



جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standardization Organization



استاندارد ایران - ایزو -

آی ای سی

۱۳۸۸۸-۲

چاپ اول

INSO-ISO/IEC

13888-2

1st. Edition
Identical with

ISO/IEC 13888-2:2010

فناوری اطلاعات - فنون امنیتی - سلب انکار -
قسمت ۲: سازوکارهای به کارگیری فنون متقارن

IT security techniques – Non repudiation –
Part 2 : Mechanisms using symmetric
techniques

ICS : 35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسه استاندارد و تحقیقات صنعتی ایران به موجب بند یک ماده ۳ قانون اصلاح قوانین و مقررات مؤسسه 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 و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانه صاحبان حق و نفع، شامل تولیدکنندگان، مصرف کنندگان، 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 می شود و پس از دریافت نظرها و پیشنهادات در کمیته 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 در کمیته ملی طرح و بررسی و در صورت 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 شماره ۵ تدوین و در کمیته ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)^۱، کمیسیون بین المللی الکتروتکنیک (IEC)^۲ و سازمان بین المللی اندازه شناسی قانونی (OIML)^۳ است و به عنوان تنها رابط^۴ کمیسیون کدکس غذایی (CAC)^۵ 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 بین المللی بهره گیری می شود.

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 درجه بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینه مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سیستم های مدیریت کیفیت و مدیریت زیست محیطی، 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، گواهینامه 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

« فنون امنیتی فناوری اطلاعات - سلب انکار - بخش ۲: سازوکارهای به کارگیری فنون متقارن »

رئیس:

کشاوری ، فرزاد
(لیسانس مهندسی کامپیوتر نرم افزار)

سمت و / یا نمایندگی

کارشناس رایانه

دبیر:

امیری ، حسین
(لیسانس مهندسی کامپیوتر نرم افزار)

مدیر عامل شرکت پیشتازان پردازش اطلاعات

اعضاء: (اسامی به ترتیب حروف الفبا)

خندزاد ، بهزاد
(لیسانس مهندسی کامپیوتر نرم افزار)

کارشناس رایانه

خندزاد ، بیتا
(کارشناس ارشد هوش مصنوعی و رباتیک)

کارشناس ارشد ادارات مرکزی هواپیمائی
جمهوری اسلامی ایران هما

درفشی ، رکسانا
(لیسانس زبان انگلیسی)

کارشناس تایید صلاحیت سازمان استاندارد

سروشیان ، سپیده
(لیسانس مهندسی کامپیوتر نرم افزار)

کارشناس رایانه

کلاکی ، اتنا سادات
(کارشناس ارشد هوش مصنوعی)

کارشناس شورای عالی انفورماتیک

نصیری زنوز ، مجید
(لیسانس مهندسی برق - قدرت)

کارشناس شرکت مهندسین مشاور موندکو ایران

فهرست مندرجات

صفحه	عنوان
ب	آشنایی با سازمان ملی استاندارد
ج	کمیسیون فنی تدوین استاندارد
ه	پیش گفتار
۱	۱ هدف و دامنه کاربرد
۱	۲ مراجع الزامی

پیش گفتار

استاندارد " فنون امنیتی فناوری اطلاعات - سلب انکار - بخش ۲: سازوکارهای به کارگیری فنون متقارن " که پیش نویس آن در کمیسیون های مربوط توسط شرکت پیشتازان پردازش اطلاعات بر مبنای روش تنفیذ مورد اشاره در راهنمای ISO/IEC Guide21-1 (پذیرش منطقه ای یا ملی استانداردهای "بین المللی/ منطقه ای" و دیگر مدارک استاندارد) به عنوان استاندارد ملی ایران، تهیه شده و در یکصد و هشتاد و پنجمین اجلاس کمیته ملی استاندارد رایانه و فرآوری داده ها مورخ ۱۳۹۰/۱۲/۲۱ 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 می گردد.

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 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 بر اساس پذیرش استاندارد بین المللی به شرح زیر است:

ISO/IEC 13888-2:2010, IT security techniques – Non repudiation – Part 2 : Mechanisms using symmetric techniques

فنون امنیتی فناوری اطلاعات - سلب انکار - بخش ۲: سازوکارهای بکارگیری فنون متقارن

۱ هدف و دامنه کاربرد

این استاندارد ملی، بر اساس پذیرش استاندارد بین‌المللی ISO/IEC 13888-2: 2010 تدوین شده است. هدف از تدوین این استاندارد، برای خدمت سلب انکار تولید، گردآوری، نگهداری، در دسترس قرار دادن و گواهی تایید در خصوص رویداد یا کنش خواسته شده برای حل اختلافات در مورد به وقوع و عدم وقوع رویداد یا کنش است. این بخش از این استاندارد توضیحاتی از ساختارهای عمومی را فراهم می‌کند که می‌توانند برای خدمات سلب انکار و بعضی از طرزکارهای خاص مرتبط با ارتباطات جهت فراهم نمودن سلب انکار مبدا (NRO)^۱ و سلب انکار تحویل (NRD)^۲ بکار برده شوند. سایر خدمات سلب انکار می‌توانند با بکارگیری ساختارهای عمومی تشریح شده در این بخش از این استاندارد برای مواجهه با نیازهای تعریف شده توسط خط مشی امنیتی ساخته شوند.

این بخش از این استاندارد به وجود شخص ثالث مورد اعتماد (TTP)^۳ برای جلوگیری از انکار تقلب یا تهمت استناد می‌کند. بطور معمول یک TTP برخط مورد نیاز است. سلب انکار فقط می‌تواند در زمینه خط مشی امنیتی که بطور واضح تعریف شده است، برای کاربردی ویژه و محیط قانونی‌اش فراهم شود. خط مشی‌های سلب انکار در استاندارد بین‌المللی ISO/IEC 10181-4 تعریف شده‌اند.

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 ایران محسوب می‌شود. در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده است، اصلاحیه‌ها و تجدیدنظرهای 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 آن‌ها مورد نظر است. استفاده از مراجع زیر برای این استاندارد الزامی است:

2-1: ISO/IEC 9798-1:1997، Information technology - Security techniques - Entity authentication - Part 1: General

2-2: ISO/IEC 10118 (all parts)، Information technology - Security techniques - Hash-functions

2-3: ISO/IEC 13888-1، Information technology - Security techniques - Non-repudiation - Part 1: General

کلیه بندهای استاندارد بین‌المللی ISO/IEC 13888-2: 2010 در مورد این استاندارد معتبر و الزامی است.

1- non-repudiation of origin
2- non-repudiation of delivery
3- trusted third party