg:remoteAddress>
<cfg:sendNotification>true</cfg:sendNotification>

<cfg:idType>ID_DER_ASN1_DN</cfg:idType>
<cfg:useIPsecExpire>true</cfg:useIPsecExpire>
<cfg:useReplayDetection>true</cfg:useReplayDetection>
<cfg:useInternalAddress>true</cfg:useInternalAddress>
<cfg:dpdHeartbeat>600</cfg:dpdHeartbeat>
<cfg:natKeepalive>100</cfg:natKeepalive>
<cfg:rekeyingThreshold>90</cfg:rekeyingThreshold>
<cfg:proposal protocol="IKE">
<cfg:encryptionAlgorithm keyLength="256">
AES_CBC
</cfg:encryptionAlgorithm>
<cfg:integrityAlgorithm>
AES_XCBC_96
</cfg:integrityAlgorithm>
<cfg:pseudoRandomFunction>
AES128_XCBC
</cfg:pseudoRandomFunction>
<cfg:groupDescription>MODP_1536</cfg:groupDescription>
<cfg:groupType>MODP</cfg:groupType>
<cfg:lifetime>
<cfg:seconds>28800</cfg:seconds>
<cfg:kBytes>5000</cfg:kBytes>
</cfg:lifetime>
</cfg:proposal>
<cfg:authenticationMethod>
RSA Digital Signature
</cfg:authenticationMethod>
<cfg:credentialID>100</cfg:credentialID>
</cfg:ike>
</cfg:ipsecCFG>
</profileData>
</profileConfig>
</tads>

پ-۲-۲ نمونه مبتنی بر خط‌مشی بدون کلید مشترک IPsec

پ-۲-۲-۱ نمونه تابع TransportAgentCapabilities‌ی IPsec

این پرونده تابع TransportAgentCapabilities ساده، توانمندی موتور IPsec را شرح می‌دهد.

```
<?xml version="1.0" encoding="UTF-8"?>
<tads xmlns="urn:schemas-upnp-org:ra:tads"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:cfg="urn:schemas-upnp-org:ra:tacfg:ipsec"
xsi:schemaLocation="urn:schemas-upnp-org:ra:tads
http://www.upnp.org/schemas/ra/tads-v1.xsd
urn:schemas-upnp-org:ra:tacfg:ipsec
http://www.upnp.org/schemas/ra/tacfg-ipsec-v1.xsd">
<transportAgentCapability transportAgentName="IPsec">
<transportAgentOptions>
<cfg:ipsecOPT
authenticationMethod="Shared Key Message Integrity Code"
credentialEncoding="Pre-Shared Key"
keyExchangeProtocol="IKEv2">
<cfg:encryptionAlgorithm>NULL</cfg:encryptionAlgorithm>
```

<cfg:authenticationAlgorithm></cfg:authenticationAlgorithm>
<cfg:integrityAlgorithm>HMAC_SHA1_96</cfg:integrityAlgorithm>
<cfg:pseudoRandomFunction>
HMAC_SHA1
</cfg:pseudoRandomFunction>
</cfg:ipsecOPT>
</transportAgentOptions>
</transportAgentCapability>
</tads>
C.2.2.2 Sample IPsec ConfigInfo for Server
<?xml version="1.0" encoding="UTF-8"?>
<tads
xmlns="urn:schemas-upnp-org:ra:tads"
xmlns:cfg="urn:schemas-upnp-org:ra:tacfg:ipsec"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:schemas-upnp-org:ra:tads
http://www.upnp.org/schemas/ra/tads-v1.xsd
urn:schemas-upnp-org:ra:tacfg:ipsec
http://www.upnp.org/schemas/ra/tacfg-ipsec-v1.xsd">
<profileConfig dataStructureType="client">
<profileInfo id="12" transportAgentName="IPsec">
IPsec configuration
</profileInfo>
<profileData>
<cfg:ipsecCFG configurationType="server">
<cfg:policy>
<cfg:perfectForwardSecrecy>
true
</cfg:perfectForwardSecrecy>
<cfg:replayWindowLength>10</cfg:replayWindowLength>
<cfg:remoteIdentity>bob@home.com</cfg:remoteIdentity>
<cfg:proposal protocol="ESP">
<cfg:encryptionAlgorithm>
NULL
</cfg:encryptionAlgorithm>
<integrityAlgorithm>
HMAC_SHA1_96
</integrityAlgorithm>
<cfg:lifetime>
<cfg:seconds>28800</cfg:seconds>
<cfg:kBytes>5000000</cfg:kBytes>
</cfg:lifetime>
</cfg:proposal>
</cfg:policy>
<cfg:ike version="IKEv2">
<cfg:sendNotification>true</cfg:sendNotification>
<cfg:idType>ID_KEY_ID</cfg:idType>
<cfg:useIPsecExpire>true</cfg:useIPsecExpire>
<cfg:useReplayDetection>true</cfg:useReplayDetection>
<cfg:rekeyingThreshold>90</cfg:rekeyingThreshold>
<cfg:proposal protocol="IKE">
<cfg:encryptionAlgorithm keyLength="128">
AES_CBC
</cfg:encryptionAlgorithm>

<cfg:integrityAlgorithm>
HMAC_SHA1_96
</cfg:integrityAlgorithm>
<cfg:pseudoRandomFunction>
HMAC_SHA1
</cfg:pseudoRandomFunction>
<cfg:groupDescription>MODP_768</cfg:groupDescription>
<cfg:groupType>MODP</cfg:groupType>
<cfg:lifetime>
<cfg:seconds>28800</cfg:seconds>
<cfg:kBytes>5000</cfg:kBytes>
</cfg:lifetime>
</cfg:proposal>
<cfg:authenticationMethod>
Shared Key Message Integrity Code
</cfg:authenticationMethod>
<cfg:credentialID>100</cfg:credentialID>
</cfg:ike>
</cfg:ipsecCFG>
</profileData>
</profileConfig>
</tads>

پ-۲-۲-۳اطلاعات پیکربندی IPsec نمونه

این پرونده ConfigInfo، یک کارخواه IPsec را قادر می‌سازد تا اتصال IPsec را با کارساز IPsec پیکربندی شده در بند ۰، برقرار کند.

<?xml version="1.0" encoding="UTF-8"?>
<tads
xmlns="urn:schemas-upnp-org:ra:tads"
xmlns:cfg="urn:schemas-upnp-org:ra:tacfg:ipsec"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:schemas-upnp-org:ra:tads
http://www.upnp.org/schemas/ra/tads-v1.xsd
urn:schemas-upnp-org:ra:tacfg:ipsec
http://www.upnp.org/schemas/ra/tacfg-ipsec-v1.xsd">
<profileConfig dataStructureType="client">
<profileInfo id="12" transportAgentName="IPsec">
IPsec configuration
</profileInfo>
<profileData>
<cfg:ipsecCFG configurationType="client">
<cfg:policy>
<cfg:perfectForwardSecrecy>
true
</cfg:perfectForwardSecrecy>
<cfg:replayWindowLength>10</cfg:replayWindowLength>
<cfg:remoteIdentity>alice@home.com</cfg:remoteIdentity>
<cfg:proposal protocol="ESP">
<cfg:encryptionAlgorithm>
NULL
</cfg:encryptionAlgorithm>
<integrityAlgorithm>

HMAC_SHA1_96
</cfg:integrityAlgorithm>
<cfg:lifetime>
<cfg:seconds>28800</cfg:seconds>
<cfg:kBytes>5000000</cfg:kBytes>
</cfg:lifetime>
</cfg:proposal>
</cfg:policy>
<cfg:ike version="IKEv2">
<cfg:remoteAddress>129.178.89.81</cfg:remoteAddress>
<cfg:sendNotification>true</cfg:sendNotification>
<cfg:idType>ID_KEY_ID</cfg:idType>
<cfg:useIPsecExpire>true</cfg:useIPsecExpire>
<cfg:useReplayDetection>true</cfg:useReplayDetection>
<cfg:useInternalAddress>true</cfg:useInternalAddress>
<cfg:dpdHeartbeat>600</cfg:dpdHeartbeat>
<cfg:natKeepalive>100</cfg:natKeepalive>
<cfg:rekeyingThreshold>90</cfg:rekeyingThreshold>
<cfg:proposal protocol="IKE">
<cfg:encryptionAlgorithm keyLength="128">
AES_CBC
</cfg:encryptionAlgorithm>
<cfg:integrityAlgorithm>
HMAC_SHA1_96
</cfg:integrityAlgorithm>
<cfg:pseudoRandomFunction>
HMAC_SHA1
</cfg:pseudoRandomFunction>
<cfg:groupDescription>MODP_768</cfg:groupDescription>
<cfg:groupType>MODP</cfg:groupType>
<cfg:lifetime>
<cfg:seconds>28800</cfg:seconds>
<cfg:kBytes>5000</cfg:kBytes>
</cfg:lifetime>
</cfg:proposal>
<cfg:authenticationMethod>
Shared Key Message Integrity Code
</cfg:authenticationMethod>
<cfg:credentialID>100</cfg:credentialID>
</cfg:ike>
</cfg:ipsecCFG>
</profileData>
</profileConfig>
</tads>

C.2.3 Sample IPSec based on shared key advanced policy

C.2.3.1 Sample IPsec TransportAgentCapabilities

This simple TransportAgentCapabilities file describes the capability of the IPsec engine.

<?xml version="1.0" encoding="UTF-8"?>
<tads xmlns="urn:schemas-upnp-org:ra:tads"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:cfg="urn:schemas-upnp-org:ra:tacfg:ipsec"
xsi:schemaLocation="urn:schemas-upnp-org:ra:tads
http://www.upnp.org/schemas/ra/tads-v1.xsd
urn:schemas-upnp-org:ra:tacfg:ipsec

http://www.upnp.org/schemas/ra/tacfg-ipsec-v1.xsd">
<transportAgentCapability transportAgentName="IPsec">
<transportAgentOptions>
<cfg:ipsecOPT
authenticationMethod="Shared Key Message Integrity Code"
credentialEncoding="Pre-Shared Key"
keyExchangeProtocol="IKEv2">
<cfg:encryptionAlgorithm>AES_CBC</cfg:encryptionAlgorithm>
<cfg:authenticationAlgorithm></cfg:authenticationAlgorithm>
<cfg:integrityAlgorithm>HMAC_SHA1_96</cfg:integrityAlgorithm>
<cfg:pseudoRandomFunction>HMAC_SHA1</cfg:pseudoRandomFunction>
</cfg:ipsecOPT>
</transportAgentOptions>
</transportAgentCapability>
</tads>

C.2.3.2 Sample IPsec ConfigInfo for Server

<?xml version="1.0" encoding="UTF-8"?>
<tads
xmlns="urn:schemas-upnp-org:ra:tads"
xmlns:cfg="urn:schemas-upnp-org:ra:tacfg:ipsec"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:schemas-upnp-org:ra:tads
http://www.upnp.org/schemas/ra/tads-v1.xsd
urn:schemas-upnp-org:ra:tacfg:ipsec
http://www.upnp.org/schemas/ra/tacfg-ipsec-v1.xsd">
<profileConfig dataStructureType="client">
<profileInfo id="12" transportAgentName="IPsec">
IPsec configuration
</profileInfo>
<profileData>
<cfg:ipsecCFG configurationType="server">
<cfg:policy>
<cfg:perfectForwardSecrecy>
true
</cfg:perfectForwardSecrecy>
<cfg:replayWindowLength>10</cfg:replayWindowLength>
<cfg:remoteIdentity>bob@home.com</cfg:remoteIdentity>
<cfg:proposal protocol="ESP">
<cfg:encryptionAlgorithm keyLength="128">
AES_CBC
</cfg:encryptionAlgorithm>
<integrityAlgorithm>
HMAC_SHA1_96
</integrityAlgorithm>
<cfg:lifetime>
<cfg:seconds>28800</cfg:seconds>
<cfg:kBytes>5000000</cfg:kBytes>
</cfg:lifetime>
</cfg:proposal>
</cfg:policy>
<cfg:ike version="IKEv2">
<cfg:sendNotification>true</cfg:sendNotification>
<cfg:idType>ID_KEY_ID</cfg:idType>
<cfg:useIPsecExpire>true</cfg:useIPsecExpire>

<cfg:useReplayDetection>true</cfg:useReplayDetection>
<cfg:rekeyingThreshold>90</cfg:rekeyingThreshold>
<cfg:proposal protocol="IKE">
<cfg:encryptionAlgorithm keyLength="128">
AES_CBC
</cfg:encryptionAlgorithm>
<cfg:integrityAlgorithm>
HMAC_SHA1_96
</cfg:integrityAlgorithm>
<cfg:pseudoRandomFunction>
HMAC_SHA1
</cfg:pseudoRandomFunction>
<cfg:groupDescription>MODP_1536</cfg:groupDescription>
<cfg:groupType>MODP</cfg:groupType>
<cfg:lifetime>
<cfg:seconds>28800</cfg:seconds>
<cfg:kBytes>5000</cfg:kBytes>
</cfg:lifetime>
</cfg:proposal>
<cfg:authenticationMethod>
Shared Key Message Integrity Code
</cfg:authenticationMethod>
<cfg:credentialID>100</cfg:credentialID>
</cfg:ike>
</cfg:ipsecCFG>
</profileData>
</profileConfig>
</tads>

C.2.3.3 Sample IPsec ConfigInfo for Client

This ConfigInfo file allows a IPsec client to establish IPsec connection with the IPsec server configured in clause 0.

<?xml version="1.0" encoding="UTF-8"?>
<tads
xmlns="urn:schemas-upnp-org:ra:tads"
xmlns:cfg="urn:schemas-upnp-org:ra:tacfg:ipsec"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:schemas-upnp-org:ra:tads
http://www.upnp.org/schemas/ra/tads-v1.xsd
urn:schemas-upnp-org:ra:tacfg:ipsec
http://www.upnp.org/schemas/ra/tacfg-ipsec-v1.xsd">
<profileConfig dataStructureType="client">
<profileInfo id="12" transportAgentName="IPsec">
IPsec configuration
</profileInfo>
<profileData>
<cfg:ipsecCFG configurationType="client">
<cfg:policy>
<cfg:perfectForwardSecrecy>
true
</cfg:perfectForwardSecrecy>
<cfg:replayWindowLength>10</cfg:replayWindowLength>
<cfg:remoteIdentity>alice@home.com</cfg:remoteIdentity>
<cfg:proposal protocol="ESP">
<cfg:encryptionAlgorithm keyLength="128">

AES_CBC
</cfg:encryptionAlgorithm>
<integrityAlgorithm>
HMAC_SHA1_96
</integrityAlgorithm>
<cfg:lifetime>
<cfg:seconds>28800</cfg:seconds>
<cfg:kBytes>5000000</cfg:kBytes>
</cfg:lifetime>
</cfg:proposal>
</cfg:policy>
<cfg:ike version="IKEv2">
<cfg:remoteAddress>129.178.89.81</cfg:remoteAddress>
<cfg:sendNotification>true</cfg:sendNotification>
<cfg:idType>ID_KEY_ID</cfg:idType>
<cfg:useIPsecExpire>true</cfg:useIPsecExpire>
<cfg:useReplayDetection>true</cfg:useReplayDetection>
<cfg:useInternalAddress>true</cfg:useInternalAddress>
<cfg:dpdHeartbeat>600</cfg:dpdHeartbeat>
<cfg:natKeepalive>100</cfg:natKeepalive>
<cfg:rekeyingThreshold>90</cfg:rekeyingThreshold>
<cfg:proposal protocol="IKE">
<cfg:encryptionAlgorithm keyLength="128">
AES_CBC
</cfg:encryptionAlgorithm>
<cfg:integrityAlgorithm>
HMAC_SHA1_96
</cfg:integrityAlgorithm>
<cfg:pseudoRandomFunction>
HMAC_SHA1
</cfg:pseudoRandomFunction>
<cfg:groupDescription>MODP_1536</cfg:groupDescription>
<cfg:groupType>MODP</cfg:groupType>
<cfg:lifetime>
<cfg:seconds>28800</cfg:seconds>
<cfg:kBytes>5000</cfg:kBytes>
</cfg:lifetime>
</cfg:proposal>
<cfg:authenticationMethod>
Shared Key Message Integrity Code
</cfg:authenticationMethod>
<cfg:credentialID>100</cfg:credentialID>
</cfg:ike>
</cfg:ipsecCFG>
</profileData>
</profileConfig>
</tads>

پیوست ت

(اطلاعاتی)

استفاده از OpenVPN به عنوان انتقال دسترسی از دور

هدف این پیوست شرح چگونگی استفاده از پروتکل OpenVPN به عنوان سازوکار انتقال دسترسی از دور، در UPnP است.

ت-۱ الگوهای OpenVPN

ت-۱-۱ الگوی پیکربندی OpenVPN

الگوی پیکربندی OpenVPN رایج در درجه اول طراحی می‌شود تا برای مستقر کردن پرونده پیکربندی OpenVPN مورد استفاده توسط OpenVPN، استفاده شود.

```
<?xml version="1.0" encoding="UTF-8"?>
<openvpnCFG xmlns="urn:schemas-upnp-org:ra:tacfg:openvpn"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:schemas-upnp-org:ra:tacfg:openvpn
http://www.upnp.org/schemas/ra/tacfg-openvpn-v1.xsd"
configurationType="server">
<protocol type="UDP">
<dev>tap0</dev>
</protocol>
<sslTls>
<cipher>AES-128-CBC</cipher>
<credentialID>100</credentialID>
</sslTls>
<client remoteHost="vpn.mydomain.org" remotePort="1194">
<resolveRetry seconds="-1"/>
<devNode>MyVPNInterface</devNode>
<httpProxy proxyIP="10.0.0.40" proxyPort="7788"/>
</client>
<server listeningIP="10.0.0.10" listeningPort="1194">
<persistPool>pool.txt</persistPool>
<bridge ip="10.1.1.10" netMask="255.255.255.0" startingIP="10.1.1.20"
endingIP="10.1.1.30"/>
<routedIP ip="10.1.1.0" netMask="255.255.255.0"/>
<push>
<route ip="192.168.1.0" subnetMask="255.255.255.0"/>
<gateway redirect="true"/>
<dhcpOption name="DNS" data="10.66.0.4"/>
</push>
<clientToClient>true</clientToClient>
<duplicateKeyPairs>0</duplicateKeyPairs>
<maxClients>5</maxClients>
</server>
<options>
<keepAlive interval="10" timeout="120"/>
<enableCompression algorithm="lzo">true</enableCompression>
<status update="1" filename="status.txt"/>
<log enabled="1" append="1" filename="log.txt" verbosity="4"
silenceAfter="5"/>
</options>
</openvpnCFG>
xml
```

اجباری برای تمام اسناد xlm. حساس به حروف کوچک.

openvpnCFG

اجباری. باید ”urn:schemas-upnp-org:ra:tacfg:openvpn“ را به عنوان مقداری برای ویژگی‌های xmlns داشته باشد؛ این به طرح الگوی پیکربندی OpenVPN کمیته کاری دسترسی از دور UpnP ارجاع می‌دهد. تا زمانی که از xmlns یکسان استفاده می‌شود، الگوی ساختار داده باید سازگار با قبل باشد، یعنی توسط پیاده‌سازی‌های موروثی قابل استفاده باشد. شامل ویژگی‌ها و زیر عناصر زیر است:

@configurationType

اجباری .xs :نشانه. نوع پیکربندی را تعیین می‌کند. مقادیر ممکن "client" یا "server" است.

protocol

اجباری . لایه زیرین انتقال OpenVPN را تعیین می‌کند. شامل زیر عناصر و ویژگی‌های زیر است:

@type

اجباری .xs :نشانه. تعیین می‌کند که آیا انتقال زیربنایی TCP است یا UDP. مقادیر ممکن "TCP" یا " UDP" است.

dev

اجباری .xs :نشانه. نوع تونل را مشخص می‌کند.

"tun“، یک تونل IP مسیریابی شده[1] ایجاد خواهد کرد،

"tap“، یک تونل اترنت ایجاد خواهد کرد.

اگر شما پل اترنت هستید و از قبل یک واسط tap0 مجازی ایجاد و به واسط اترنتی خود وصل کرده‌اید، از "tap0“استفاده کنید.

sslTls

اجباری. تنظیمات SSL/TLS استفاده شده توسط OpenVPN را مشخص می‌کند. شامل زیر عناصر زیر است:

Cipher

اختیاری .xs :نشانه. فرآیند رمزنگاری اعمال شده است. مقادیر قابل قبول عبارتند از:

”BF-CBC“، بلوفیش[2] (پیش فرض)

AES ،”AES-128-CBC“

”DES-EDE3-CBC“، DES سه گانه

credentialID

اجباری. xs: رشته. شامل ID منحصر به فرد یک اعتبارنامه ذخیره شده روی RATA است.

Client

اختیاری. پیکربندی خاص کارخواه را مشخص می‌کند. باید اگر @configurationTyp ، "client" باشد، مشخص شود. شامل زیر عناصر و ویژگی‌های زیر است:

@remoteHost

اجباری. xs: رشته. نام میزبان کارساز OpenVPN برای اتصال به آن.

@remotePort

1- routed IP tunnel
2- Blowfish

اجباری. xs: صحیح. شماره درگاهی کارساز OpenVPN برای اتصال به آن.

resolveRetry

اجباری. مدت زمان تلاش مجدد برای برگردان کردن نام میزبان راه دور، را مشخص می‌کند. باید دارای ویژگی زیر باشد:

@seconds

اجباری. xs: صحیح. تعداد ثانیه‌هایی که بهتر است همچنان کارخواه OpenVPN به تلاش مجدد برای برگردان کردن نام میزبان، در صورت عدم موفقیت آن ادامه دهد. مقدار ۱- به این معنا است که بهتر است کارخواه برای یک مدت زمان نامحدود به تلاش مجدد ادامه دهد.

devNode

اختیاری. xs: رشته. نام واسط OpenVPN را مشخص می‌کند. باید روی سامانه عامل‌های ویندوزی استفاده شود.

httpProxy

اختیاری. استفاده از یک پروکسی HTTP برای اتصال به کارساز OpenVPN را مشخص می‌کند. شامل ویژگی‌های زیر است:

@proxyIP

اجباری. xs: رشته. نشانی IP یا FQDN پیشکار[1] http.

@proxyPort

اجباری. xs: صحیح. شماره درگاهی پیشکار http.

Server

اختیاری. پیکربندی خاص کارساز را مشخص می‌کند. باید اگر @configurationTyp، "server" باشد، مشخص شود. شامل زیر عناصر و ویژگی‌های زیر است:

@listeningIP

اختیاری. xs: رشته. نشانی IP محلی که کارساز به آن متصل می‌شود.

@listeningPort

اختیاری. xs: صحیح. شماره درگاهی که کارساز به آن متصل می‌شود.

persistPool

اختیاری. xs: رشته. می‌تواند به کارخواه‌هایی که مجددا وصل می‌شوند، همان نشانی IP مجازی از مجموعه‌ای که قبلا استفاده، اختصاص یابد. مقدار مشخص شده، نام پرونده استفاده شده برای ذخیره این اطلاعات پایدار است..

bridge

اختیاری. حالت کارساز را برای پل اترنت پیکربندی کنید. پیکربندی باید یک گستره IP را با زیر شبکه[2] مشخص شده کنار بگذارد تا به کارخواه‌های متصل شده اختصاص یابد. اگر کارساز برای پل اترنت پیکربندی شده باشد، باید مشخص شود. نباید در رابطه با عنصر IP مسیریابی شده، استفاده شود. شامل ویژگی‌های زیر است:

1- proxy server
2- subnet

@ip

اجباری. xs: رشته. نشانی IP واسط پل.

@netMask

اجباری. xs: رشته. زیر شبکه ماسک واسط پل.

@startingIP

اجباری. xs: رشته. نشانی IP آغازین برای اختصاص به مجموعه IP.

@endingIP

اجباری. xs: رشته. نشانی IP پایانی برای اختصاص به مجموعهIP .

routedIP

اختیاری. حالت کارساز را برای IP مسیریابی شده پیکربندی می‌کند، تا برای OpenVPN، یک زیر شبکه VPN به منظور بیرون کشیدن نشانی‌های کارخواه از آن تامین کند. کارساز اولین نشانی IP را برای خودش برخواهد داشت. بقیه نشانی‌های IP برای اختصاص به کارخواه‌ها موجود است. هر کارخواه قادر خواهد بود تا روی آن نشانی IP خود اختصاص یافته، به کارساز دسترسی پیدا کند. نباید در رابطه با عنصر پل استفاده شود. اگر کارساز برای IP مسیریابی شده پیکربندی شود، باید مشخص شود. شامل ویژگی‌های زیر است:

@ip

اجباری. xs: رشته. نشانی IP زیر شبکه تونل VPN مسیریابی شده.

@netMask

اجباری. xs: رشته. پوشش زیر شبکه (سابنت ماسک) [1] نشانی زیر شبکه.

Push

اختیاری. به کارساز اجازه می‌دهد تا گزینه‌های گوناگون را در کارخواه بنشاند. شامل یک یا چند زیر عناصر زیر است:

route

اختیاری. به کارساز اجازه می‌دهد تا مسیرها را در کارخواه بنشاند تا آن بتواند به سایر زیر شبکه‌های اختصاصی با اتکا به کارساز دست یابد. شامل ویژگی‌های زیر است:

@ip

اجباری. xs: رشته. نشانی IP قسمتی از مسیر که باید نشانده شود.

@subnetMask

اجباری. xs: رشته. قسمتی از پوشش شبکه مسیر که باید نشانده شود.

gateway

اختیاری.به کارساز اجازه می‌دهد تا دروازه پیش فرض را برای کارخواه مشخص کند. شامل ویژگی زیر است:

@redirect

اجباری. xs: بولی. مشخص می‌کند که آیا باید دروازه پیش فرض به کارساز OpenVPN هدایت شود یا خیر.

dhcpOption

اختیاری. به کارساز اجازه می‌دهد تا گزینه‌های DHCP را روی کارخواه بنشاند. شامل ویژگی‌های زیر است:

@name

اجباری. xs: رشته. نام گزینه DHCP برای نشاندن..

@data

1- Subnet mask

اجباری. xs: رشته. مقداری برای گزینه DHCP مشخص شده در بالا.

clientToClient

اختیاری. xs: بولی. مشخص می‌کند که آیا کارخواه‌های متصل شده برای یکدیگر قابل مشاهده هستند یا خیر.

duplicateKeyPairs

اختیاری. xs: بولی. مشخص می‌کند که آیا لازم است که کارخواه‌ها با گواهی‌های منحصر به فرد وارد شود. OpenVPN توصیه می‌کند که در محیط‌های اشکال زدایی تنها گواهی‌های دونسخه‌ای مجاز می‌باشند.

maxClients

اختیاری. xs: صحیح. بیشینه تعداد کارخواه‌های همزمان مجاز را مشخص می‌کند.

options

اختیاری. گزینه‌های دیگر را مشخص می‌کند. شامل زیر عناصر زیر است:

keepAlive

اختیاری. پارامترهای زنده نگهداشتن را برای نقطه پایانی کارساز/کارخواه مشخص می‌کند. شامل ویژگی‌های زیر است:

@interval

اجباری. xs: صحیح. بازه بسامد برحسب ثانیه مشخص شده است. یک Keep Alive هر X ثانیه ارسال خواهد شد، در اینجا X مقدار مشخص شده است.

@timeout

اجباری. xs: صحیح. تعداد ثانیه‌هایی که باید بدون دریافت یک Keep Alive قبل از آنکه نقطه پایانی نشست را منقضی شده درنظر بگیرد، سپری شود.

enableCompression

اختیاری. xs: بولی. مشخص می‌کند که آیا پیوند OpenVPN، فشرده سازی را به کار می‌برد. شامل ویژگی زیر است:

@algorithm

اختیاری .xs :نشانه. در حال حاضر ”lzo“ پشتیبانی می‌شود. باید اگر فشرده‌سازی استفاده شود، وجود داشته باشد.

status

اختیاری. یک پرونده وضعیت که اتصال‌های جاری را نشان می‌دهد، هر دقیقه بریده و بازنویسی می‌شود، را مشخص می‌کند. شامل ویژگی‌های زیر است:

@update

اجباری. xs: بولی. مشخص می‌کند که آیا به روزرسانی‌های پرونده فعال است.

@filename

اجباری. xs: رشته. نام پرونده‌ای که باید به روز رسانی‌ها در آن نوشته شود، را مشخص می‌کند.

Log

اختیاری. xs: رشته. به صورت پیش فرض، پیام‌های ثبت وقایع[1] به syslog خواهد رفت (یا در ویندوزها، اگر به عنوان یک خدمت اجرا شوند، آنها به دایرکتوری "\Program Files\OpenVPN\log"[2] خواهند رفت). این اجازه می‌دهد که این رفتار پیش فرض لغو شود. شامل ویژگی‌های زیر است:

@enabled

اجباری. xs: بولی. مشخص می‌کند که آیا رفتار لغو خواهد شد.

@append

اجباری. xs: بولی. مشخص می‌کند که آیا پرونده ثبت وقایع اضافه یا لغو خواهد شد.

@filename

اجباری. xs: رشته. نام پرونده‌ای که ثبت وقایع باید در آن نوشته شود، را مشخص می‌کند.

@verbosity

اختیاری. xs: صحیح. درازای پرونده ثبت وقایع، از ۰ تا ۹.

۰ به جز درمورد خطاهای جدی ساکت است.

۴ مناسب برای استفاده عمومی

۵ تا ۶ می‌تواند به اشکال زدایی مشکلات اتصال کمک کند.

۹ بسیار دراز است

@silenceAfter

اختیاری. xs: صحیح. پیام‌های تکرارکننده سکوت. در بیشتر n پیام‌های متوالی از همان رده پیام خروجی ثبت وقایع خواهد بود، در اینجا n مقدار مشخص شده است.

ت-۲ پیکربندی OpenVPN نمونه

ت-۲-۱ پیکربندی نمونه برای کارساز

```
<?xml version="1.0" encoding="UTF-8"?>
<tads
xmlns="urn:schemas-upnp-org:ra:tads"
xmlns:cfg="urn:schemas-upnp-org:ra:tacfg:openvpn"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:schemas-upnp-org:ra:tads
http://www.upnp.org/schemas/ra/tads-v1.xsd
urn:schemas-upnp-org:ra:tacfg:openvpn
http://www.upnp.org/schemas/ra/tacfg-openvpn-v1.xsd">
<profileConfig dataStructureType="server">
<profileInfo id="12" transportAgentName="OpenVPN">
OpenVPN configuration
</profileInfo>
<profileData>
<cfg:openvpnCFG configurationType="server">
<cfg:protocol type="UDP">
<cfg:dev>tap0</cfg:dev>
</cfg:protocol>
<cfg:sslTls>
<cfg:cipher>AES-128-CBC</cfg:cipher>
```

1- log
2- directory

```
<cfg:credentialID>100</cfg:credentialID>
</cfg:sslTls>
<cfg:server listeningPort="1194">
<cfg:persistPool>pool.txt</cfg:persistPool>
<cfg:bridge
ip="10.1.1.10"
netMask="255.255.255.0"
startingIP="10.1.1.20"
endingIP="10.1.1.30"/>
<cfg:push>
<cfg:gateway redirect="true"/>
</cfg:push>
<cfg:clientToClient>true</cfg:clientToClient>
</cfg:server>
<cfg:options>
<cfg:keepAlive interval="10" timeout="120"/>
<cfg:enableCompression algorithm="lzo">
true
</cfg:enableCompression>
</cfg:options>
</cfg:openvpnCFG>
</profileData>
</profileConfig>
</tads>
```

ت-۲-۲ پیکربندی نمونه برای کارخواه

```
<?xml version="1.0" encoding="UTF-8"?>
<tads
xmlns="urn:schemas-upnp-org:ra:tads"
xmlns:cfg="urn:schemas-upnp-org:ra:tacfg:openvpn"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:schemas-upnp-org:ra:tads
http://www.upnp.org/schemas/ra/tads-v1.xsd
urn:schemas-upnp-org:ra:tacfg:ipsec
http://www.upnp.org/schemas/ra/tacfg-openvpn-v1.xsd">
<profileConfig dataStructureType="server">
<profileInfo id="12" transportAgentName="OpenVPN">
OpenVPN configuration
</profileInfo>
<profileData>
<cfg:openvpnCFG configurationType="client">
<cfg:protocol type="UDP">
<cfg:dev>tap</cfg:dev>
</cfg:protocol>
<cfg:sslTls>
<cfg:cipher>AES-128-CBC</cfg:cipher>
<cfg:credentialID>100</cfg:credentialID>
</cfg:sslTls>
<cfg:client remoteHost="vpn.mydomain.org" remotePort="1194">
<cfg:resolveRetry seconds="-1"/>
<cfg:devNode>MyVPNInterface</cfg:devNode>
</cfg:client>
<cfg:options>
<cfg:keepAlive interval="10" timeout="120"/>
```

<cfg:enableCompression algorithm="lzo">
true
</cfg:enableCompression>
</cfg:options>
</cfg:openvpnCFG>
</profileData>
</profileConfig>
</tads>