استاندارد ملی ایران ایزو آی ای سی
۲۹۳۴۱-۸-۵
چاپ اول
۱۳۹۱

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standardization Organization

INSO-ISO-IEC
29341-8-5
1st. Edition
2012
Endorsement of
ISO/IEC 29341-8-5:2008

فن‌آوری اطلاعات- معماری افزاره جامع اتصال و اجرا UPnP
قسمت ۸-۵: پروتکل کنترل افزاره دروازه اینترنت – افزاره نقطه دسترسی شبکه محلی بی‌سیم

Information technology - UPnP Device Architecture – Part 8-5: Internet Gateway Device Control Protocol – Wireless Local Area Network Access Point Device

ICS:35.200

به‌نام 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 حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فن‌آوری 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، سازمان‌های دولتی و غیر دولتی حاصل می شود. پیش‌نویس 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 می‌کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود . بدین ترتیب ، استانداردهایی ملی تلقی می‌شوند 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 پیشرفت‌های 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 صدور گواهی 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

" فن‌آوری اطلاعات – معماری افزاره UPnP – قسمت ۸-۵: پروتکل کنترل افزاره دروازه اینترنت – افزاره نقطه دسترسی شبکه محلی بی‌سیم"

رئیس:	**سمت و/یا نمایندگی**
نعمتی، فرهاد (فوق لیسانس مهندسی کامپیوتر)	دانشگاه آزاد اسلامی تبریز

دبیر:

خوشقدم، سهیلا (لیسانس مهندسی کامپیوتر)	شرکت ریزفناوران آرکا پژوه

اعضاء: (اسامی به ترتیب حروف الفبا)

اصل‌زاد، محمدعلی (لیسانس مهندسی کامپیوتر)	شرکت ریزفناوران آرکاپژوه
الهی، بهمن (لیسانس مکانیک)	شهرداری تبریز
بدلی افشرد، بابک (لیسانس مهندسی کامپیوتر)	اداره کل استاندارد آذربایجان‌شرقی
بدلی افشرد، محمدرضا (فوق لیسانس برق الکترونیک)	نیروگاه برق تبریز
جباری خامنه، حسین (دکترای آمار)	دانشگاه سراسری تبریز
خاکپور، علی (لیسانس مهندسی کامپیوتر)	شرکت ایران دیتا
علیوند، فاطمه (لیسانس مهندسی کامپیوتر)	شرکت ریزفناوران آرکاپژوه

پیش‌گفتار

استاندارد " فن‌آوری اطلاعات – معماری افزاره جامع اتصال و اجرا UPnP قسمت ۸-۵: پروتکل کنترل افزاره دروازه اینترنت – افزاره نقطه دسترسی شبکه محلی بی‌سیم" که پیش‌نویس آن در کمیسیون فنی مربوط، توسط شرکت ریزفناوران آرکا پژوه بر مبنای روش تنفیذ مورد اشاره در راهنمای **ISO/IEC Guide 21-1 (پذیرش ملی استانداردهای "بین‌المللی" و دیگر مدارک استاندارد)** به‌عنوان استاندارد ملی ایران، تهیه شده و در یکصدو شصت و دومین اجلاسیه کمیته ملی استاندارد رایانه و فرآوری داده مورخ ۹۱/۰۲/۱۰ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات سازمان ملی استاندارد ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع ، علوم و خدمات، استانداردهای ملی ایران در موقع لزوم تجدیدنظر خواهد شد و هرگونه پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، همواره از آخرین تجدیدنظر آن‌ها استفاده خواهد شد.

این استاندارد ملی بر اساس پذیرش استاندارد "بین‌المللی" به شرح زیر است:

ISO/IEC 29341-8-5: 2008, Information technology – UPnP Device Architecture- Part 8-5: Internet Gateway Device Control Protocol – Wireless Local Area Network Access Point Device.

فن‌آوری اطلاعات- معماری افزاره جامع اتصال و اجرا UPnP قسمت ۸-۵: پروتکل کنترل افزاره دروازه اینترنت – افزاره نقطه دسترسی شبکه محلی بی‌سیم

۱ هدف و دامنه کاربرد

این استاندارد ملی، براساس پذیرش استاندارد بین‌المللی ISO/IEC 29341-8-5:2008 تدوین شده است.

این استاندارد یکی از مجموعه استانداردهای ایران ایزو آی ای سی به شماره 29341 است.

هدف از تدوین این استاندارد، توصیف افزاره‌ای برای دسترسی بی‌سیم در شبکه است.

قالب این افزاره با معماری افزاره جامع اتصال و اجرا نسخه ۱.۰ سازگار است.

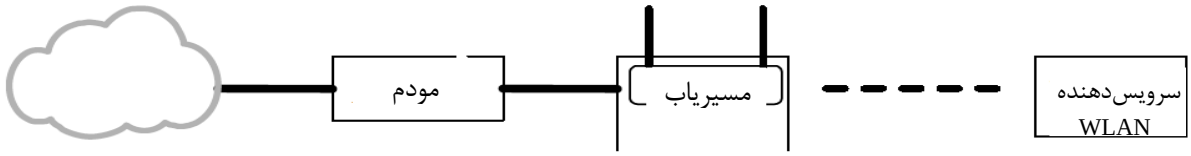
این استاندارد افزاره ریشه مورد نیاز را تعریف می‌کند.

urn:schemas-upnp-org:device:WLANAccessPointDevice.

در این استاندارد WLANAccessPointDevice خدمت‌هایی را برای پروتکل کنترل افزاره نقطه دسترسی[۱] محصورسازی[۲] می‌کند.

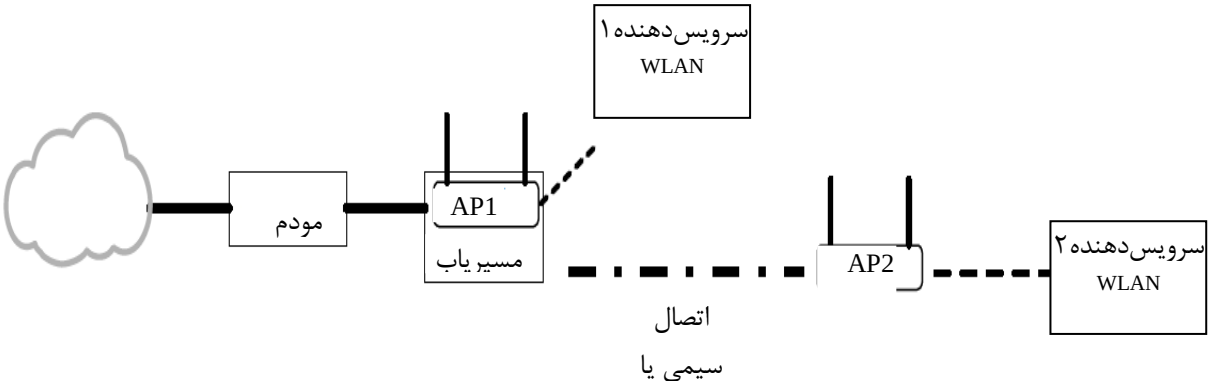
نقطه دسترسی[۳] شبکه محلی بی‌سیم[۴] افزاره‌ای است که استانداردهای بی‌سیم IEEE 802.11 را برای فراهم آوردن یک زیرساخت برای شبکه‌های خانگی یا تجاری کوچک، پیاده می‌کند. تعریف افزاره شامل استفاده افزاره در شبکه‌های سرمایه گذاری یا Hotspot[۵] نمی‌باشد.

نقطه دسترسی مانند یک پل اترنت عمل می‌کند که امکان اتصال چند گروه را به شبکه محلی فراهم می‌کند. شکل الف-۱ توپولوژی مشترک مورد استفاده برای یک شبکه محلی بی‌سیم را نشان می‌دهد. شکل ب-۱ مصرف نقطه دسترسی برای گسترش دسترسی به یک شبکه محلی را نشان می‌دهد. DCP هر دو مورد را پوشش می‌دهد.



شکل ۱- الف– افزاره نقطه دسترسی شبکه محلی بی‌سیم – مدل مورد استفاده رایج

1- Device Control Protocol (DCP)
2- Encapsulates
3- Access Point (AP)
4- Wireless (WLAN)
۵- یک ناحیه‌ی جغرافیایی می‌باشد که در آن اینترنت توسط یک یا چند AP به صورت رایگان یا تجاری ارائه می‌شود مثل هتل‌ها-رستوران‌ها - فرودگاه‌ها و... صاحب این مکان‌ها می‌توانند به ارائه اینترنت رایگان، جذب مشتری کنند.



شکل ۱- ب- توسعه شبکه موجود – توپولوژی نمونه

۱-۱ نقطه تمرکز و اهداف DCP نسخه ۱/۰

گروه کاری افزاره دروازه اینترنت (IGD) توافق کرده‌اند که بر روی ویژگی‌های زیر تمرکز نمایند:

الف- پیکربندی و پرس‌وجوی پارامترهای نقطه دسترسی ۸۰۲/۱۱؛

ب- راه‌اندازی امنیت پیوند برای WLAN که از نقطه دسترسی‌های ۸۰۲/۱۱ استفاده می‌کنند. این امر شامل معرفی و شناسایی امن سرویس‌گیرندگان بی‌سیم و افزاره‌های AP می‌شود. هدف، راه‌اندازی و تنظیم ساده‌تر امنیت WLAN برای APهای ۸۰۲/۱۱ و مدیریت اجازه دسترسی WLAN می‌باشد.

۱-۲ مواردی که برای DCP نسخه ۱/۰ هدف نمی‌باشند

موارد کاری زیر به روشنی مورد بحث و بررسی قرار گرفته و خارج از محدوده این نسخه از DCP می‌باشد.

الف- تعویض و افزایش مکانیسم امنیت پیوند که توسط AP فراهم شده است؛

ب- خدمت‌های پیکربندی که برای نقطه دسترسی در شبکه‌های سرمایه گذاری یا hotspotها است.

۱-۳ توصیه‌ها و الزامات امنیت WLAN

امنیت پیوند در شبکه‌های خانگی بی‌سیم، بحرانی است زیرا اتصال توسط سیم‌ها و پورت‌های فیزیکی برقرار نمی‌شود. احتمال تداخل خط مخرب و غیرعمدی توسط حمله‌ها، با مهمتر شدن WLAN افزایش می‌یابد. این امر به ضرر شبکه‌های بی‌سیم بوده، مانع معرفی محصولات و مدل‌های جدید خواهد شد. ارائه دهندگان خدمت و مصرف کنندگان خواستار امنیت پیوند به‌عنوان بخشی از بسته WLAN هستند.

راه حل دیگر برای تامین امنیت پیوند، محافظت منابع خاصی با مکانیسم‌های امنیتی شامل لایه‌های بالاتر پشته نرم‌افزار شبکه است هرچند نمی‌توان از اکثر کاربران خانگی انتظار داشت فهم و اطلاعات تکنیکی داشته باشند و بتوانند تمام نقاط آسیب‌پذیر شبکه خانگی را شناسایی کرده، هرکدام را با روش خاصی رفع کنند.

درحال حاضر متداول‌ترین روش ایمنی پیوندهای ۸۰۲/۱۱ در خانه، شامل تبادل نظر معادل با حریم خصوصی[1] مبنی بر احراز اصالت می‌باشد. ریسک‌های امنیتی در هنگام استفاده از WEP شناخته شده

1- Wired-Equivalent Privacy (WEP)

هستند. حمله کننده می‌تواند کلید WEP را با جمع‌آوری بسته‌ها از طریق packet sniffer بی‌سیم[1]، و اجرای برنامه‌های موجود برای شناسایی کلید WEP، رمزگشایی نماید. اگر مالک WLAN از خطر امنیتی آگاه شود، کلید WEP روی تمام سرویس‌گیرندگان و AP باید به‌روز شود.

برای اطمینان خاطر کاربر و نیز افزایش مصرف برنامه‌های کاربردی بی‌سیم، الزامی است که افزاره‌های WLAN خانگی، از مکانیسم‌های امنیتی قوی‌تری استفاده کنند. همچون WPA که در صنعت ۸۰۲/۱۱ در نظر گرفته شده است. در بلند مدت انتظار می‌رود گروه کاری 802.11i روی خصوصیات امنیت کار کند و راه‌حل‌های مناسب برای مکانیسم‌های امنیتی قوی، روی AP ارائه دهد. توسعه امنیت، احراز اصالت را به ازای هر کاربر، هر کلید جلسه، تغییر کلیدهای متناوب و روش‌هایی مانند استاندارد رمزنگاری قوی‌تر[2]، فراهم می‌آورد.

یکی از موارد اصلی استفاده از امنیت در WLAN فرآیند تنظیم پارامترهای امنیتی است. مکانیسم‌های فعلی برای مقداردهی امنیت پیوندها روی یک افزاره AP زیاد کاربرپسند نیستند. برای مثال در یک مدل مبتنی بر WEP کاربر مجبور است کلید طولانی WEP را برای AP از طریق یک ارتباط سیمی مطمئن و یا یک سرویس‌گیرنده جدید، به درستی بازیابی کند. این مسئله خود در باره راه‌اندازی همچنین در مورد مکانیسم‌هایی که برای توسعه امنیت مبتنی بر WEP ایجاد می‌شوند نیز صادق است. به همین دلیل کاربران مایلند که امنیت را در شبکه خود راه‌اندازی نکنند تا آسیب پذیر نشوند. نظریه مکانیسم مقداردهی امنیت ۸۰۲/۱۱ با استفاده از فن‌آوری UPnP که در این استاندارد مطرح است، به منظور کاهش دخالت کاربر و معرفی مدل کاربرد برای کاربران است تا از مزایای سطح بالای امنیتی که نقاط دسترسی را ارائه می‌دهند، بهره‌مند شوند.

به‌طور کلی، راه‌حل‌های امنیتی باید کاربر را از حملات نفوذگران میانی[3] حفاظت کند. به این ترتیب که سرویس‌گیرندگان، کاربر را از ارتباط با APهای بیگانه و AP کاربر در ارتباط با سرویس‌گیرندگان بیگانه منع می‌کند. همچنین باید با اطمینان یافتن از اینکه تمام پیام‌های بین AP و سرویس‌گیرندگان، معتبر است، از حملات سرقت اطلاعات[4] جلوگیری کند.

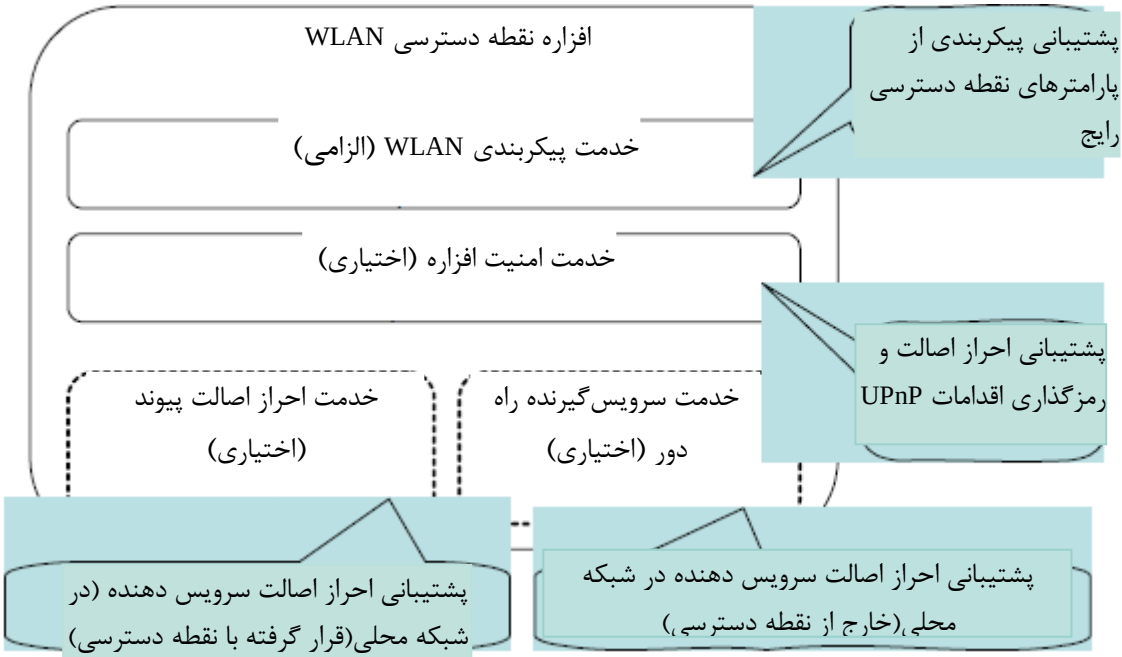
نظریه DCP برای فعال سازی WLAN ایمن با افزاره‌های AP است که عناصر مورد نیاز معرفی شده در DCP را پیاده می‌کند. شکل زیر عمده اجزای عملیاتی افزاره WLANAccessPoint را نشان می‌دهد.

۱- یکی از قدیمی‌ترین روش‌های سرقت اطلاعات در یک شبکه، استفاده از این فرآیند است در این روش مهاجمان از تکنیک‌هایی به منظور تکثیر بسته‌های اطلاعاتی که در طول شبکه حرکت می‌کنند، استفاده نموده و در ادامه با آنالیز از وجود اطلاعات حساس در شبکه آگاهی می‌یابند.

2- Advanced Encryption Standard (AES)

۳- نفوذگران میانی (man in the middle) یا MITM در شبکه نام حمله‌ای است که توسط آن می‌توان، در ارتباط میان دو سامانه تجسس کرد. در این حملات شخص مهاجم مسیر ارتباطی بین دو سامانه را به مسیر دلخواه خود تغییر می‌دهد و به‌راحتی می‌تواند از اطلاعات در حال تبادل میان دو سامانه استفاده کند.

۴- از روش‌های سرقت اطلاعات می‌باشد. (session-hijack)



شکل ۲ – مولفه‌های تابعی از افزاره نقطه دسترسی WLAN

۱-۳-۱ تنظیم پارامترهای AP

خدمت WLANConfiguration خدمتی مورد نیاز برای افزاره WLANAccessPoint است که متغیرهایی را برای برخی پارامترهای نقاط دسترسی تهیه می‌کند که توسط گروه کاری تعیین شده‌اند تا برای تنظیمات از طریق سرویس گیرندگان UPnP مفید واقع شود. آن‌ها قابلیتی را فراهم می‌کنند که امنیت و پارامترهای عملیاتی به راحتی تنظیم شود، اطلاعات تشخیصی را پیشنهاد می‌دهد و قابلیت تکرار را تنظیم می‌کند. به‌علاوه فن‌آوری UPnP قابلیت اطلاع رسانی رخداد برای سرویس‌گیرندگان علاقه‌مند را فراهم می‌کند. نقطه دسترسی که با فن‌آوری UPnP فعال نشده است، کاربران ممکن است به برخی از این پارامترها از طریق جستجوگرهایی که مکانیسم تشخیص هویت و کنترل دسترسی قوی ندارند، دسترسی داشته باشند. همچنین فعالیت‌های پیکربندی که بین آن AP و سرویس‌گیرنده مبادله شده است، از لحاظ محرمانه بودن، امن نیستند و در مقابل حملات آسیب‌پذیرند.

در مورد AP DCP توصیه می‌شود که مکانیسمی وجود داشته باشد که دسترسی به فعالیت‌های UPnP را تصدیق نموده، محرمانگی داده را فراهم نماید. همچنین توصیه می‌شود که مکانیسمی وجود داشته باشد تا مانع دسترسی‌های غیر محرمانه و تصدیق نشده به پارامترهایی شود که تنها از طریق فعالیت‌های UPnP امن قابل دسترسی هستند. بدون وجود چنین کنترل دسترسی، هر افزاره سرویس گیرنده در شبکه محلی می‌تواند تنظیمات AP را تغییر دهد که کل شبکه را تحت تاثیر قرار می‌دهد. سرویس گیرنده که به پیوند امنی دسترسی دارد، لزوماً نمی‌تواند مورد اعتماد قابلیت‌های مدیریت واقع شود. این شرایط مخصوصاً مناسب محیط‌های اداری کوچک می‌باشد. جلوگیری از دسترسی صحیح به پارامترهای AP، پشتیبانی فروشندگان تجهیزات شبکه و ارائه دهندگان خدمت را کاهش می‌دهد.

توصیه می‌شود از فعالیت‌هایی استفاده شود که در خدمت امنیت افزاره برای پیاده‌سازی کنترل دسترسی معرفی شده است. گروه کاری، فعالیت‌های خاصی را در پیکربندی WLAN، LinkAuthentication و RadiusClient service ارائه کرده‌اند که برای ایمن بودن توصیه می‌شود.

۱-۳-۲ پشتیبانی اعتبار

نقطه دسترسی ممکن است قابلیت پشتیبانی تصدیق سرویس گیرندگان یک WLAN منحصر به فرد را با اعتبار منحصر به فرد، داشته باشد. ممکن است این کار را بدون یک سرویس دهنده تشخیص هویت و با استفاده از کلیدهای PSK WPA چندگانه انجام دهد. یا ممکن است این کار را با داشتن اشاره‌گری به سرویس دهنده تشخیص هویت مانند RADIUS که یک افزاره خارجی برای نقطه دسترسی است از طریق متغیرهایی که در خدمت RadiusClient ارائه شده است، انجام دهد. همچنین AP ممکن است عاملیت سرویس دهنده تصدیق را پشتیبانی کند و آن را به عنوان یک خدمت UPnP، مخصوصاً خدمت LinkAuthentication ارائه دهد. این یک خدمت اختیاری است که می‌تواند با AP DCP استفاده شود تا تصدیق per-client را با سرویس دهنده تشخیص هویت مجاور، پشتیبانی کند.
لطفاً برای اطلاعات بیشتر به LinkAuthentication و RadiusClient service مراجعه نمایید.

کلیه بندهای استاندارد بین‌المللی ISO/IEC 29341-8-5: 2008 در مورد این استاندارد، معتبر و الزامی است.