INSO
18719
1st. Edition
2014

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

استاندارد ملی ایران
۱۸۷۱۹
چاپ اول
۱۳۹۳

فناوری اطلاعات- شناسایی و مدیریت اقلام سیار- پروتکل حفظ حریم مصرف‌کننده برای خدمات شناسایی بسامد رادیویی (RFID) سیار

Information technology – Mobile item identification and management – Consumer privacy-protection protocol for Mobile RFID services

ICS: 35.040

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 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- شناسایی و مدیریت اقلام سیار- پروتکل حفظ حریم مصرف‌کننده برای خدمات شناسایی بسامد رادیویی (RFID) سیار»

رئیس:	**سمت و / یا نمایندگی**
مشرف، بهنوش (فوق لیسانس مهندسی فناوری اطلاعات- شبکه‌های کامپیوتری)	کارشناس استاندارد – کارشناس پایگاه‌داده شرکت برق منطقه‌ای هرمزگان
دبیر:	
ترابی ، مهرنوش (فوق لیسانس مهندسی فناوری اطلاعات – تجارت الکترونیک)	کارشناس استاندارد- کارشناس تجزیه و تحلیل سیستم شرکت برق منطقه‌ای هرمزگان
اعضاء: (اسامی به ترتیب حروف الفبا)	
احمدی، محمد (فوق لیسانس مهندسی برق- مخابرات)	کارشناس استاندارد- کارشناس فیبرنوری شرکت برق منطقه‌ای هرمزگان
ذاکری، صفورا (فوق لیسانس مهندسی کامپیوتر- نرم‌افزار)	عضو هیات علمی دانشگاه آزاد اسلامی بندرعباس
زمانی ، کرشنا (فوق لیسانس مهندسی فناوری اطلاعات – تجارت الکترونیک)	کارشناس مرکز رایانه دانشگاه مازندران
شایسته، محمد (فوق لیسانس مهندسی کامپیوتر- نرم‌افزار)	عضو هیات علمی دانشگاه آزاد اسلامی بندرعباس
صداقت، وجیهه (لیسانس مترجمی زبان)	کارشناس ارشد آموزش برق منطقه‌ای هرمزگان
قاسمی‌زاده، صدیقه (لیسانس مهندسی کامپیوتر- نرم‌افزار)	کارشناس شبکه برق منطقه‌ای هرمزگان
مومنی، حمیدرضا (فوق لیسانس مهندسی کامپیوتر- هوش مصنوعی)	عضو هیات علمی دانشگاه تنکابن

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد «فناوری اطلاعات- شناسایی و مدیریت اقلام سیار- پروتکل حفظ حریم مصرف‌کننده برای خدمات شناسایی بسامد رادیویی (RFID) سیار» که پیش نویس آن در کمیسیون فنی مربوط، توسط سازمان ملی استاندارد ایران، تهیه و تدوین شده و در سیصدوپنجاهمین اجلاسیه کمیته ملی استاندارد رایانه و فرآوری داده مورخ ۹۳/۸/۱۹ مورد تصویب قرار گرفته است اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران مصوب بهمن ماه ۱۳۷۱ به عنوان استاندارد ملی منتشر می شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهند شد و هر گونه 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 تجدیدنظر استانداردهای ملی استفاده کرد.

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

ISO/IEC 29176:2011, Information technology – Mobile item identification and management – Consumer privacy-protection protocol for Mobile RFID services

فناوری اطلاعات- شناسایی و مدیریت اقلام سیار- پروتکل حفظ حریم مصرف‌کننده برای خدمات شناسایی بسامد رادیویی (RFID)[1] سیار

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین پروتکل حفظ حریم مصرف‌کننده برای خدمات RFID سیار می‌باشد. این استاندارد، راه‌حل فنی برای شرح حریم مرتبط با اقلام برچسب‌گذاری‌شده برای مصرف‌کنندگان فراهم می‌کند.

این استاندارد، در رابطه با ارتباطات برچسب- به- بازجو[2] به منظور فراهم‌آوری راه‌حل حفظ حریم مصرف‌کننده، متمرکز است. این استاندارد برای موضوعات امنیت سامانه بازجو- به- میزبان[3] و میزبان (سازمان پشتیبان[4]) کاربرد ندارد.

۲ تطابق

این استاندارد برای استفاده مرتبط با سایر استانداردهای مربوط به خدمات RFID سیار درنظرگرفته‌شده است. این استاندارد برای برچسب‌ها و بازجوهای منطبق بر استانداردهای ISO/IEC 18000-6 Type C و ISO/IEC 18000-3 MODE 3 RFID به‌کار می‌رود. همچنین برای برچسب‌ها و بازجوهای مناسب و عملی که در واسطهای هوایی استانداردهای ISO/IEC 18000-6 Type C و ISO/IEC 18000-3 MODE 3 RFID پوشش داده نشده هم کاربرد دارد.

۳ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب می‌شود. در صورتی‌که 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 مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

2-1 ISO/IEC 18000-3, Information technology — Radio frequency identification for item management — Part 3: Parameters for air interface communications at 13,56 MHz

2-2 ISO/IEC 18000-6, Information technology — Radio frequency identification for item management — Part 6: Parameters for air interface communications at 860 MHz to 960 MHz

---

1 - Radio Frequency Identification
2- Tag-to-interrogator
3- Interrogator-to-host
4- Back-end Enterprise

2-3 ISO/IEC 19762 (all parts), Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary
2-4 ISO/IEC 29172, Information technology — Mobile item identification and management — Reference architecture for Mobile AIDC services

۴ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف زیر به‌کار می‌رود:

۴-۱ مخفی‌کردن با کدبندی[۱]

روشی است که بازجو، اطلاعات انتقالی به برچسب را مخفی می‌کند؛ این کار را به‌وسیله درخواست عدد تصادفی از برچسب انجام می‌دهد؛ سپس عمل EXOR بیت به بیت[۲] داده یا اسم‌رمز[۳] با عدد تصادفی دریافتی انجام می‌دهد و در نهایت رشته مخفی‌شده با کدبندی[۴] (که متن رمز[۵] نیز نامیده می‌شود) را به برچسب منتقل می‌کند. برچسب، داده یا اسم‌رمز را با به‌کارگیری EXOR بر روی رشته مخفی‌شده با کدبندی دریافتی با عدد تصادفی اصلی از حالت مخفی خارج می‌کند.
[ISO/IEC 18000-6]

یادآوری- بازجو برای مخفی کردن کدبندی شناسایی اقلام سیار کدگذاری‌شده (EMII)[۶]، عمل XOR بیت به بیت EMII را با با اطلاعات ورودی انجام می‌دهد و برای خارج کردن EMII از حالت مخفی، عمل XOR بیت به بیت EMII مخفی‌شده با کدبندی با همان اطلاعات ورودی انجام می‌دهد.

۴-۲ پایانه RFID سیار[۷]

افزاره الکترونیکی مجهز به یک یا چند بازجوی RFID سیار که فناوری‌های کارکردهای شناسایی و مدیریت اقلام سیار (MIIM)[۸] را پشتیبانی می‌کند.

۵ پیش‌زمینه

۵-۱ مدل مرجع برای حفظ حریم مصرف‌کننده

این استاندارد اقدامات مصرف‌کننده مانند خریداری برخی از اقلام پرچسب‌دار را به‌عنوان مدل مرجع درنظر می‌گیرد. شکل ۱ مثالی از خواندن اطلاعات از برچسب کم‌هزینه مصرف‌کننده را شرح می‌دهد. در این مدل مرجع با استفاده از استانداردهای ISO/IEC 18000-6 Type C یا ISO/IEC 18000-3 MODE 3 tags، حافظه شناسانه اقلام منحصر به فرد (UII)[۹]، حافظه شناسانه برچسب (TID)[۱۰] و حافظه User به راحتی به

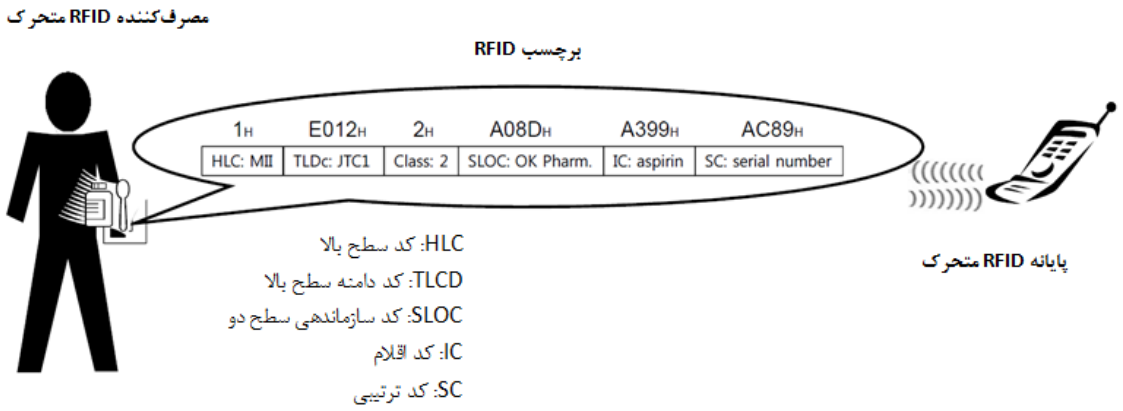
1 - Cover-coding
2- Bit-wise
3- Password
4- Cover-coded
5- Ciphertext
6- Encoded Mobile Item Identification
7 - Mobile RFID Terminal
8- Mobile Item Identification and Management
9- Unique Item Identifier
10- Tag Identifier

پایانه های RFID منطبق با این استاندارد، اعلام شده‌اند. توجه داشته باشید که TID بدون تغییر باقی می‌ماند.

مشکلات حریم مصرف‌کننده که ناشی از این داده حافظه اعلام‌شده است به شرح زیر در استاندارد ITU-T X.1171 تجزیه و تحلیل شده است (برای جزئیات بیشتر به فصل ۹ استاندارد ITU-T X.1171 مراجعه شود):

۱) فاش شدن اطلاعات مربوط به شناسانه

۲) فاش شدن داده زمینه تاریخی



شکل ۱- مدل مرجع برای حفظ حریم مصرف‌کننده

۵-۲ پیش‌نیازها

شرایط زیر پیش‌نیازهای تعریف پروتکل حفظ حریم مصرف‌کننده برای این استاندارد هستند.

۱) برچسب باید فرمان Access از استانداردهای ISO/IEC 18000-6 Type C یا ISO/IEC 18000-3 MODE 3 را پشتیبانی کند.

- اگر برچسب، فرمان Access را پشتیبانی نکند، برچسب نباید برای اجرای پروتکل حفظ حریم مصرف‌کننده این استاندارد استفاده کند.

۲) برچسب باید اسم‌رمز دسترسی با مقدار غیرصفر پشتیبانی کند.

- اگر برچسب، اسم‌رمز دسترسی با مقدار غیرصفر را پشتیبانی نکند، برچسب نباید برای اجرای پروتکل حفظ حریم مصرف‌کننده این استاندارد استفاده کند.

۳) پروتکل حفظ حریم مصرف‌کننده از سایر روش‌های امن‌سازی برچسب RFID ممانعت نمی‌کند.

۶ پروتکل حفظ حریم مصرف‌کننده

۶-۱ هدف

هدف از پروتکل حفظ حریم مصرف‌کننده مخفی‌کردن EMII اصلی[1] است. پروتکل حفظ حریم مصرف‌کننده شامل ۵ مرحله است: ۱) انتقال به وضعیت امن، ۲) اکتساب اسم‌رمز دسترسی اصلی، ۳) تولید اسم‌رمز

1- Original EMII

دسترسی مصرف‌کننده و مخفی‌کردن کدبندی EMII ۴) به‌روزرسانی بانک‌های حافظه و ۵) قفل‌کردن بانک‌های حافظه

۶-۲ مرحله ۱. انتقال به وضعیت امن

اولین مرحله مربوط به اقداماتی است که بلافاصله بعد از خریداری اقلام برچسب‌گذاری‌شده است. هدف این مرحله، گذر برچسب به وضعیت امن است. این استاندارد دو مورد راجع‌به اسم‌رمز دسترسی به برچسب درنظر می‌گیرد. اولی اسم‌رمز دسترسی با همه مقادیر صفر هنگام خرید است و دیگری مقدار اسم‌رمز دسترسی غیرصفر هنگام خرید است.

هنگامی‌که اسم‌رمز دسترسی، با همه مقادیرصفر است، برچسبی که در وضعیت تصدیق‌شده قرار دارد، پس از دریافت فرمان Req_RN معتبر می‌تواند به وضعیت امن انتقال یابد. بنابراین، پایانه RFID سیار مصرف‌کننده می‌تواند اسم‌رمز دسترسی جدید را در فیلد Access Passwd از بانک حافظه Reserved از برچسب، بنویسد (به زیربند ۹-۳-۲-۱ با عنوان Tag Memory از استاندارد ISO/IEC 18000-6:2010 مراجعه شود). در این مورد، مرحله دوم، اکتساب اسم‌رمز دسترسی اصلی، ممکن است نادیده گرفته شود زیرا اسم‌رمز دسترسی با همه مقادیرصفر، مقدار پیش‌فرض در این استاندارد است.

هنگامی‌که اسم‌رمز دسترسی غیرصفر است، برچسب برای گذر به حالت امن، باید از فرمان Access با اسم‌رمز دسترسی معتبر استفاده کند. بنابراین، پایانه RFID سیار مصرف‌کننده باید برای به‌دست‌آوردن اسم‌رمز دسترسی اصلی به مرحله بعد برود.

۶-۳ مرحله ۲. اکتساب اسم‌رمز دسترسی اصلی

دومین مرحله، به‌دست‌آوردن اسم‌رمز دسترسی اصلی برچسب است. سازوکار انتقال اسم‌رمز دسترسی از رایانه میزبان یا کارساز[1] مدیریت کلیدی، خارج از دامنه کاربرد این استاندارد است.

این استاندارد فرض را بر این می‌گذارد که اسم‌رمز دسترسی برچسب به پایانه RFID سیار مصرف‌کننده به‌طور امن منتقل می‌شود.

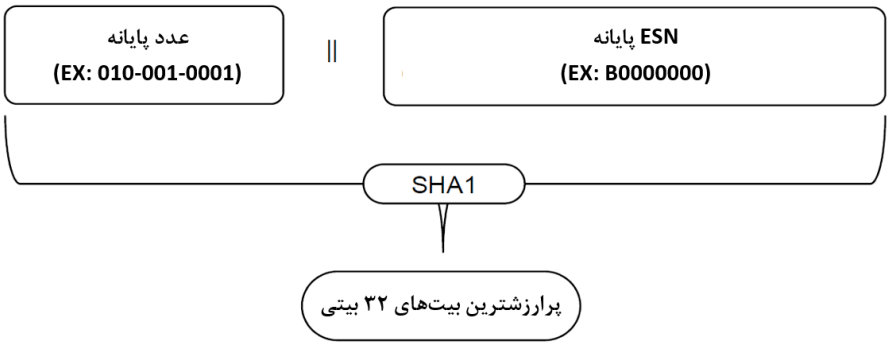
۶-۴ مرحله ۳. تولید اسم‌رمز دسترسی مصرف‌کننده و مخفی‌کردن کدبندی EMII

در مرحله سوم، پایانه RFID سیار مصرف‌کننده اسم‌رمز دسترسی خود را تولید و EMII را با کدبندی مخفی می‌کند. این استاندارد، سه روش تولید اسم‌رمز دسترسی را فراهم می‌کند.

یکی از روش‌ها، استفاده از شماره پایانه RFID سیار و شناسانه افزاره سیار پایانه است. شماره پایانه RFID سیار نمونه، شماره تلفن استاندارد ITU-T E.164 است و شناسانه‌های افزاره سیار نمونه، شماره ترتیبی الکترونیکی (ESN)[2]، شناسانه تجهیزات سیار (MEID)[3] و هویت بین‌المللی تجهیزات سیار (IMEI)[4] است. در مورد تلفن سیار 2G CDMA ، شماره تلفن ۰۱۰۱۲۳۴۵۶۷۸ می‌تواند مثالی از شماره پایانه باشد و ESN از B0000000 می‌تواند مثالی از شناسانه افزاره سیار باشد.

1- Server
2- Electronic Serial Number
3- Mobile Equipment Identifier
4- International Mobile Equipment Identity

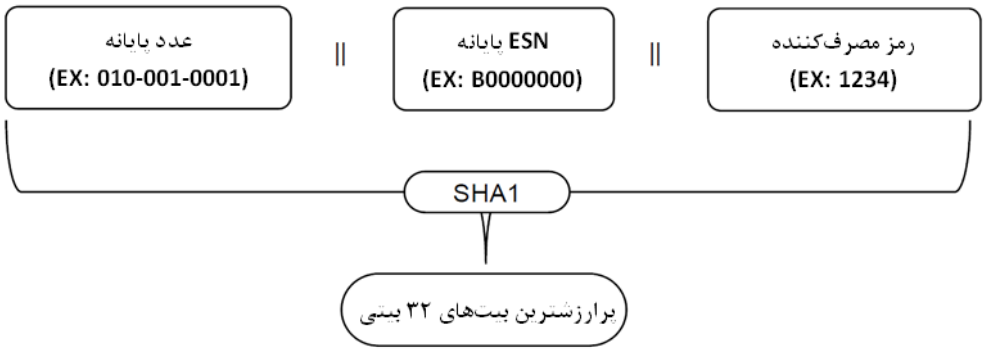
شکل ۲ روش تولید اسم‌رمز دسترسی مصرف‌کننده را نشان می‌دهد. ویژگی اصلی این روش این است که اسم‌رمز دسترسی به‌طور خودکار و بدون مداخله مصرف‌کننده به‌دست آمده است. برنامه شروع RFID سیار، الگوریتم چکیده‌سازی امن۱ (SHA1)[1] را انجام می‌دهد و پرارزش‌ترین بیت‌ها (MSB)[2]ی ۳۲ بیتی را به‌عنوان اسم‌رمز دسترسی انتخاب می‌کند. برنامه شروع RFID سیار، برنامه کاربردی ویژه‌ای است که کاربر نهایی پایانه در ابتدا هنگام استفاده از خدمات RFID سیار، می‌بیند. هنگامی‌که کاربر نهایی کلید اختصاصی را فشار می‌دهد یا آیکون منو را انتخاب می‌کند، برنامه شروع RFID سیار، اجرا می‌شود.



شکل ۲- تولید اسم‌رمز دسترسی بدون مداخله مصرف‌کننده

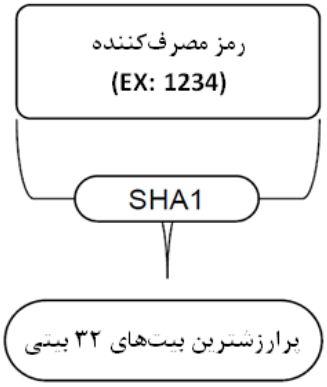
روش دوم، از اطلاعات ورودی مصرف‌کننده، همانند شماره پایانه RFID سیار و شناسانه افزاره سیار پایانه استفاده می‌کند. شکل ۳ روش تولید اسم‌رمز دسترسی را با استفاده از اطلاعات مصرف‌کننده نشان می‌دهد. ویژگی اصلی این روش این است که اسم‌رمز دسترسی به‌طور متفاوت و برطبق ورودی مصرف‌کننده به‌دست می‌آید. برای مثال، اگر شماره پایانه RFID سیار ۰۱۰۰۰۰۱۰۰۰۱، ESN از پایانه B0000000 و ورودی مصرف‌کننده از صفحه‌کلید[3] پایانه ۱۲۳۴ باشد، برنامه شروع RFID سیار، بعد از به‌هم‌چسباندن[4] این مقادیر، SHA1 را انجام می‌دهد و پرارزش‌ترین بیت‌های ۳۲ بیتی را به‌عنوان اسم‌رمز دسترسی انتخاب می‌کند. مزایای این روش سبب می‌شود که کاربر بتواند اطلاعات محصول را به‌وسیله طبقه[5] مدیریت کند. یعنی اگر مصرف‌کننده عدد «۱۰۰۰» را به محصولات پزشکی اختصاص دهد و عدد «۲۰۰۰» را به پوشاک، این اعداد می توانند نقش شاخص گروه را بازی کنند.

1- Secure Hash Algorithm 1
2- Most Significant Bits
3- Keypad
4- Concatenating
5- Category



شکل ۳- تولید اسم‌رمز دسترسی با استفاده از اطلاعات ورودی مصرف‌کننده و پایانه

آخرین روش، فقط از اطلاعات ورودی مصرف‌کننده استفاده می‌کند. شکل ۴ روش تولید اسم‌رمز دسترسی را فقط با ورودی مصرف‌کننده نشان می‌دهد. ویژگی اصلی این روش این است که مصرف‌کننده می تواند EMII برچسب پیوست‌شده به اقلام خریداری‌شده را با استفاده از سایر پایانه‌های RFID سیار بخواند. چون دو روش بالا از اطلاعات پایانه ویژه استفاده می‌کنند، فقط پایانه RFID سیار مصرف‌کننده می‌تواند اسم‌رمز دسترسی را به‌طور مجدد تولید کند. از سوی دیگر، در این روش، اگر ورودی مصرف‌کننده ارائه شده باشد، سایر پایانه‌های RFID سیار می‌توانند اسم‌رمز دسترسی را به‌طور مجدد تولید کند.



شکل ۴- تولید اسم‌رمز دسترسی با استفاده از فقط ورودی مصرف‌کننده

با استفاده از خروجی SHA1 تولیدشده، EMII، مخفی‌شده با کدبندی می‌شود. الگوریتم پیش‌فرض مخفی‌کردن با کدبندی، XOR بیت به بیت است. EMII باید با MSBهای خروجی SHA1، مخفی‌شده با کدبندی شود. اندازه MSBهای استفاده شده همانند طول EMII است. اگر طول EMII بزرگتر از ۱۶۰ باشد که ۱۶۰ طول خروجی SHA1 است، MSBهای کافی به طور مکرر برای مخفی‌کردن با کدبندی استفاده می‌شوند. علاوه بر این، بررسی افزونگی دوره‌ای-۱۶ (CRC-16)[1] باید بر روی کلمه کنترل پروتکل (PC)[2] و EMII جدید محاسبه شود.

1- Cyclic Redundancy Check-16
2- Protocol Control

۶-۵ مرحله ۴. به‌روزرسانی بانک‌های حافظه

مرحله چهارم، به‌روزرسانی حافظه برچسب است. اهداف این مرحله، فیلد UII از بانک حافظه UII و فیلد Access Passwd از بانک حافظه Reserved می‌باشد.

به‌طور کلی، شناسایی اقلام برچسب‌گذاری‌شده می‌تواند توسط EMII اعلام شود. بنابراین، پس از این‌که مصرف‌کننده اقلام برچسب‌گذاری‌شده را خریداری کرد، EMII باید به‌روزرسانی شود.

EMII می‌تواند با EMII جدید که مقدارش مخفی‌شده با کدبندی شده EMII اصلی است، به‌روزرسانی شود.

علاوه بر این، فیلد CRC-16 از بانک حافظه UII می تواند با یک CRC-16 جدید به‌روزرسانی شود.

به‌علاوه، اسم‌رمز دسترسی با اسم‌رمز دسترسی جدید که در مرحله ۳ تولید شده است، به‌روز می‌شود.

این عملیات به‌روزرسانی در وضعیت امن و با استفاده از فرمان Write یا BlockWrite انجام می‌شود.

۶-۶ مرحله ۵. قفل‌کردن بانک‌های حافظه

پنجمین مرحله، قفل‌کردن بانک‌های حافظه برچسب است. اهداف قفل‌کردن، بانک حافظه UII و فیلد Access Passwd از بانک حافظه Reserved می‌باشد.

بعد از مرحله ۴، برچسب در وضعیت امن باقی می‌ماند و دارای EMII مخفی‌شده با کدبندی و اسم‌رمز دسترسی به‌روزشده است. بنابراین، باید بانک‌های حافظه مرتبط را قفل‌کرد که بازجوها نتوانند حافظه را به‌روزرسانی کنند.

عملیات قفل‌کردن با استفاده از فرمان Lock انجام می‌شود. جدول ۱ قالب بارمفید[1] فرمان Lock و مقادیر اجباری بیت‌های Mask و Action را نشان می‌دهد (به بند ۹-۳-۲-۱۱-۳-۵ با عنوان Lock از استاندارد ISO/IEC 18000-6:2010 مراجعه شود).

1- Payload

جدول ۱- بارمفید قفل و استفاده در مرحله ۴

		فیلدهای Mask و Action مرتبط									
		Kill pwd		Access pwd		حافظه UII		حافظه TID		حافظه User	
Mask	بیت	۱۹	۱۸	۱۷	۱۶	۱۵	۱۴	۱۳	۱۲	۱۱	۱۰
	مفهوم	نادیده گرفتن/ نوشتن	نادیده گرفتن/ نوشتن	نادیده گرفتن/ نوشتن	نادیده گرفتن/ نوشتن	نادیده گرفتن/ نوشتن	نادیده گرفتن/ نوشتن	نادیده گرفتن/ نوشتن	نادیده گرفتن/ نوشتن	نادیده گرفتن/ نوشتن	نادیده گرفتن/ نوشتن
	مقدار	×	×	۱	×	۱	×	×	×	×	×
Action	بیت	۹	۸	۷	۶	۵	۴	۳	۲	۱	۰
	مفهوم	خواندن/ نوشتن اسم‌رمز	خواندن/ نوشتن اسم‌رمز	خواندن/ نوشتن اسم‌رمز	خواندن/ نوشتن اسم‌رمز	خواندن/ نوشتن اسم‌رمز	خواندن/ نوشتن اسم‌رمز	خواندن/ نوشتن اسم‌رمز	خواندن/ نوشتن اسم‌رمز	خواندن/ نوشتن اسم‌رمز	خواندن/ نوشتن اسم‌رمز
	مقدار	×	×	۱	×	۱	×	×	×	×	×

×: مهم نیست

۷ فرانامه[1] عملیات

۷-۱ پایانه معتبر RFID سیار مصرف‌کننده

این استاندارد را می‌توان برای همه برچسب‌های مطابق با استانداردهای ISO/IEC 18000-6 Type C و ISO/IEC 18000-3 MODE 3 به‌کاربرد. بنابراین، توصیه می‌شود که پایانه RFID سیار مصرف‌کننده، نقش مهمی را در حفظ حریم مصرف‌کننده بازی کند.

روند زیر مرتبط است با رفتارهای پایانه معتبر RFID سیار مصرف‌کننده که مطابق با این استاندارد در هنگام خرید می‌باشد.

۱) (مصرف‌کننده) اقلام برچسب‌گذاری‌شده را خریداری می‌کند.

۲) (پایانه RFID سیار) برچسب‌ها را می‌سازد و به وضعیت امن گذر می‌دهد.

- اگر اسم‌رمز دسترسی برچسب، یک اسم‌رمز دسترسی با مقدار تمام‌صفر باشد، برچسب بدون هیچ اقدام به‌دست‌آوری کلیدی، به وضعیت امن گذر می‌کند.
- اگر اسم‌رمز دسترسی برچسب، یک اسم‌رمز دسترسی با مقدار غیرصفر باشد، برچسب پس از به‌دست‌آوردن اسم‌رمز دسترسی معتبر، با استفاده از فرمان Access به وضعیت امن گذر می‌کند.

۳) (پایانه RFID سیار) اسم‌رمز دسترسی مصرف‌کننده را تولید می‌کند.

1- Scenario

- اگر ورودی مصرف‌کننده استفاده شود، برنامه شروع RFID سیار، واسطی را فراهم می‌کند تا ورودی را دریافت نماید.

۴) (پایانه RFID سیار) EMII را کدبندی مخفی می‌کند.

- EMII با MSBهای خروجی SHA1 که در مرحله قبل تولید شده است، مخفی‌شده با کدبندی، می‌شود.

- بر روی کلمه PC و EMII مخفی‌شده با کدبندی، CRC-16 محاسبه می‌شود.

۵) (پایانه RFID سیار) بانک‌های حافظه به‌روزرسانی می‌شود.

- فیلد UII از بانک حافظه UII با EMII جدید به‌روزرسانی می‌شود که مقدارش مخفی‌شده با کدبندی از EMII اصلی است.

- فیلد CRC-16 از بانک حافظه UII با CRC-16 جدید که در مرحله قبل محاسبه شده است، به‌روزرسانی می‌شود.

- فیلد Access Passwd از بانک حافظه Reserved با اسم‌رمز دسترسی مصرف‌کننده، به‌روزرسانی می‌شود.

۶) (پایانه RFID سیار) بانک‌های حافظه به‌روزرسانی‌شده قفل می‌شود.

- فیلد pwd-write از بانک حافظه UII به مقدار ۱ تنظیم می‌شود.

- به‌دلیل فیلد Access Passwd از بانک حافظه Reserved، فیلد pwd-read/write به مقدار ۱ تنظیم می‌شود.

بعد از تملک اقلام برچسب‌گذاری‌شده، مصرف‌کننده روش زیر را برای استفاده از خدمت RFID سیار انجام می‌دهد:

۱) (پایانه RFID سیار) از برچسب‌هایی که به اموال مصرف‌کننده پیوست شده است، فهرست‌برداری می‌کند.

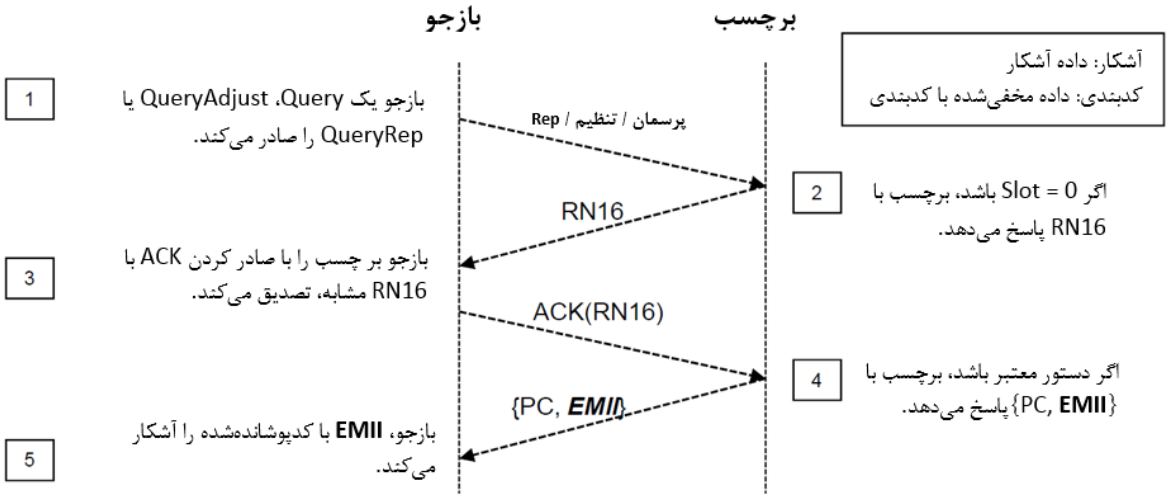
- اگر اطلاعاتی که از پایانه RFID سیار مصرف‌کننده است استفاده شده باشد، فقط پایانه می‌تواند EMII مخفی‌شده با کدبندی را آشکار کند.

- اگر ورودی مصرف‌کننده استفاده شده باشد، برنامه شروع RFID سیار، واسطی را برای دریافت ورودی فراهم می‌کند.

۲) (پایانه RFID سیار) EMII مخفی‌شده با کدبندی را آشکار می‌کند.

- برچسب‌های مصرف‌کننده به فرمان Ack پاسخ می‌دهد. این پاسخ به‌وسیله EMII مخفی‌شده با کدبندی است که مقدارش متفاوت از مقدار EMII اصلی است.

۳) (مصرف‌کننده) پس از آشکارسازی، از خدمت RFID سیار که از EMII استفاده می‌کند، لذت می‌برد.



شکل ۵- فهرست کالای برچسب مصرف‌کننده

۲-۷ پایانه نامعتبر RFID سیار مصرف‌کننده

در مورد روشی که بین پایانه نامعتبر RFID سیار مصرف‌کننده که اسم‌رمز دسترسی را نمی‌داند و برچسبی که با EMII مخفی‌شده با کدبندی، به‌روزرسانی شده‌است، پایانه RFID سیار، EMII مخفی‌شده با کدبندی را به‌عنوان EMII اصلی شناسایی می‌کند.

بنابراین، کسی‌که نمی‌تواند اسم‌رمز دسترسی صحیح تولید کند، نمی‌تواند به اطلاعات اقلام که از EMII شناسایی‌شده است، پی ببرد.

پیوست الف
(اطلاعاتی)
تجزیه و تحلیل امنیت

الف-۱ کلیات

این استاندارد به مسائل امنیتی مانند روش احرازهویت متقابل، روش رمزنگاری[1] داده و مجموعه الگوریتم رمز[2]، رسیدگی نمی‌کند. این استاندارد شامل روش عملیاتی بازجو برای حفظ حریم مصرف‌کننده نمی‌باشد.

این استاندارد برای برچسب‌ها و بازجوهایی که منطبق بر واسط‌های هوایی استانداردهای ISO/IEC 18000-6 Type C و ISO/IEC 18000-3 MODE 3 RFID است، بدون هیچ اصلاح سخت‌افزاری یا فرمان اضافه، می‌تواند به‌کار رود.

الف-۲ ضعف شناخته‌شده

عملیات این استاندارد به دو قسمت تقسیم می‌شود: در زمان خرید و پس از مالکیت. مراحل ۱ تا ۵ مربوط به زمان خرید هستند. در طی مراحل ۱ تا ۵، استراق‌سمع‌کننده می‌تواند EMII اصلی، جدید و اسم‌رمز استفاده‌شده را بازیابی کند. این نقطه ضعف، نتیجه رویه فهرست کالای اصلی است که به‌صورت متن آشکار[3] منتقل می‌شود. برای اینکه حریم مصرف‌کننده از استراق‌سمع پس از مالکیت اقلام برچسب‌گذاری‌شده حفظ شود، توصیه می‌شود در هنگام خرید، مراحل ۱ تا ۵ به‌صورت امن اجرا شود.

الف-۳ گمنامی و حفظ حریم

گمنامی برچسب، به‌وسیله مخفی‌کردن با کدبندی EMII محافظت می‌شود. به‌منظور حذف ارتباط میان اموال مصرف‌کننده و برچسب پیوست‌شده به اموال مصرف‌کننده، EMII اصلی با اسم‌رمز مصرف‌کننده مخفی‌شده با کدبندی می‌شود.

به‌طور کلی، فروشگاه می‌تواند EMIIهای برچسب‌های RFID که بر روی محصول پیوست‌شده را مخفی‌شده با کدبندی کند. این عمل را با استفاده از اسم‌رمز خودش انجام می‌دهد تا EMII به‌روزرسانی‌شده را از عمل نوشتن، محافظت کند. در این مورد، EMII اصلی اعلام نمی‌شود زیرا مخفی‌شده با کدبندی می‌باشد. فروشگاه مجاز است در منطقه TID و همچنین برای بررسی اصالت خرید هنگام درخواست استرداد از کد اختصاصی استفاده کند.

مصرف‌کنندگانی که به امنیت بیشتر تمایل دارند، می‌توانند از اسم‌رمزهای گوناگون که مستقل از ورودی مصرف‌کننده و مطابق با هر محصول است، استفاده کنند. در این مورد، حتی اگر یکی از اسم‌رمزها هم آشکار شود، EMIIهای فردی، نمی‌توانند بازیابی شوند.

1- Encryption
2- Cipher Algorithm Suite
3- Plaintext

با این حال، به فردی که اسم‌رمز را نمی‌داند مقادیر TID و EMII که بازگردانده می‌شود، ایستا و یکتا برای برچسب خواهد بود. اگر در هنگام استفاده سایر مشکلات حریم وجود داشته باشد، توصیه می‌شود برای کمک به جلوگیری از این‌که برچسب بدون اطلاع کاربر خوانده شود، از برچسب‌های با برد خواندنی کوتاه[1] استفاده شود.

1- Short Read-range

کتابنامه

[1] ISO/IEC Directives, Part 2, Rules for the structure and drafting of International Standards, 2011

[2] IETF RFC 3174, US Secure Hash Algorithm 1 (SHA1), September 2001

[3] FIPS PUB 197, Advanced Encryption

[4] Standard (AES), November 2001

[5] ISO/IEC 29143, Information technology — Automatic identification and data capture techniques — Air interface specification for Mobile RFID interrogators

[6] ISO/IEC 29167-1, Information technology — Automatic identification and data capture techniques — Part 1: Air Interface for security services and file management for RFID architecture1)

[7] ISO/IEC 29167-3, Information technology — Automatic identification and data capture techniques — Part 3: Air Interface for security services and file management for RFID at 13.56 MHz1)

[8] ISO/IEC 29167-6, Information technology — Automatic identification and data capture techniques — Part 6: Air Interface for security services and file management for RFID at 860-960 MHz1)

[9] ISO/IEC 29173-1, Information technology — Automatic identification and data capture techniques — Mobile item identification and management — Part 1: Mobile RFID interrogator device protocol for ISO/IEC 18000-6 type B and type C1)

[10] ISO/IEC 29174-1, Information technology — Automatic identification and data capture techniques — UII scheme and encoding format for Mobile AIDC services — Part 1: Identifier scheme for multimedia information access triggered by tag-based identification1)

[11] ISO/IEC 29175, Information technology — Mobile item identification and management — Application data structure encoding format for Mobile AIDC services1)

[12] ISO/IEC 29177, Information technology — Mobile item identification and management — Object Directory Service for Mobile AIDC services1)

[13] ISO/IEC 29178, Information technology — Mobile item identification and management — Service broker for Mobile AIDC services1)

[14] ISO/IEC 29179, Information technology — Mobile item identification and management — Mobile AIDC application programming interface1)

[15] ITU-T Recommendation X.1171, Threats and requirements for protection of personally identifiable information in applications using tag-based identification