جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران-
ایزو-آی-ای-سی
۱۱-۱۳-۲۹۳۴۱
چاپ اول
۱۳۹۱

INSO-ISO-IEC
29341-13-11
1st. Edition
2012
Identical with
ISO/IEC 29341-13-11:2008

# فناوری اطلاعات- معماری افزاره جامع اتصال و اجرا UPnP-
# قسمت ۱۳-۱۱: پروتکل کنترل امنیت افزاره- خدمت کنسول امنیت

# Information technology – UPnP Device Architecture – Part 13-11: Device Security Device Control Protocol – Security Console Service

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

**کمیسیون فنی تدوین استاندارد**

**«فناوری اطلاعات – معماری افزاره جامع اتصال و اجرا UPNP-**

**قسمت ۱۳-۱۱: پروتکل کنترل امنیت افزاره- خدمت کنسول امنیت»**

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

**دبیر:**

| | |
|---|---|
| خوشقدم، سهیلا<br>(لیسانس مهندسی کامپیوتر) | شرکت ریزفناوران آرکا پژوه |

**اعضاء:** (اسامی به ترتیب حروف الفبا)

| | |
|---|---|
| اصل‌زاد، محمدعلی<br>(لیسانس مهندسی کامپیوتر) | شرکت ریزفناوران آرکاپژوه |
| بدلی افشرد، بابک<br>(فوق لیسانس مهندسی کامپیوتر) | اداره کل استاندارد و تحقیقات صنعتی آذربایجان‌شرقی |
| خاکپور، علی<br>(لیسانس مهندسی کامپیوتر) | شرکت ایران دیتا |
| الهی، بهمن<br>(لیسانس مهندسی مکانیک) | شهرداری تبریز |
| سرسرای، فرناز<br>(لیسانس مکانیک) | شرکت ریزفناوران آرکاپژوه |
| عظیمی حسینی، سارا<br>(لیسانس مهندسی کامپیوتر) | شرکت ریزفناوران آرکاپژوه |
| علیوند، فاطمه<br>(لیسانس مهندسی کامپیوتر) | شرکت ریزفناوران آرکاپژوه |

## پیش‌گفتار

استاندارد «فناوری اطلاعات – معماری افزاره جامع اتصال و اجرا UPnP- قسمت ۱۳-۱۱: پروتکل کنترل کنترل امنیت افزاره- خدمت کنسول امنیت» 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 یکصد و شصت و یکمین اجلاس کمیته ملی استاندارد رایانه و فرآوری داده‌ها مورخ ۹۱/۰۲/۱۲ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات سازمان استاندارد و تحقیقات صنعتی 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 29341-13-11: 2008, Information technology – UPnP Device Architecture – Part 13-11: Device Security Device Control Protocol – Security Console Service.

# فناوری اطلاعات- معماری افزاره جامع اتصال و اجرا UPnP-
# قسمت ۱۳-۱۱: پروتکل کنترل امنیت افزاره- خدمت کنسول امنیت

## ۱ هدف و دامنه کاربرد

این استاندارد ملی، براساس پذیرش استاندارد بین‌المللی ISO/IEC 29341-13-11:2008 تدوین شده است. هدف از تدوین این استاندارد، تعریف خدمت[1] که توسط یک کنسول[2] امنیتی[3] پیشنهاد شده، می‌باشد.

این کنسول امنیتی کاربر واسطی[4] را برای مدیریت کنترل دسترسی به افزاره‌های جامع اتصال و اجرا[5] امنیتی امنیتی آگاه، پیشنهاد می‌کند. (برای توصیف اقدامات مورد استفاده در ایجاد و ویرایش فهرست‌های کنترل دسترسی[6] و گرفتن مالکیت امنیتی افزاره‌ها به امنیت افزاره ۱ مراجعه شود) چنان‌که افزاره کنسول امنیتی متعلق به خود است. در صورتی که کاربر به هرگونه اقدامات کنترل شده دسترسی داشته باشد در آن صورت این اقدامات توسط کاربران انسانی مدیریت می‌شود نه اینکه توسط برخی دیگر از کنسول‌های امنیتی مدیریت شود. بنابراین یک کنسول امنیتی نیازمند یک خدمت امنیت افزاره نمی‌باشد و دارای حافظه نهان گواهی شده می‌باشد اما به‌جای یک حافظه نهان داخلی دارای یک حافظه نهان خارجی است.

شبکه ایجاد شده از خود مؤلفه‌های کاربران، هیچ اتصالی با دامنه کاربران شخصی خارجی ندارد و تاکنون هیچ نقطه کنترلی به کسی غیر از کاربر شبکه‌ای که نیازمند ویژگی‌های امنیتی اتصال و اجرا می‌باشد، متصل نشده است. ازقبل جداسازی شبکه، سطحی از امنیت فیزیکی را حاصل کرده است. ما نگران امنیت اتصال و اجرای شبکه در بیشتر نقاط کنترل کاربران خودی هستیم که بر روی شبکه فیزیکی ارائه شده‌اند و رسیدن به افزاره‌های کاربر را با پیام فعال کرده‌اند. این شرایط می‌تواند شامل موارد زیر باشد:

۱- استفاده از شبکه‌بندی بی‌سیم، خط نیرو یا مودم کابلی بدون فایروال[7] به مهاجم این اجازه را می‌دهد تا بدون اجازه کاربر یا بدون اطلاع او به شبکه ملحق شود؛

۲- زیرساخت‌های شبکه مشترک، از قبیل خوابگاه دانشگاه یا یک ساختمان حکومتی مشترک سیمی برای اترنت به عنوان یک بخش شبکه به بیش از یک نفر ساکن، خدمت رسانی می‌کند؛

---

1- Service
2-Console
3-Security Console (SC)
4-Interface
5- Universal Plug and Play (UPnP)
6- Access Control Lists (ACL)
7- Firewall

۳- خانواده‌ها از افراد مختلف یا نوجوانان هستند که در آن هر فرد می‌خواهد یک دامنه امنیتی خصوصی ایجاد نماید. علاوه بر این در هر دامنه از افزاره‌ها یا نقاط کنترل مشترک در میان آن‌ها از دامنه شبکه مشترک استفاده می‌کنند؛

۴- اتصال به اینترنت توسط افزاره‌ها یا خدمات که بخش شبکه واحدی از مشترکین متعدد را که به عنوان یک اثر جانبی اتصال به شبکه را ارائه می‌دهند، ایجاد می‌کند. (مانند برخی از مودم‌های کابلی و برخی از اتصالات فراهم کننده خدمت اینترنت)[۱] ؛

۵- خانواده‌هایی که در آن مهمان‌ها ممکن است افزاره تلفن همراه یا به طور موقت نقاط کنترلی درون شبکه را داشته باشند.

در چنین شبکه‌هایی از اشتراک‌گذاری عمومی و اتفاقی نمی‌توان بر امنیت شبکه فیزیکی جهت حفظ افزاره‌ها یا روش‌های کشف (برای مثال پروتکل کشف خدمت ساده چند پخشی)[۲] برای کامپایل فهرستی از "افزاه‌های من[۳]" یا "نقاط کنترل من[۴]" تکیه کرد. این برگ‌ها تا حدی کاربر را به صورت دستی برای افزاره‌های قابل دسترس فیزیکی و نقاط کنترل انتخاب می‌کند، انتخاب کسانی که علاقه به کاربری دارند. یکی از توابع اصلی از کنسول امنیتی، فعال کردن کاربر برای انتخاب است. این فرآیند نیازمند دو عملیاتی است که در طرح اصلی از اتصال و اجرا پیش بینی نشده است.

۱- کشف نقاط کنترل و

۲- نام‌گذاری افزاره‌ها و نقاط کنترلی براساس هر کاربر.

اقدامات فراهم شده در این خدمت اجازه انجام دو تابع را به کنسول امنیتی می‌دهد.

علاوه بر این برخی اوقات اشتراک گذاری افزاره در سراسر دامنه امنیتی برای استفاده از تصدیق‌های[۵] مجاز با عنوان بندهای توصیف شده در ۱-۱-۳ و ۳-۳ فراخوانی می‌شوند. این خدمت اقداماتی برای تحویل گواهینامه‌ها (یا زنجیره‌های گواهینامه) (به بند ۲-۵-۳ مراجعه کنید) و برای ابطال گواهینامه (از طریق تکرار)(به بند ۲-۵-۴ مراجعه کنید) فراهم می‌کند.

### ۱-۱ اقدامات کنسول امنیتی

1- Internet Service Provider (ISP)
2- Simple Service Discovery Protocol (SSDP)
3-My Devices
4-My Control Points
5-Authorizationes

موقعی که کنسول امنیتی با افزاره امنیتی آگاه در تعامل است از طریق اقدامات ارائه شده توسط افـزاره انجـام می‌پذیرد. با این حال کنسول امنیتی باید با نقاط کنترل[1] در تعامل باشد. در عوض نقاط کنترلـی اجبـاری بـه افزاره تبدیل می‌شود، جهت پشتیبانی از این تعاملات، اقداماتی را که کنسـول امنیتـی ارائـه مـی‌دهـد تعریـف می‌کنیم. این اقدامات از این خدمت در سه بخش عملکردی می‌باشد:

۱- کشف نقاط کنترل؛

۲- ارتباط با فرهنگ لغت نام محلی؛

۳- فرآیند گواهینامه.

### ۱-۱-۱ کشف نقاط کنترل

نسخه 1.0 معماری افزاره جامع اتصال و اجرا شامل پروتکل کشف خدمت ساده برای کشـف افـزاره‌هـا توسـط نقاط کنترلی می‌باشد. با این حال هیچ پروتکلی برای کشف نقاط کنترل توسط دیگر نقاط کنترل یا افزاره‌هـا، وجود ندارد.

کنسول امنیتی نیازمند کشف نقاط کنترل می‌باشد به‌طوری‌که بتواند کسانی را که در دامنه امنیتی محلی حق دسترسی به افزاره را دارند، شناسایی کند.

ما به این کشف توسط برگرداندن منطق کشف اتصال و اجرا دست یافته‌ایم. یک نقطه کنترل آگاه امنیتی یـک کنسول امنیتی که اقدام Presentkey را ارائه می‌دهد، کشف خواهد کرد و سپس عمـل فراخـوانی خـود را بـه کنسول امنیتی اعلام خواهد کرد. از آنجا که نقاط کنترل ممکن است در دامنه امنیتی چندگانه عمل کند باید خود را به هر کنسول امنیتی که آن را تشخیص می‌دهد اعلام کند. عمل اعلام، به معنـی دریافـت هـر حقـی توسط کاربر باشد چون واگذاری حقوق، بیان کننده تصمیم کاربر می‌باشـد. بـا ایـن حـال یـک نقطـه کنتـرل نمی‌تواند از قبل تشخیص دهد که آیا یک کنسول امنیتی خاص برای واگذاری برخـی حقـوق انتخـاب خواهـد شد، بنابراین باید خود را به همه کنسول‌های امنیتی اعلام کند.

### ۱-۱-۲ ارتباط با فرهنگ لغت محلی

یکی از عملکردهای اصلی کنسول امنیتی، شناسایی افزاره‌ها و نقاط کنترل در شبکه محلی کاربر می‌باشد. در حداقل یک پیاده‌سازی از کنسول امنیتی، این فرآیند شامل اجازه کاربر به واگذاری انتخاب نام کاربری خـود (نام‌های محلی) به افزاره‌ها و نقاط کنترلی می‌باشد. از آنجا که افزاره‌ها و نقاط کنترل ممکن است قابل دیدن باشند (به‌دلیل نام)، دامنه امنیتی مختلف، توسط کاربران مختلـف یـک افـزاره واحـد یـا نقـاط کنترلـی کـه می‌توانند شامل چندین نام محلی باشند، انجام می‌شوند. بنابراین این اسامی ویژگی کاربر باقی مـی‌مانـد (بـه

6-Control Points (CPs)

طور خاص از کنسول امنیتی) به‌جای این‌که نام افزاره یا نقاط کنترل خود باقی بماند. به طور معمول آن‌ها در داخل ساکن خواهند بود و از کنسول امنیتی منتشر نمی‌شوند.

به‌عنوان مثال، اشتراک گذاری یک شبکه در یک محل با دو نفر کاربر را در نظر بگیرید. هر یک دارای دامنه شخصی از افزاره جامع اتصال و اجرا و نقاط کنترل می‌باشند اما برخی مولفه‌ها بین آن‌ها به اشتراک گذاشته شده است. یک افزاره مشترک بایگانی عکس‌های دیجیتالی شخص یک می‌باشد. شخص یک به آن توسط نام "عکس" مراجعه می‌کند در حالی‌که شخص دو نام "بایگانی عکس فوری شخص یک" را به آن داده است. هیچ کدام از اسامی متناسب با برتری کاربر دیگر نیست بنابراین هیچ نامی به عنوان نام دوستانه منحصر به فرد برای افزاره مشترک مناسب نیست در همین حال افزاره بایگانی توسط یک نام منحصر به‌فرد در شبکه مانند DE7Z-GVGK-QTYR-TWPO-YF54-GB4M-OGFH-XJYM شناخته شده که هیچ کاربری نمی‌خواهد با آن کار کند. نگاشت نام دوستانه به نام منحصر به‌فرد تابعی از رابط کاربر برای هر کاربر است (کنسول امنیتی در این مورد) در اینجا نگاشت به فرهنگ لغت محلی مراجعه می‌کند.

### ۱-۱-۳ فرآیند گواهینامه

کنسول امنیتی برای اعطای حقوق دسترسی به افزاره های تحت کنترل خود مسئول است. اگر یک افزاره در میان دامنه های متعدد به اشتراک گذاشته شود کنسول امنیتی متعدد وجود خواهد داشت که نیازمند اعطای حقوق در آن افزاره می‌باشد این اشتراک گذاری حقوق برای اعطای دسترسی می‌تواند از طریق مشارکت حاصل شود (اعطای مالکیت در امنیت افزاره: ۱) اما یک مالک مشترک تمام دسترسی به افزاره را دارد و در میان دیگر موارد قادر به از بین بردن حقوق دسترسی از اولین مالک از جمله وضعیت مالکیت می‌باشد در صورتی که برخی از کنسول‌های امنیتی قدرت اشتراک‌گذاری بیش از حدی داشته باشند می‌توانند مجوزهایی از طریق فهرست کنترلی افزاره را درست مثل هر نقطه کنترل اعطا نمایند. در این مورد کنسول امنیتی با اضافه کردن ورودی‌های فهرست کنترل دسترسی[1]، حقوقی را به نقاط کنترل (یا دیگر کنسول‌های امنیتی) اعطا نخواهد نمود پس حق ویرایش فهرست کنترل دسترسی را ندارد مگر از طریق گواهینامه‌های مجاز (به افزاره امنیت ۱: برای تعریفی از گواهی نامه‌های مجاز مراجعه نمایید).

ممکن است یک کنسول امنیتی مالکیت یک افزاره و همچنین اعطای حقوق با گواهینامه را نیز داشته باشد برای مثال در صورتی که افزاره ذخیره‌سازی بیش از حد برای یک فهرست کنترل دسترسی کوچک باشد یا افزاره در زمان روی خط نبودن، حق دسترسی داشته باشد نیازمند اعطا می‌شود. گواهینامه مجاز شبیه یک ورودی فهرست کنترل دسترسی است اما امضای دیجیتالی شده و شامل یک صادر کننده مشخصات افزاره است که به آن اعمال می‌شود و احتمالا شامل یک تاریخ انقضاء و زمان می‌باشد. دو اقدام وجود دارد که در اینجا به منظور تسهیل فرایند گواهینامه ارائه شده است:

1- Access Control List (ACL)

۱- به‌دست آوردن گواهینامه: که به عنوان یک مکانیسم اداره پست اجازه می‌دهد یک نقطه کنترل یا کنسول امنیتی دیگر گواهینامه‌ها را که توسط کنسول امنیتی صادر شده واکشی نماید (این عمل توسط رویدادهای متغیر، لیست انتظار نقاط کنترلی توسط هر نقطه کنترلی یا کنسول امنیتی دیگر پشتیبانی می‌شود)

۲- تمدید گواهینامه: توسط یک نقطه کنترل می‌تواند یک نسخه به‌روز شده از یک گواهینامه منقضی شده (یا به زودی منقضی خواهد شد)را برای کسب جزئیات بیشتر در خواست نماید. در مورد بازسازی به بند ۳ تئوری عمل مراجعه نمایید.

اگرچه به‌دست آوردن گواهینامه یک مکانیسم ارتباطی برای گواهینامه می‌باشد اما مانع مکانیسم‌های ارتباطی دیگر برای برنامه های کاربردی کنسول امنیتی پیاده‌سازی شده نمی‌شود. برای مثال ممکن است از پست الکترونیکی، sneaker-net، برخی خدمات دایرکتوری یا HTTP برای این توابع ارتباط استفاده نماید. در یک شبکه واقعا پیچیده با تعداد زیادی از گواهینامه‌ها یک خدمت دایرکتوری هوشمند به نقطه کنترل دقیقا زنجیره گواهینامه که نیازمند دسترسی به یک عمل خاص در یک افزاره می‌باشد را بر می‌گرداند، این موارد برنامه‌های کاربردی طراحی مسائل و خارج از محدوده این خصوصیات پروتکل می‌باشد. به‌دست آوردن گواهینامه به عنوان مشتق کننده مشترک جهت حصول اطمینان از قابلیت همکاری می‌باشد (با فرض مولفه هایی که حداقل گاهی اوقات در یک شبکه اشتراک گذاشته شده‌اند).

کلیه بندهای استاندارد بین‌المللی ISO/IEC 29341-13-11:2008 در مورد این استاندارد، معتبر و الزامی است.