استانداردایران–
آی ای سی
۱۴۸۸۸-۳
چاپ اول

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standardization Organization

INSO-IEC
14888-3
1st. Edition
Identical with ISO/IEC 14888-3: 2006+ Cor1:2007 + Cor2:2009 + Amd1:2010+ Amd2:2012

فناوری اطلاعات - فنون امنیتی – امضاهای رقمی (دیجیتال) با پیوست قسمت ۳: سازوکارهای برپایه لگاریتم گسسته

Information technology - Security techniques - Digital signatures with appendix Part 3: Discrete logarithm based mechanisms

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 - فنون امنیتی – امضاهای رقمی (دیجیتال) با پیوست قسمت ۳: سازوکارهای برپایه لگاریتم گسسته »

رئیس:	**سمت و/ یا نمایندگی**
کشاورزی ، فرزاد (لیسانس مهندسی کامپیوتر نرم افزار)	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 هوش‌مصنوعی)	کارشناس شورای عالی انفورماتیک
نصیری زنوز ، مجید (لیسانس مهندسی برق - قدرت)	کارشناس شرکت مهندسین مشاور مونتکو ایران

فهرست مندرجات

پیش گفتار

استاندارد " فناوری اطلاعات - فنون امنیتی – امضاهای رقمی (دیجیتال) با پیوست قسمت ۳: سازوکارهای برپایه لگاریتم گسسته" که پیش‌نویس آن در کمیسیون‌های مربوط توسط شرکت پیشتازان پردازش اطلاعات 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 یکصدوهشتادونهمین اجلاس کمیته ملی استاندارد رایانه و فرآوری داده‌ها مورخ ۱۳۹۱/۰۱/۲۶ 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 می‌گردد.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم وخدمات، 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 قرارخواهدگرفت. بنابراین همواره از آخرین تجدیدنظرآنها استفاده خواهد شد.

این استاندارد ملی بر اساس پذیرش استاندارد بین‌المللی به شرح زیر است:

ISO/IEC 14888-3:2006، Information technology – Security techniques - Digital signatures with Appendix Part 3: Discrete logarithm based mechanisms + Cor1:2007 + Cor2:2009 + Amd1:2010+ Amd2:2012

فناوری اطلاعات - فنون امنیتی - امضاهای رقمی (دیجیتال) با پیوست قسمت ۳: سازوکارهای برپایه لگاریتم گسسته

۱ هدف و دامنه کاربرد

این استاندارد ملی، بر اساس پذیرش استاندارد بین‌المللی ISO/IEC 14888-3: 2006+ Cor1:2007 + Cor2:2009 + Amd1:2010+ Amd2:2012 تدوین شده است.

هدف از تدوین این استاندارد، سازوکارهای امضای رقمی (دیجیتال) با پیوستی که امنیت آن بر پایه مساله لگاریتم گسسته است، را مشخص می‌کند. این استاندارد، موارد زیر را فراهم می‌کند:

- توصیف کلی از سازوکار امضای رقمی (دیجیتال) با پیوست.
- تنوعی از سازوکارهایی که امضاهای رقمی (دیجیتال) با پیوست را فراهم می‌کنند.
- برای هر طرز کار این قسمت از این استاندارد را مشخص می‌کند
- فرایند ایجاد یک جفت کلید
- فرایند تولید امضاها
- فرایند درستی‌سنجی امضاها

درستی‌سنجی امضای دیجیتالی به کلید درستی‌سنجی هستار امضاء نیاز دارد. از این رو برای شخصی که درستی‌سنجی می‌کند، ضروری است که بتواند کلید درستی سنجی‌صحیح را همراه با هستار امضاء، یا بطور دقیق‌تر با (قسمت‌هایی از) داده‌های شناسائی هستار امضاء، وابسته سازد.

این وابستگی مابین داده‌های شناسائی و کلید درستی‌سنجی عمومی امضاء کننده می‌تواند یا بوسیله هستار یا سازوکار بیرونی، یا بطور ذاتی در کلید درستی‌سنجی خودش تضمین شود. طرحواره در حالت قبلی "گواهینامه - مبنا" بودن، گفته می‌شود. طرحواره در حالت آخر، "هویت - مبنا" بودن گفته می‌شود. بطور نمونه در یک طرحواره هویت- مبنا، شخصی که درستی‌سنجی می‌کند می‌تواند کلید درستی‌سنجی عمومی امضاء را از داده‌های شناسائی امضاء استنتاج کند. طرز کارهای امضاء رقمی (دیجیتال) که در این استاندارد مشخص شده‌اند، در طرز کارهای گواهینامه - مبنا و هویت - مبنا دسته‌بندی می‌شوند.

یادآوری: برای طرز کارهای گواهینامه – مبنا، استانداردهای زیر ساختار کلید عمومی (PKI[1]) گوناگونی می‌توانند برای مدیریت کلید استفاده شوند. برای اطلاعات بیشتر استانداردهای بین‌المللی ISO/IEC 15945 و ISO/IEC 9594-8 (همچنین با عنوان X.509 شناخته شده است) و نیز به استاندارد بین‌المللی ISO/IEC 15945 مراجعه شود.

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.

1- Public key infrastructure

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 10118 (all parts)، Information technology - Security techniques - Hash-functions.

2-2: ISO/IEC 14888-1، Information technology - Security techniques - Digital signatures with appendix - Part 1:General

کلیه بندهای استاندارد بین‌المللی ISO/IEC 14888-3: 2006+ Cor1:2007 + Cor2:2009 + + Amd1:2010 Amd2:2012 در مورد این استاندارد معتبر و الزامی است.