INSO
16386-6
1st. Edition
2015

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۱۶۳۸۶-۶
چاپ اول
۱۳۹۳

کارت‌های شناسایی-واسط‌های برنامه نویسی کارت‌های مدار مجتمع-

قسمت ۶: رویه‌های مرجع ذی‌صلاح ثبت پروتکل‌های اصالت‌سنجی به منظور هم‌کنش‌پذیری

Identification cards - Integrated circuit card programming interfaces —Part 6: Registration authority procedures for the authentication protocols for interoperability

ICS: 35.240.15

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 نمد . 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

«کارت‌های شناسایی-واسط‌های برنامه نویسی کارت‌های مدار مجتمع- قسمت ۶: رویه‌های مرجع ذی‌صلاح ثبت پروتکل‌های اصالت‌سنجی به منظور هم‌کنش‌پذیری»

رئیس:	**سمت و/ یا نمایندگی**
تدین تفت، علی اکبر (دکترای مخابرات-سیستم)	عضو هیات علمی دانشگاه یزد
دبیر:	
ماندگاری، مریم (فوق لیسانس صنایع-مدیریت سیستم و بهره وری)	رئیس واحد انفورماتیک اداره کل استاندارد یزد
اعضاء: (اسامی به ترتیب حروف الفبا)	
تقوی، مسعود (لیسانس مهندسی کامپیوتر)	کارشناس انفورماتیک اداره کل استاندارد یزد
زارعی محمود آبادی، محمد حسین (دکترای برق-الکترونیک)	کارشناس استاندارد
زهتاب یزدی، محمد حسن (لیسانس مهندسی الکترونیک)	کارشناس استاندارد
جاودانی، ندا (لیسانس مهندسی کامپیوتر)	کارشناس انفورماتیک آب منطقه‌ای یزد
طباطبایی، فریده (لیسانس مهندسی کامپیوتر)	کارشناس انفورماتیک برق منطقه‌ای یزد
مالی، محمدرضا (فوق لیسانس مهندسی برق-الکترونیک)	مشاور طرح کارت ملی سازمان ملی ثبت احوال و اسناد کشور
مغانی، مهدی (فوق لیسانس ریاضی محض)	کارشناس تدوین استانداردهای حوزه فناوری اطلاعات-سازمان فناوری اطلاعات ایران

فهرست مندرجات

عنوان		صفحه
آشنایی با سازمان ملی استاندارد		ب
کمیسیون فنی تدوین استاندارد		ج
پیش گفتار		و
۱	هدف و دامنه کاربرد	۱
۲	مراجع الزامی	۱
۳	اصطلاحات و تعاریف	۱
۴	نمادها و کوته‌نوشت‌ها	۲
۵	کلیات	۲
۶	انتصاب مرجع ذی‌صلاح ثبت	۵
۷	مرور درخواست	۶
۸	محتوای درخواست	۶
پیوست الف (الزامی)	درخواست برای ثبت یک پروتکل اصالت‌سنجی ثبت شده استاندارد ملی شماره ۱۶۳۸۶	۸
پیوست ب (الزامی)	الگوی پروتکل اصالت سنجی	۱۲
پیوست پ (الزامی)	برگه گواهی پروتکل اصالت سنجی	۱۷
پیوست ت (الزامی)	ثبت درخواست پذیرش پروتکل اصالت سنجی	۲۰
پیوست ث(اطلاعاتی)	مرجع ذی‌صلاح ثبت	۲۴

پیش گفتار

استاندارد «کارت‌های شناسایی-واسط‌های برنامه‌نویسی کارت‌های مدار مجتمع- قسمت ۶: رویه‌های مرجع ذی‌صلاح ثبت پروتکل‌های اصالت‌سنجی به منظور هم‌کنش‌پذیری» که پیش نویس آن در کمیسیون های مربوط، توسط سازمان ملی استاندارد تهیه و تدوین شده است و در سیصد و شصت و هفتمین اجلاس کمیته ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۳/۱۲/۶ 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 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 24727-6: 2010, Identification cards - Integrated circuit card programming interfaces - Part 6: Registration authority procedures for the authentication protocols for interoperability.

کارت‌های شناسایی-واسط‌های برنامه نویسی کارت‌های مدار مجتمع- قسمت ۶: رویه‌های مرجع ذی‌صلاح ثبت پروتکل‌های اصالت‌سنجی به منظور هم‌کنش‌پذیری

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین و تعریف رویه‌هایی برای:

-ثبت نام پروتکل‌های اصالت‌سنجی (AP)[1]، از جمله الگوریتم‌های رمزنگاشتی مربوط، روش‌های آزمون و معیار ارزیابی انطباق، و

-ثبت نام پذیرش APهای استاندارد ملی ایران شماره ۱۶۳۸۶ به وسیله قسمت‌های که تمایل دارند تا همکنش‌پذیری AP را اعلان کنند، است.

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.

۲-۱ استاندارد ملی ایران شماره ۳-۱۶۳۸۶، کارت‌های شناسایی ـ واسط‌های برنامه نویسی کارت دارای مدار مجتمع ـ قسمت ۳ : واسط برنامه کاربردی.

۲-۲ استاندارد ملی ایران شماره ۲-۱۶۱۷۶، فناوری اطلاعات: اتصال متقابل سامانه‌های باز -رویه‌هایی برای عملیات مراجع ثبت اتصال متقابل سامانه‌های باز OSI قسمت ۲ :رویه‌های ثبت برای انواع سند OSI .

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به کار می رود:

۳-۱

متقاضی

سازمان یا شخص متقاضی ثبت نام.

۳-۲

پذیرش پروتکل اصالت‌سنجی

از APهای استاندارد ملی ایران شماره ۳-۱۶۳۸۶ و این استاندارد استفاده شود (یا در عملیات استفاده شود یا در مشخصات، استانداردها یا توصیه‌نامه‌های مرتبط مرجع‌دهی شده باشد)

1- authentication protocol

۳-۳

مرجع ذی‌صلاح ثبت

سازمانی که توسط هیات مدیریت فنی ISO/IEC برای آماده‌سازی و حفظ ثبت‌های استاندارد ISO/IEC 24727-6 نامزد و منصوب شده است.

۴-۳

ثبت کننده

سازمان یا شخصی که یا یک پروتکل اصالت‌سنجی و یا پذیرش یک پروتکل اصالت‌سنجی را ثبت می‌کند.

۴ نمادها و کوته نوشت‌ها

برای اهداف این استاندارد نمادها و کوته‌نوشت‌های استاندارد ملی ایران شماره ۳-۱۶۳۸۶ و موارد زیر به کار می‌رود:

AP	authentication protocol	پروتکل اصالت‌سنجی
APDU	application protocol data unit	واحد داده پروتکل کاربردی
APT	authentication protocol template	الگوی پروتکل اصالت‌سنجی
APTP	authentication protocol test plan	برنامه آزمون پروتکل اصالت‌سنجی
OID	object identifier	شناسانه شیء
RA	registration authority	مرجع ذی‌صلاح ثبت
RAP	registered authentication protocol	پروتکل اصالت‌سنجی ثبت شده
URL	uniform resource locator	منبع یاب یکپارچه

۵ کلیات

۵-۱ هدف

این استاندارد رویه‌های ایزو را برای موارد زیر تعریف می‌کند:

- ثبت APهای جدید یا تجدیدنظر شده مطابق با استاندارد ملی ایران شماره ۳-۱۶۳۸۶ و این استاندارد. این APها در پیوست الف (مجموعه‌ای از APها) استاندارد ملی ایران شماره ۳-۱۶۳۸۶ آمده است.
- ثبت الگوریتم‌های رمزنگاشتی مربوطه، APTP و معیار ارزیابی انطباق؛
- ثبت نام پذیرش APهای استاندارد ملی شماره ۱۶۳۸۶ بوسیله قسمت‌های که تمایل دارند تا همکنش‌پذیری AP را اعلان کنند.

۵-۲ وابستگی‌ها

این استاندارد به دو قسمت دیگر از مجموعه استانداردهای ملی شماره ۱۶۳۸۶ و استاندارد ISO/IEC 24727 وابسته است:

- استاندارد ملی شماره ۳-۱۶۳۸۶:
  - روش استاندارد شده برای توصیف واضح یک گستره از APهای متفاوت؛

- روش استاندارد شده برای توصیف واضح یک گستره از الگوریتم‌های رمزنگاشتی متفاوت استفاده شده توسط APها.

- استاندارد ISO/IEC 24727-5: (باید منتشر شود)

-یک روش استاندارد شده برای آزمون انطباق یک گستره از APهای متفاوت؛

-الزامات آزمون برای یک پروتکل اصالت‌سنجی.

۵-۳ دامنه‌های شناسانه شیء (OID)[1] پروتکل اصالت‌سنجی

روش OID ارائه شده در استاندارد ملی ایران شماره ۳-۱۶۳۸۶ به دامنه استاندارد ملی ایران شماره ۲-۱۶۱۷۶ محدود شده است و توسعه دامنه توسط رویه‌های مرجع ذی‌صلاح ثبت را پشتیبانی نمی‌کند.

این استاندارد این توانمندی‌ها را با استفاده از یک دامنه مرجع ذی‌صلاح ثبت توسعه می‌دهد، تا گسترش‌پذیری کامل و الزامات همکنش‌پذیری را برای APهای جدید استانداردهای سری ISO/IEC 24727 تحت دامنه مرجع ذی‌صلاح ثبت استاندارد ملی شماره ۲-۱۶۱۷۶ مدیریت کند.

دامنه مرجع ذی‌صلاح ثبت این استاندارد در زیر آمده:

{ISO (1) registration-authority (1) ISO 24727(24727) part6 (6) *new-protocol-short-name* (*new-protocol-number*)}

۵-۴ ثبت پروتکل اصالت‌سنجی

برای پیاده‌سازی‌های استاندارد ملی ایران شماره ۱۶۳۸۶ با استفاده از APهای مختلف برای رسیدن به همکنش‌پذیری، لازم است که APهای پیاده‌شده به طور واضح مشخص شوند.

برای رسیدن به همکنش‌پذیری با یک گستره از APها، پیاده‌سازها نیاز دارند که جزئیات APها در قالبی منتشر شوند که امکان ارجاع به آنها وجود داشته باشد. این بند یک رویه برای ثبت APها ارائه می‌دهد و همچنین یک رویه برای آن جزئیات ثبتی که باید در قالبی مدیریت شده توسط یک ISO/IEC RA، در یک URL در دسترس عموم قرار گیرند، ارائه می‌دهد.

۵-۴-۱ رویه‌های ثبت پروتکل اصالت‌سنجی

رویه پشتیبانی شده توسط این استاندارد با روش شناسانه شیء ASN.1 استاندارد ملی ایران شماره ۲-۱۶۱۷۶ سازگار است. الزامات ثبت و رویه‌ای برای ثبت APها به شرح و ترتیب زیر رخ می‌دهد:

- متقاضی باید تمام اسنادی را که بخشی از ثبت AP هستند، تکمیل کند؛

- RA، ثبت AP را برای کامل بودن و انطباق مستندات ارائه شده با این استاندارد را بررسی می‌کند. RA تنها مسئول عملیات اجرایی به منظور حفظ ثبّات[2] که شامل مطالب فنی موجود در درخواست متقاضی نمی‌شود، است.

- چنان‌چه در مورد هر یک از داده‌های ارائه شده، یا کمال، درستی، همخوانی یا مالکیت درخواست شکی وجود داشت باشد، آنگاه RA باید در موارد مشکوک بررسی انجام دهد. بهتر است RA در ابتدا با متقاضی مشورت کند.

1- Object Identifier

2 - register

- اگر کلیه الزامات برآورده شود، آنگاه درخواست پذیرفته می‌شود و متقاضی توسط RA آگاه می‌شود.
- اگر RA مشخص کند که درخواست AP کامل نیست یا الزامات این استاندارد را برآورده نمی‌کند، آنگاه متقاضی آگاه شده و این فرصت به متقاضی داده می‌شود تا اسناد را با توجه به موارد بیان شده در شرایط درخواست که توسط مرجع ذی‌صلاح ثبت تعیین شده، بازنگری نموده و دوباره درخواست کند.
-هنگامی‌که درخواست موفقیت‌آمیز است، RA با استفاده از رویه‌های استاندارد ملی ایران شماره ۱۶۱۷۶، یک OID را تخصیص می‌دهد و به متقاضی اطلاع می‌دهد که آنها از تاریخ اولین انتشار، ثبت‌کننده رسمی OID تخصیص یافته هستند؛
- RA، AP جدید و جزئیات ثبت‌کننده را در پایگاه داده به روز و در دسترس عموم OIDهای ثبت شده و APهای این استاندارد در خدمتی مبتنی بر وب روی اینترنت، قرار می‌دهد. جزئیات در پیوست ث ارائه می‌شود.
- به محض موفقیت‌آمیز بودن ثبت، ثبت‌کننده مجاز است به صورت اختیاری برای یک دوره مشخص شده توسط ثبت‌کننده به ثبت پرچم «فقط پیش‌نویس» را بزند. در این مورد، مجاز است که جزئیات AP بیان شده در پیوست ب، تا زمانی‌که ثبت‌کننده به RA اطلاع دهد که AP باید با عنوان «نهایی» منتشر شود، توسط ثبت‌کننده تغییر کند. به محض انتشار AP با عنوان «نهایی»، دیگر نباید هیچ تغییری در نمایش فنی متقاضی AP (همانگونه که در پیوست ب بیان شده) اعمال شود؛
-پرونده‌های عمومی پروتکل اصالت‌سنجی ثبت‌شده باید تا زمانی که ثبت‌کننده با توجه به موارد موجود در شرایط درخواست که توسط RA تعیین‌شده درخواست پس گرفتن آنها را داشته باشد، باقی بماند.
- وضعیت ثبت با توجه به شرایط درخواست که توسط RA تعیین‌شده، ممکن است به «در انتظار لغو ثبت[1]» تغییر کند. RA باید تمام ثبت‌کننده‌ها را از همه رویه‌های مربوط به تغییر وضعیت پروتکل آگاه کند.

۵-۵ ثبت پذیرش پروتکل اصالت‌سنجی

برای اینکه عملیات، مشخصات، استانداردها یا توصیه‌نامه‌ها تحت استاندارد ملی ایران شماره ۱۶۳۸۶به همکنش‌پذیری دست یابند، لازم است که اجزای قابل تعویض از پروتکل‌های اصالت‌سنجی استاندارد و الگوریتم‌های رمزنگاشتی قابل اجرا استفاده کنند.
این بند یک رویه برای ثبت پذیرش پروتکل اصالت‌سنجی توسط یک دسته، دسته‌ها یا گروه‌ها شامل جوامع موردنظر ارائه می‌دهد.

۵-۵-۱ رویه‌های ثبت پذیرش پروتکل اصالت‌سنجی

روش پشتیبانی شده توسط این استاندارد با ASN.1 استاندارد ملی ایران شماره ۲-۱۶۱۷۶ روش شناسانه شیء (OID) سازگار است. الزامات ثبت و رویه‌ای برای ثبت پذیرش پروتکل اصالت‌سنجی به شرح و ترتیب زیر رخ می‌دهد:
- متقاضی فرم درخواست پیوست ت را تکمیل نموده و آن را مطابق با شرایط درخواست تعیین شده توسط RA ارائه می‌دهد؛

1- de-registration

- RA درخواست را ارزیابی می‌کند تا کامل بودن و انطباق مستندات ارائه شده با این استاندارد را تعیین کند. اگر درخواست تمام الزامات را برآورده کند باید پذیرفته و متقاضی آگاه شود.
- اگر RA تعیین کند که درخواست کامل نیست یا الزامات این استاندارد را برآورده نمی‌کند آنگاه به متقاضی اطلاع داده و این فرصت داده می‌شود تا با توجه به همه شرایط دیگر درخواست که توسط RA تعیین شده، بازنگری نموده و دوباره درخواست کند.
- اگر درخواست موفقیت‌آمیز باشد، RA یک پایگاه داده عمومی (قابل دسترس در نشانی RA URL) را با جزئیات متقاضی به روز رسانی می‌کند تا شامل RAP OID باشد. سپس متقاضی باید آگاه شود.
- RA یک رونوشت از جزئیات ثبت‌های به روز و در دسترس عموم و RAP OID های پذیرفته شده را روی اینترنت در یک خدمت مبتنی بر وب در نشانی URL بیان شده در پیوست E نگه می‌دارد؛
- پرونده‌های عمومی پذیرش پروتکل اصالت سنجی جاری باقی می‌مانند تا زمانی که ثبت‌کننده درخواست کند که پس گرفته شود یا شرایط ثبت تعیین شده توسط RA محقق شود.
- با توجه به شرایط درخواست که توسط مرجع ذی‌صلاح ثبت تعیین شده، ممکن است وضعیت پذیرش پروتکل اصالت‌سنجی به «در انتظار لغو ثبت[1]» تغییر کند. RA باید تمام ثبت‌کننده‌ها را از تمام رویه‌های مربوط به تغییر وضعیت ثبت پذیرش پروتکل اصالت‌سنجی آگاه کند.

۶ انتصاب مرجع ذی‌صلاح ثبت

از جمله اختیارات ISO/IEC این است که ثبت را مطابق این استاندارد، ساماندهی کند. به منظور اجرای این، ISO/IEC، مطابق الزامات و قوانین داخلی خود، یک سازمان را منصوب می‌کند تا به عنوان RA برای این استاندارد عمل کند.

اطلاعات تماس RA را می‌توان در پیوست E پیدا کرد.

هرچند وقت یک‌بار ممکن است جزئیات RA تغییر کند؛ در نتیجه ایزو هم یک فهرست بروز از نمایندگی‌های تعمیر و نگهداری و مراجع ذی‌صلاح ثبت، را در URL زیر حفظ و نگهداری می‌کند:
http://www.iso.org/iso/standards_development/maintenance_agencies.htm

۷ مرور درخواست‌ها

۷-۱ رویه

برای پردازش یک درخواست، درخواست باید شامل اطلاعات کافی باشد تا به متقاضی این توانایی را بدهد که به عنوان یک سازمان واجد شرایط[2] شناخته شود و قادر به تطابق با شرایط درخواست تنظیم شده توسط مرجع ذی‌صلاح ثبت باشد. مرجع ذی‌صلاح ثبت مجاز است که درخواست‌های غیرواضح و ناقص را که شرایط درخواست را ندارند، بررسی کند. اگر متقاضی با بررسی موافق نباشد، درخواست رد می‌شود.

1- de-registration
2- bona-fide

اگر درخواست شامل اطلاعات مشخص شده در شرایط درخواست نباشد، ممکن است درخواست با استناد به این زیر بند و اطلاعات خاص از دست رفته، رد شده و به متقاضی اعلام شود.

اگر RA تعیین کند که درخواست مناسب است، سپس آن را در فرآیند تصدیق بند ۷-۳ قرار می‌دهد.

اگر RA تعیین کند که درخواست ممکن است مناسب نباشد، باید هریک از مراحل موجود در شرایط خود برای درخواست را طی‌کند.

۷-۲ زمان پاسخ

بررسی یک درخواست تحت رویه‌های مشخص شده در بند ۷-۱، معمولا باید در مدت ۱۰ روز کاری از دریافت درخواست کامل شود.

۷-۳ فرآیند تصدیق

جزئیات درخواست موفق باید در یک وب سایت که توسط RA نگهداری می‌شود، ثبت گردد و متقاضی باید از URL این سایت و OIDهای ثبت شده آگاه شود.

۸ محتوای درخواست‌ها

۸-۱ کلیات

اطلاعات مورد نیاز RA برای اجرای فرآیند ثبت، ممکن است توسط پست الکترونیکی، دورنگار، لوح فشرده یا کپی کاغذی ارائه شود، یا (بهتر است RA انتخاب کند که از این گزینه‌ها پشتیبانی کند) از طریق برگه تحت وب یا با استفاده از پروتکل‌های خدمات وب ارائه شود. اطلاعات دیگر در مورد تعهدات متقاضیان و اطلاعات درخصوص قوانین قابل اجرا در شرایط درخواست مرجع ذی‌صلاح ثبت، آمده است.

۸-۲ درخواست‌ها

درخواست برای ثبت AP، باید شامل تمام اطلاعات مورد نیاز پیوست‌های الف، ب و پ باشد و برای ثبت پذیرش AP باید شامل تمام اطلاعات پیوست ت و الزامات مربوطه بیان شده در پیوست‌های قبل برای شمول اسناد، غرامت‌ها و نمودارها باشد.

برگه‌های درخواست اطلاعات زیر را برای ثبت AP جمع‌آوری می‌کند:

۱- اطلاعات شناسه تجاری و تماس متقاضی؛

۲- یک الگوی پروتکل اصالت‌سنجی کامل‌شده (استخراج شده از پیوست الف و ب استاندارد ملی ایران شماره ۳-۱۶۳۸۶) دارای جزئیات خاص پروتکل اصالت‌سنجی پیشنهاد شده و الگوریتم‌های رمزنگاشتی پشتیبانی شده؛

۳- جزئیات مالکیت معنوی متقاضی و AP شامل، کشور ثبت اختراع، شماره و مالکیت ثبت اختراع؛

۴-یک برنامه آزمون پروتکل اصالت‌سنجی (APTP) [1] که دارای جزئیات خاص مورد نیاز برای آزمون AP پیشنهاد شده مطابق استاندارد ISO/IEC 24727-5 (باید منتشر شود) است.

۵-برگه گواهی، به پیوست پ مراجعه شود؛

1 - authentication-protocol-test-plan

۶-سایر نظرات موردنیاز متقاضی برای انتشار؛

برگه درخواست اطلاعات زیر را برای ثبت پذیرش، جمع‌آوری می‌کند:

۱- اطلاعات تجاری و تماس متقاضی؛

۲-نام عملیات، مشخصات، استاندارد و توصیه‌نامه که از RAP OID استفاده می‌کند؛

۳-RAP OID که باید استفاده شود؛

۴-الگوریتم‌های رمزنگاشتی پشتیبانی شده؛

۵-مدل پشته[1] استاندارد ملی ایران شماره ۴-۱۶۳۸۶ پشتیبانی‌شده؛

۶-سایر نظرات موردنیاز متقاضی برای انتشار.

۳-۸ نگهداری یک ثبات مبتنی بر وب

RA باید دو ثبات به شرح زیر را نگه دارد:

-پروتکل اصالت‌سنجی ثبت‌شده از جمله OID ثبت شده؛

-یک ثبات پذیرش پروتکل اصالت‌سنجی از جمله OID پذیرفته شده.

هر ورودی باید اطلاعات شناسانه را به همراه یک پیوند[2] به جزئیات کامل ارائه شده در درخواست مصوب به استثنای اطلاعات مربوط به پرداخت و امضاها را بدهد. RA باید یک وب سایت تهیه کند که محتوای ثبات‌ها را نمایش می‌دهد. RA باید مسئول تعیین رویه‌های داخلی لازم برای حفظ ثبات در یک وضعیت بهنگام و مناسب باشد. RA گزارش سالیانه را برای زیر کمیته ISO/IEC JTC1/SC 17 و دبیرخانه ISO تهیه می‌کند. این‌ها با درخواست از کمیته فرعی در دسترس هستند.

1- Stack
2- link

پیوست الف
(الزامی)

درخواست برای ثبت یک پروتکل اصالت‌سنجی ثبت شده استاندارد ملی شماره ۱۶۳۸۶

به: مرجع ذی‌صلاح ثبت پروتکل اصالت‌سنجی استاندارد ملی ایران شماره ۶-۱۶۳۸۶

بهتر است متقاضیان توجه کنند که تمام اطلاعات ارائه شده بوسیله این برگه از جمله کلیه جزئیات پیوست شده به جز جزئیات پرداخت‌ها، روی وب سایت RA منتشر می‌شود.

الف-۱ اطلاعات تماس سازمان متقاضی RAP

نام سازمان:

_____

شماره شناسایی ملی کسب و کار:

_____

کشور و استان/منطقه به منظور شناسایی کسب و کار:

_____

نشانی:

_____
_____
_____
_____
_____

تلفن:

_____

نمابر:

_____

پست الکترونیکی:

_____

الف-۲ نماینده مجاز

نام:

_____

عنوان:

_____

نشانی:

_____
_____
_____
_____

پست الکترونیکی:

_____

امضا: _____

الف-۳ نام شناسایی مختصر RAP پیشنهاد شده

_____

از همان شناسانه استفاده شده در الگو پروتکل اصالت‌سنجی ثبت شده استفاده شود.

الف-۴ شرح کوتاه کارکرد RAP پیشنهاد شده

_____
_____

جزئیات کامل به صورت جداگانه در الگوی پروتکل اصالت‌سنجی ثبت‌شده، موردنیاز است.

الف-۵ اختراعات ثبت‌شده قابل اعمال به RAP پیشنهاد شده

آیا پروتکل اصالت‌سنجی پیشنهاد شده منوط به ثبت اختراعی نیست؟

- □ منوط به شماره ثبت اختراعات در کشورهای ذکر شده در زیر
- □ دامنه عمومی
- □ غیر وابسته به ثبت اختراع
- □ پروتکل ISO/IEC

الف-۵-۱ شماره‌ها/کشورهای ثبت اختراعی که قابل اعمال به RAP است

_____
_____
_____
_____

تمام ثبت اختراعات شناخته شده باید ذکر شود.

الف-۶ شرایط مجوز

آیا شرایطی وجود دارد که یک مجری باید به منظور استفاده از پروتکل اصالت‌سنجی پیشنهاد شده، برآورده سازد؟

□ به زیر مراجعه کنید

□ نه- دامنه عمومی

□ بله- با صاحب مجوز تماس بگیرید

□ بله – به استاندارد ISO/IEC همانگونه که در زیر بیان شده، مراجعه کنید

□ بله –متن باز- به جزئیات مجوز که در زیر ذکر شده مراجعه کنید

الف-۶-۱ شرایط مجوز

_____
_____
_____
_____
_____
_____

الف-۷ تماس به منظور ثبت اختراع/مجوزدهی

_____
_____
_____
_____
_____

الف-۸ امضاءکنندگان

روز _____ ماه _____ سال _____

توسط: _____ (نام) امضاء: _____

امضاء شد.

مهر شرکت:

گواهی می‌شود توسط:

توسط: _____ (نام) امضاء: _____

نشانی تماس و شماره تلفن گواهی دهندگان

_____
_____
_____
_____
_____
_____

پیوست ب
(الزامی)
الگوی پروتکل اصالت‌سنجی

به: مرجع ذی‌صلاح ثبت پروتکل اصالت‌سنجی استاندارد ملی ایران شماره ۶-۱۶۳۸۶
APT زیر از پیوست الف استاندارد ملی ایران شماره ۳-۱۶۳۸۶ استخراج شده است. بهتر است متقاضیان برای مشاهده مثال‌ها و جزئیات نحوه تکمیل این الگو به استاندارد ملی ایران شماره ۶-۱۶۳۸۶رجوع کند.

ب-۱ شناسایی AP پیشنهاد شده

نام شناسایی مختصر پیشنهادی برای AP پیشنهاد شده.

_____

از شناسانه یکسان با برگه درخواست پروتکل اصالت‌سنجی ثبت شده، استفاده کنید. این شناسانه باید بین ۲۰ تا ۴۰ نویسه داشته باشد. توجه کنید که اگر تعارض نامی با AP دیگری که پیش‌تر ثبت‌شده روی دهد، RA مجاز است شناسانه را تغییر دهد.

شرح مختصر از کارکرد AP پیشنهاد شده.

_____
_____

از شرح یکسان با برگه درخواست پروتکل اصالت‌سنجی ثبت شده استفاده کنید.

شرح مفصل AP پیشنهاد شده.

_____
_____
_____
_____

این باید حاوی اطلاعاتی باشد که به خواننده در انتخاب AP کمک کند.

فهرست سایر RAP OID استاندارد ملی ایران شماره ۱۶۳۸۶ که در این AP پیشنهاد شده از آنها استفاده شده است.

_____
_____

اگر در AP پیشنهاد شده از سایر APهای استاندارد ملی ایران شماره ۳-۱۶۳۸۶ یا شماره ۶-۱۶۳۸۶ استفاده شود، OID اینها باید در اینجا فهرست شود.

نمودار بلوکی[1] پروتکل اصالت‌سنجی پیشنهاد شده.

یک نمودار توالی بلوکی در قالب JPEG، که به سبک استفاده شده در پیوست الف استاندارد ملی ایران شماره ۳-۱۶۳۸۶ قالب‌بندی شده، را ضمیمه کنید (مثالی از آن در زیر آمده است). این نمودار توالی باید بخش‌های زیر را شرح دهد:

-برنامه کاربردی کارخواه[2]؛

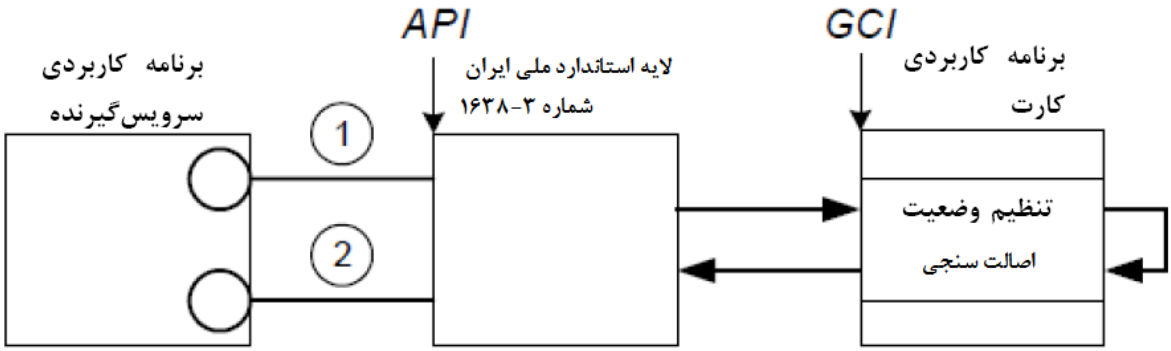
-پیاده‌سازی لایه استاندارد ملی ایران شماره ۳-۱۶۳۸؛

-بخش برنامه کاربردی کارت[3]؛

-واسط SAL-API؛

-واسط GCI.

این نمودار باید تمام مراحل مهم مورد نیاز AP برای پشتیبانی از هم‌کنش‌پذیری را بیان کند.



شکل ب-۱- مثالی از نمودار بلوکی

ب-۲ علامت‌گذار[4]

سازه را با استفاده از روشگان استاندارد ملی ایران شماره ۳-۱۶۳۸ شرح دهید.

1- block diagram
2- client-application
3- card-application
4- Marker

ب-۳ DIDCreate

سازه را با استفاده از روشگان استاندارد ملی ایران شماره ۳-۱۶۳۸ شرح دهید.

ب-۴ DIDUpdate

سازه را با استفاده از روشگان استاندارد ملی ایران شماره ۳-۱۶۳۸ شرح دهید.

ب-۵ DIDGet

سازه را با استفاده از روشگان استاندارد ملی ایران شماره ۳-۱۶۳۸ شرح دهید.

ب-۶ اصالت‌سنجی

جزئیات پروتکل را با استفاده از روشگان استاندارد ملی ایران شماره ۳-۱۶۳۸ شرح دهید، دقت کنید که تمام مراحل و شاخه‌های[1] پروتکل و همچنین پیوندهای واضح به مراحل اصالت‌سنجی شماره‌دار نشان داده شده در نمودار قسمت ب-۱-۱، شرح داده شود.

ب-۷ رمزگذاری[2]

به طور واضح نتیجه مورد انتظار از این درخواست را شرح دهید.

ب-۸ رمزگشایی[3]

به طور واضح نتیجه مورد انتظار از این درخواست را شرح دهید.

1- branches
2- Encipher
3- Decipher

ب-۹ GetRandom

_____
_____

به طور واضح نتیجه مورد انتظار از این درخواست را شرح دهید.

ب-۱۰ Hash

_____
_____

به طور واضح نتیجه مورد انتظار از این درخواست را شرح دهید.

ب-۱۱ Sign

_____
_____

به طور واضح نتیجه مورد انتظار از این درخواست را شرح دهید.

ب-۱۲ تایید امضا

_____
_____

به طور واضح نتیجه مورد انتظار از این درخواست را شرح دهید.

ب-۱۳ تایید گواهی‌نامه

_____
_____

به طور واضح نتیجه مورد انتظار از این درخواست را شرح دهید.

ب-۱۴ آزمون

_____
_____

جزئیات کامل برنامه‌های آزمون یا روش‌های آزمون جایگزین همچون کارت‌های آزمون یا نمونه‌ساز (شامل پیوندهایی به محتوای پشتیبانی) را با استفاده از روشگان آزمون استاندارد ISO/IEC 24727-5 برای APها ضمیمه کنید.

ب-۱۵ الزامات الگوریتم رمزنگاشتی

الگوریتم(ها) رمزنگاشتی خاص و OIDهای آنها که توسط پروتکل پشتیبانی می‌شود را فهرست کنید.

ب-۱۶ گواهی

برگه گواهی پیوست پ را به عنوان یک خودگواهی[1] یا به عنوان یک گواهی انجام شده توسط یک مرجع ذی‌صلاح مستقل، کامل و ارائه کنید.

برای ثبت اولیه یک AP، متقاضی مجاز است خودگواهی کند. شرایطی که تجدید ثبت را برآورده می‌کند، در اصلاحیه آینده این استاندارد بیان خواهد شد. در مورد خودگواهی، باید اظهارنامه متقاضی براساس اطمینان از انطباق AP، با استاندارد ملی شماره ۱۶۳۸۶ باشد.

1- self-certification

پیوست پ

(الزامی)

برگه گواهی پروتکل اصالت‌سنجی

به: مرجع ذی‌صلاح ثبت پروتکل اصالت‌سنجی استاندارد ملی ایران شماره ۶-۱۶۳۸۶

بهتر است متقاضیان توجه کنند که تمام اطلاعات ارائه شده بوسیله این برگه از جمله کلیه جزئیات پیوست شده به جز جزئیات پرداخت‌ها روی وب سایت RA منتشر می‌شود.

پ-۱ اطلاعات تماس سازمان گواهی‌دهنده

نام سازمان:

_____

شماره شناسایی ملی کسب و کار:

_____

کشور و استان/منطقه به منظور شناسایی کسب و کار:

_____

نشانی:

_____

_____

_____

_____

_____

تلفن:

_____

نمابر:

_____

پست الکترونیکی:

_____

پ-۲ نماینده مجاز

نام:

_____

عنوان:

_____

نشانی:

_____
_____
_____
_____
_____

پست الکترونیکی:

_____

امضاء: _____

پ-۳ نام شناسایی پروتکل اصالت‌سنجی گواهی شده

_____

پ-۴ گواهی

نوع گواهی

<بله/نه> خودگواهی (متقاضی و گواهی دهنده یک سازمان است).

<بله/نه> گواهی مستقل (متقاضی و گواهی دهنده سازمان‌های متفاوت هستند).

جزئیات گواهی

<بله/نه> آیا پروتکل اصالت‌سنجی حداقل الزامات یک پروتکل اصالت‌سنجی را مطابق استاندارد ملی ایران شماره ۳-۱۶۳۸ برآورده می‌کند.

<بله/نه> آیا برنامه آزمون موجود در درخواست پروتکل اصالت‌سنجی، حداقل الزامات یک برنامه آزمون پروتکل اصالت‌سنجی را مطابق استاندارد ISO/IEC 24727-5 برآورده می‌کند.

<بله/نه> آیا پروتکل اصالت‌سنجی برنامه‌های آزمون ارائه شده به همراه درخواست را با موفقیت طی می‌کند؟

پ-۵ امضاءکنندگان

روز _____ ماه _____ سال _____

توسط: _____ (نام) امضاء: _____

امضاء شد.

مهر شرکت:

گواهی می‌شود توسط:

توسط: _____ (نام) امضاء: _____

نشانی تماس و شماره تلفن گواهی دهندگان

_____

_____

_____

_____

_____

_____

پیوست ت

(الزامی)

ثبت درخواست پذیرش پروتکل اصالت‌سنجی

به: مرجع ذی‌صلاح ثبت پروتکل اصالت‌سنجی استاندارد ملی ایران شماره ۶-۱۶۳۸۶.

بهتر است متقاضیان توجه کنند که تمام اطلاعات ارائه شده بوسیله این برگه از جمله کلیه جزئیات پیوست شده به جز جزئیات پرداخت‌ها روی وب سایت RA منتشر می‌شود.

ت-۱ اطلاعات تماس سازمان

نام سازمان:

_____

شماره شناسایی ملی کسب و کار:

_____

کشور و استان/منطقه به منظور شناسایی کسب و کار:

_____

نشانی:

_____
_____
_____
_____
_____

تلفن:

_____

نمابر:

_____

پست الکترونیکی:

_____

ت-۲ نماینده مجاز

نام:

_____

عنوان:

_____

نشانی:

_____
_____
_____
_____
_____

پست الکترونیکی:

_____

امضاء: _____

ت-۳ نام شناسایی مختصر RAP پذیرفته شده

_____

همان نام شناسانه استفاده شده RAP OID ذکر شود.

ت-۴ OIDی RAP پذیرفته شده

_____

از همان شناسانه OID استفاده شده در RAP OID استفاده شود.

ت-۵ الگوریتم‌های رمزنگاشتی

_____

فهرست الگوریتم‌های رمزنگاشتی و OIDهای آنها که باید پشتیبانی شود ذکر شود.

ت-۶ مدل پشته

مدل/های پشته استاندارد ملی ایران شماره ۴-۱۶۳۸۶ را فهرست کنید که از کدام یک پشتیبانی می‌شود؟

ت-۷ نام یا URL سند/هایی که RAP OID را پذیرفته است/اند.

این نام استاندارد، مشخصات، توصیه‌نامه، سامانه یا جامعه موردنظر، که منتشر شده، است.

ت-۸ نوع پذیرش

- □ استاندارد
- □ مشخصات
- □ توصیه نامه
- □ سامانه
- □ جامعه مورد نظر
- □ سایر

ت-۹ URL یا سایر ارجاع‌ها به بند ث-۷

پیوندها یا ارجاع‌هایی به مشخصات، استاندارد، توصیه‌نامه، سامانه یا جامعه موردنظر ارائه کنید. توصیه می‌شود که آن اسناد شامل یک پیوند معکوس به RA و RAP OID نیز باشند تا از شفاف‌سازی در RAP/ها دقیق مشخص شده برای پیاده‌سازی‌ها اطمینان حاصل شود.

ت-۱۰ سایر نظرات برای انتشار

این باید شامل هرگونه نظرات فنی به خصوص نظرات مربوط به پیاده‌سازی برای انتشار که به همکنش‌پذیری یا پیاده سازی کمک می‌کند، باشد.

ت-۱۱ امضاءکنندگان

روز _____ ماه _____ سال _____

توسط: _____ (نام) امضاء: _____

امضاء شد.

مهر شرکت:

گواهی می‌شود توسط:

توسط: _____ (نام) امضاء: _____

نشانی تماس و شماره تلفن گواهی دهندگان

_____

_____

_____

_____

_____

_____

پیوست ث
(اطلاعاتی)
مرجع ذی‌صلاح ثبت

ث-۱ جزئیات RA

مرجع ذی‌صلاح ثبت برای این استاندارد که توسط شورای ISO/lE تائید شده عبارت است از:

SAI Global Limited

مرجع ذی‌صلاح ثبت استاندارد ISO/IEC 24727-6

استرالیا، NSW 2000، سیدنی، خیابان 286 Sussex

استرالیا، NSW 2001، سیدنی، GPO Box 5420

تلفن: ۶۱۲۸۲۰۶۶۰۶۰

نمابر: ۶۱۲۸۲۰۶۶۰۲۵

پست الکترونیکی: ISO24727-6@saiglobal.com

URL مرجع ثبت نام: http://www.saiglobal.com/ISO24727-6

کلیه درخواست‌ها برای ثبت یا استعلام در مورد ثبات‌ها که توسط مرجع ذی‌صلاح ثبت حفظ و نگهداری می‌شود باید به «مرجع ذی‌صلاح ثبت این استاندارد» به نشانی فوق ارسال شود.

ث-۱-۱ پرداخت‌ها

جزئیات حق الزحمه‌ها و هزینه‌های جاری مربوط به این RA بر روی وب سایت RA با URL ذکر شده در بالا حفظ و نگهداری می‌شود.

برگه‌های مناسب و/یا یک خدمت برخط با حق الزحمه و هزینه‌های جاری از وب سایت RA قابل دسترسی است.

متقاضیان باید توجه کنند که ثبت نام هیچ درخواستی آغاز نمی‌شود تا:

-رسید پرداخت مناسب توسط RA دریافت و تایید شود؛

-تمام الزامات این استاندارد برای درخواست برآورده شود.

ث-۱-۲ به روز رسانی‌های جزئیات RA

ممکن است جزئیات RA هرچند وقت یک‌بار تغییر کند؛ درنتیجه ایزو هم یک فهرست به روز از بنگاه‌های نگهداری و مراجع ذی‌صلاح ثبت را در URL زیر را نگه می‌دارد.

http://www.iso.org/iso/standards_development/maintenance_agencies.htmorithms.