INSO-ISO-IEC

24767-2

1st. Edition

Identical with
ISO/IEC 24767-2: 2009
2012

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

استاندارد ایران- ایزو آی ای سی

۲۴۷۶۷-۲

چاپ اول

۱۳۹۰

فن‌آوری اطلاعات- امنیت شبکه خانگی
قسمت ۲: خدمات امنیت داخلی- پروتکل ارتباطی امن برای میان افزار (SCPM)

Information technology – Home network security
Part 2: Internal security services – Secure communication protocol for middleware (SCPM)

ICS:35.110;35.200;35.240.99

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 رسمی‌کشور 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 جهت اجرا ابلاغ شده است.

تدوین استاندارد در حوزه های مختلف در کمیسیون‌های فنی مرکب از کارشناسان مؤسسه* صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود وکوششی 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 می‌شود .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 می‌شود.

پیش نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذیصلاح 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 می‌شود که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان استاندارد تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد[1] (ISO) 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 می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، 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 می‌تواند 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 سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، مؤسسهٔ استاندارد این گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. 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 Electro technical Commission
3-International Organization for Legal Metrology (Organization International de Metrologie Legal)
4-Contact point
5-Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد
" فن‌آوری اطلاعات – امنیت شبکه خانگی-
قسمت ۲: خدمات امنیت داخلی- پروتکل ارتباطی امن برای میان افزار (SCPM)"

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
بدلی افشرد، بابک (فوق لیسانس مهندسی کامپیوتر)	اداره کل استاندارد استان آذربایجان شرقی
بدلی افشرد، محمدرضا (فوق لیسانس مهندسی برق)	نیروگاه حرارتی تبریز
خاکپور، علی (لیسانس مهندسی کامپیوتر)	شرکت ایران دیتا
رحمانی، نعیم (فوق لیسانس مهندسی کامپیوتر)	شرکت پیشگامان ارتباط کهکشان
عظیمی حسینی، سارا (لیسانس مهندسی کامپیوتر)	شرکت ریزفناوران آرکاپژوه

علیوند شاهگلی، فاطمه
(لیسانس مهندسی کامپیوتر)
شرکت ریزفناوران آرکاپژوه

میکائیلی، هادی
(فوق لیسانس مهندسی کامپیوتر)
دانشگاه آزاد اسلامی شبستر

پیش‌گفتار

استاندارد" فن‌آوری اطلاعات – امنیت شبکه خانگی-قسمت ۲: خدمات امنیت داخلی- پروتکل ارتباطی امن برای میان افزار (SCPM)" که پیش‌نویس آن در کمیسیون فنی مربوط، توسط شرکت ریزفناوران آرکاپژوه 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 پنجاه و نهمین اجلاسیه کمیته ملی استاندارد رایانه و فرآوری داده مورخ ۹۰/۱۲/۰۹ 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 تجدید نظر 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 24767-2: 2009, Information technology – Home network security- Part 2: Internal security services – Secure communication protocol for middleware (SCPM).

فن‌آوری اطلاعات- امنیت شبکه خانگی-قسمت ۲: خدمات امنیت داخلی- پروتکل ارتباطی امن برای میان‌افزار (SCPM)

۱ هدف و دامنه کاربرد

این استاندارد ملی، براساس پذیرش استاندارد بین‌المللی ISO/IEC 27767-2:2009 تدوین شده است.

هدف از تدوین این استاندارد، تعیین امنیت برای شبکه خانگی برای تجهیزاتی است که با قابلیت‌های فن‌آوری اطلاعات محدود است.

این استاندارد امنیت را در یک شبکه خانگی برای تجهیزاتی با قابلیت فن‌آوری اطلاعات محدود، مشخص می‌کند. پروتکل ارتباطی امن برای میان افزار (SCPM)[1] به‌ویژه برای پشتیبانی از ایمنی شبکه آن دسته از تجهیزاتی طراحی شده است (به بند ۵-۲ مراجعه کنید) که قابلیت پشتیبانی پروتکل‌های امنیت شبکه مانند IPSec یا SSL/TLS را ندارند. اگرچه این پروتکل برای انتقال ناامن طراحی شده اما این امکان وجود دارد که برای سایر انواع انتقال نیز مورد استفاده قرار گیرد. البته، سطح کیفیت خدمات امنیتی SCPM برابر با سطح کیفیت پروتکل‌های امنیتی اینترنت نیست اما تضمین خواهد کرد که چنین میان‌افزاری می‌تواند به‌طور امن درون خانه متصل شود. هدف مورد نظر این نیست که SCPM جایگزین مکانیسم‌های ایمنی موجود پروتکل‌هایی شود که قبلاً انتشار یافته‌اند.

SCPM خدمات امنیتی را در لایه شبکه فراهم می‌کند و این پروتکل وابسته به هیچ انتقال رسانه‌ای خاصی نمی‌باشد، این استاندارد شامل مشخصات مفصل خدمات امنیتی پشتیبانی شده، قالب‌های پیام ضروری، جریان اطلاعات و پردازش بخش‌های مربوط به اطلاعات ضروری جهت پیاده‌سازی این پروتکل می‌باشد.

بنابراین این استاندارد به مسائل وابسته به رسانه‌ها و به معماری امنیتی کلی وابسته نیست، بلکه هر نوع فن‌آوری شبکه خانگی را تحت پوشش قرار می‌دهد. پروتکل مشخص شده در این استاندارد مستقل از رسانه‌ها است و خدمات امنیتی لایه شبکه را برای پروتکل‌هایی که تداخلی[2] با طرحواره[3] آدرس‌دهی لایه شبکه ندارند تحت پوشش قرار می‌دهد. خدمات امنیت لایه شبکه از طریق استفاده از ترکیب رمزنگاری و راهکارهای امنیتی فراهم می‌شوند.

هر پروتکلی موظف است جزئیات پیاده‌سازی امنیتی را مشخص کند. یک سامانه HES که بیش از یک پروتکل را پشتیبانی می‌کند، به یک دروازه در میان پروتکل‌ها نیاز دارد.

در نهایت، این استاندارد هیچ نوع برنامه کاربردی را تعریف نمی‌کند به استثنای مدیریت کلیدی که در هر خدمت امنیتی ضروری می‌باشد. علاوه بر این، محدودیت‌هایی بر روی انواع برنامه‌های کاربردهای که با SCPM مستقر شده‌اند، وجود ندارد.

1- Secure Communication Protocol
2- Conflicting
3- Scheme

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی به آن‌ها ارجاع داده شده است. بدین‌ترتیب آن مقررات جزئی از این استاندارد محسوب می‌شود.

درصورتی‌که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر 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 آن مورد نظر است.

استفاده از مراجع زیر برای کاربرد استاندارد الزامی است:

2-1 ISO/IEC 10116, Information technology – Security techniques – Modes of operation for an nbit block cipher.

2-2 ISO/IEC 11577, Information technology – Open Systems Interconnection – Network layer security protocol

2-3 ISO/IEC 11770-3, Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques.

2-4 ISO/IEC 18033-3, Information technology –Security techniques–Encryption algorithms- Part 3: Block ciphers**.**

کلیه بندهای استاندارد بین‌المللی ISO/IEC 24767-2:2009 در مورد این استاندارد، معتبر و الزامی است.