استاندارد ایران –ایزو آی ای سی
۲- ۱۱۸۸۹
چاپ اول

مرداد ۱۳۹۲

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران

Iranian National Standardization Organization

INSO-ISO-IEC
11889-2

1st. Edition

Identical with
ISO/IEC 11889-1:2009
Aug.2013

فناوری اطلاعات- پودمان سکوی مطمئن

قسمت ۲: اصول طراحی

Information technology — Trusted Platform Module — Part 2:Design principles

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 صدورگواهی 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- پودمان سکوی مطمئن قسمت ۲: اصول طراحی »

رئیس:	**سمت یا نمایندگی**
رضایی، رامین (لیسانس مهندسی برق - الکترونیک)	معاون طرح و توسعه مرکز تحقیقات صنایع انفورماتیک
دبیر:	
منافی، علیرضا (فوق لیسانس مهندسی معماری کامپیوتر)	معاون فناوری اطلاعات مرکز تحقیقات صنایع انفورماتیک
اعضاء: (اسامی به ترتیب حروف الفبا)	
افکار، علی (دکترای مهندسی برق- الکترونیک)	عضو هیات علمی دانشگاه علم و صنعت
ترابی، سعید (لیسانس مدیریت صنعتی)	مدیر فنی شرکت بازرسی کالای تجاری
تورانی، فرزام (لیسانس مهندسی کامپیوتر)	کارشناس مرکز تحقیقات صنایع انفورماتیک
زندباف، عباس (لیسانس مهندسی الکترونیک - مخابرات)	کارشناس شرکت ارتباطات زیرساخت
فرجپور، مهیار (فوق لیسانس مهندسی برق - الکترونیک)	عضو هیات مدیره شرکت سیماوا
فرخی، علی (دکتری مهندسی برق - الکترونیک)	عضو هیات علمی دانشگاه آزاد اسلامی تهران جنوب
نادری، مجید (دکترای مهندسی برق - الکترونیک)	عضو هیات علمی دانشگاه علم و صنعت

فهرست مندرجات

پیش گفتار

استاندارد "فناوری اطلاعات- پودمان سکوی مطمئن - قسمت ۲: اصول طراحی" که پیش‌نویس آن در کمیسیون فنی مربوط، توسط مرکز تحقیقات صنایع انفورماتیک، بر مبنای روش تنفیذ مورد اشاره در راهنمای ISO/IEC Guide21-1 (پذیرش منطقه‌ای یا ملی استانداردهای "بین‌المللی/ منطقه‌ای" و دیگر مدارک استاندارد) به عنوان استاندارد ملی ایران، تهیه شده و در یک صد و هشتاد و سومین اجلاسیه کمیته ملی استاندارد رایانه و فرآوری داده‌ها مورخ ۹۰/۱۲/۲۴ مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ 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 زمینه‌ی صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدیدنظر خواهد شد و هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، در هنگام تجدیدنظر در کمیسیون فنی مربوط، مورد توجه قرار خواهد گرفت. بنابراین، همواره از آخرین تجدیدنظر آنها استفاده خواهد شد.

این استاندارد ملی براساس پذیرش استاندارد " بین‌المللی " به شرح زیر است :

ISO/IEC 11889-1:2009 , Information technology — Trusted Platform Module — Part 2:Design principles

فناوری اطلاعات- پودمان سکوی مطمئن قسمت دوم: اصول طراحی

۱ هدف و دامنه کاربرد

این استاندارد ملی، براساس پذیرش استاندارد بین‌المللی ISO 11889-2: 2009 تدوین شده است.

هدف از تدوین این استاندارد سامانه‌ای برای شناساندن پودمان سکوی مطمئن است (TPM)[1]، افزاره‌ای که به طور کلی قابلیت اطمینان در سکوهای محاسباتی را ایجاد می‌کند. به منظور شفاف‌سازی نقش تمام مستندات، این استاندارد به قسمت‌های مختلفی تفکیک شده است. هر نسخه از استاندارد برای این که کامل باشد به همه قسمت‌ها نیاز دارد.

یک طراح TPM باید آگاه باشد که برای تعریف کامل همه الزامات لازم برای ساخت TPM، باید از مشخصات خاص سکو مناسب برای همه الزامات TPM استفاده کند.

قسمت ۲ اصول کلی عملیات TPM را شرح می دهد. مدهای اصلی عملیات، الگوریتم‌ها و انتخاب‌های کلیدی، به همراه شرایط همکاری اساسی، اکثریت اصلی جملات الزامی را در قسمت ۲ تشکیل می دهند.

۱-۱ لغات کلیدی

لغات کلیدی "باید"،"نباید"،"لازم است"، بایست، نبایست، توصیه می‌شود "شاید" و "اختیاری" در گزاره‌های دستوری این مستند آن طور که در تقاضای اعلام نظر (RFC-2119)[2] ، لغات کلیدی برای استفاده در RFCها به‌منظور نشان‌دادن سطوح الزام شرح داده شده است، تفسیر می‌شود.

۱-۲ نوع جمله

لطفا به تفاوت بسیار مهمی بین قسمت‌های مختلف متن در سراسر این مستند توجه داشته باشید.

در این مستند، شما با دو نوع متن متفاوت روبرو خواهید شد:توضیح اطلاعاتی و گزاره‌های دستوری.

از آن جا که بیشتر متن در این مشخصات از نوع جملات تجویزی خواهد بود، نویسندگان بطور غیررسمی آن را به عنوان پیش گزیده تعریف کرده‌اند، تنها متن از نوع توضیح اطلاعاتی را مشخصا اعلام کرده‌اند. آنها این کار را با قرار دادن یک نشانگر در ابتدا و انتهای هر توضیح اطلاعاتی و سایه روشن کردن متن به رنگ خاکستری انجام داده‌اند. این بدین این معنی است که شما می‌توانید متن را از نوع گزاره دستوری در نظر بگیرید. مگر اینکه متن به طور خاص به عنوان توضیح اطلاعاتی مشخص شده، باشد.

برای مثال:

۱-۳ شروع توضیح اطلاعاتی

این اولین پاراگراف از ۱ تا n پاراگراف شامل متن از نوع توضیح اطلاعاتی است.

1-Trusted Platform Module
2-Request For Comment

این دومین پاراگراف از متن از نوع توضیح اطلاعاتی است.

این nامین پاراگراف از متن از نوع توضیح اطلاعاتی است.
برای فهم استاندارد، استفاده کننده باید آن را بخواند.(این مورداستفاده از کلمه باید نیازمند هیچ عملی نیست).

۱-۴ انتهای توضیح اطلاعاتی

این اولین پاراگراف از یک یا تعداد بیشتری پاراگراف (و/یا قسمت‌ها) شامل متنی از نوع گزاره‌های دستوری است.

برای فهم استاندارد استفاده‌کننده باید آن را بخواند. (این مورد استفاده از **کلمه** باید نشانگر یک لغت کلیدی است و نیازمند یک اقدام است.

۲ 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 محسوب می‌شود.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد ملی الزامی است :

2-1 ISO/IEC 8825-1 | ITU-T X.690: Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

2-2 ISO/IEC 10118-3, Information technology — Security techniques — Hash-functions Part 3: Dedicated hash-functions, Clause 9, SHA-1

2-3 ISO/IEC 18033-3, Information technology — Security techniques — Encryption algorithms—Part 3, Block ciphers, Clause 5.1 AES

2-4 IEEE P1363, Institute of Electrical and Electronics Engineers: Standard Specifications For Public-Key Cryptography

2-5 IETF RFC 2104, Internet Engineering Task Force Request for Comments 2104: HMAC : Keyed-Hashing for Message Authentication

2-6 IETF RFC 2119, Internet Engineering Task Force Request for Comments 2119: Key words for use in RFCs to Indicate Requirement Levels

2-7 PKCS #1 Version 2.1, RSA Cryptography Standard. This document is superseded by P1363, except for section 7.2 that defines the V1.5 RSA signature scheme in use by the TPM.

کلیه بندهای استاندارد بین‌المللی ISO/IEC 11889-2:2009 در مورد این استاندارد معتبر و الزامی است