INSO
10825-1
1st. Edition
May.2013

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۱-۱۰۸۲۵
چاپ اول
اردیبهشت ۱۳۹۲

فناوری اطلاعات – فنون امنیتی- احراز هویت هستار قسمت ۱: کلیات

Information technology – Security techniques — Entity authentication part1: General

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 امنیت-احراز هویت هستار - قسمت ۱: کلیات »

رئیس:	سمت و/ یا نمایندگی
سعیدی، عذرا (فوق لیسانس مهندسی برق مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
دبیر:	
میراسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم افزار)	مدیر کل خدمات ارزش افزوده سازمان فناوری اطلاعات
اعضاء: (اسامی به ترتیب حروف الفبا)	
بختیاری، شیرین (لیسانس مهندسی برق)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
جمیل پناه، ناصر (فوق لیسانس مدیریت)	کارشناس سازمان فناوری اطلاعات
سلطانی، الهه (لیسانس مهندسی برق مخابرات)	کارشناس سازمان فناوری اطلاعات
صوفی زاده، جلیل (دکتری، مهندسی برق مخابرات)	مشاور و پژوهشگر در صنعت فناوری اطلاعات
فرهاد شیخ احمد، لیلا (فوق لیسانس مهندسی کامپیوتر نرم افزار)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
فولادیان، مجید (فوق لیسانس مهندسی برق مخابرات)	مشاور سازمان فناوری اطلاعات
فیاضی، مهدی (لیسانس مهندسی برق مخابرات)	کارشناس و مسئول تدوین استاندارد و امنیت شبکه سازمان فناوری اطلاعات
قسمتی، سیمین	کارشناس تدوین استاندارد سازمان فناوری

(فوق لیسانس فناوری اطلاعات)	اطلاعات
عباسپور، مقصود (دکتری کامپیوتر)	استادیار دانشگاه شهید بهشتی
معروف، سینا (لیسانس مهندسی کامپیوتر)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
موجبی، محمود (فوق لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
میرزایی رضایی، طیبه (فوق لیسانس فیزیک)	رییس اداره تدوین استانداردها و نظارت بر امنیت سرویس‌ها سازمان فناوری اطلاعات
ناظمی، اسلام (دکتری کامپیوتر)	استادیار دانشگاه شهید بهشتی
نیسی مینایی، آصف (لیسانس فناوری اطلاعات)	لیسانس فناوری اطلاعات

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد «فناوری اطلاعات- فنون امنیتی- احراز هویت هستار- قسمت ۱: کلیات» که پیش‌نویس آن درکمیسیون‌های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده و در دویستمین اجلاس کمیتهٔ ملی استاندارد رایانه و فرآوری داده مورخ ۹۱/۷/۴ مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات سازمان استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینهٔ 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 تجدیدنظر استانداردهای ملی استفاده کرد.

منبع و مأخذی که برای تهیهٔ این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 9798-1:2010, Information technology — Security techniques — Entity authentication — Part 1: General

- **مقدمه**

احراز هویت[1] هستار در سامانه‌هایی که شامل ارتباط بی درنگ[2] هستند، یک سرویس امنیتی مهم بنیادی به شمار می‌رود. بسته به برنامه کاربردی مشخص و اهداف امنیتی، احراز هویت هستار می‌تواند شامل استفاده از یک پروتکل یک گذره ساده با احراز هویت یک جانبه[3] یا یک پروتکل چند گذره با احراز هویت یک سویه یا دو سویه[4] بین گروه‌های باشد.

هدف احراز هویت هستار این است که آیا خواهان در یک هویت مشخص، به طور واقعی همان کسی است که ادعا می‌کند. به منظور دستیابی به این هدف باید زیرساخت اولیه‌ای موجود باشد که هستار را به یک رمزنگاشتی سرّی (مانند یک زیرساخت کلید عمومی) مرتبط سازد. برقراری چنین زیرساختی فراتر از دامنه‌ی استاندارد ISO/IEC 9798 است.

پروتکل گوناگون احراز هویت هستار در ISO/IEC 9798 به منظور پشتیبانی سامانه‌های امنیتی و اهداف امنیتی مختلف مشخص می‌شوند. به عنوان مثال وقتی حمله‌ی بازپخش[5] برای یک سامانه خاص، عملی یا مسئله‌ساز نیست، پروتکل‌های ساده با گذرهای کمتر بین خواهان و درستی‌سنج کافی خواهد بود. با این وجود در سامانه-های ارتباطی پیچیده‌تر، حمله‌های بازپخش و فردی- در- میان[6] یک تهدید واقعی هستند. در چنین مواردی به منظور دستیابی به اهداف امنیتی سامانه، یکی از پروتکل‌های بیشتر مرتبط با استاندارد ISO/IEC 9798 ضروری خواهد بود.

دو مدل اصلی برای پروتکل احراز هویت وجود دارد. در یک مدل، خواهان و درستی سنج، برای احراز اعتبار شناسه خواهان، به طور مستقیم ارتباط برقرار می‌کنند. در مدل دیگر، هستارها، با استفاده از طرف سوم قابل اعتمادی، اعتبار شناسه‌ها را احراز می‌نمایند.

ویژگی‌های امنیتی یک طرح که باید پیش از انتخاب پروتکل احراز هویت در نظرگرفته شوند شامل موارد زیر می‌باشند:

- جلوگیری از حمله‌ی بازپخش
- جلوگیری از حمله‌ی بازتاب[7]
- جلوگیری از تأخیر تحمیلی[8]
- احراز هویت یک‌جانبه/ دو جانبه

1- Authentication
2- Real-time
3- Unilateral
4- Mutual authentication
5- Replay attack
6- Man-in-the-middle attack
7- Reflection attack
8- Forced delay

- اینکه آیا از یک رمز پیش‌ساخته می‌توان استفاده کرد، یا برای کمک به ایجاد چنین رمز مشترکی، نیاز به درگیری طرف سوم قابل اعتمادی وجود دارد.

فناوری اطلاعات – فنون امنیتی- احراز هویت هستار
قسمت ۱: کلیات

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین یک مدل احراز هویت و الزامات کلی و محدودیت‌های سازوکارهای احراز هویت هستار مورد استفاده در فنون امنیتی است. این سازوکارها تایید می‌کنند که هر هستار همان چیزی است که ادعا می‌شود. یک هستار به منظور احراز هویت با نمایش آگاهی خود از یک رمز، هویت خود را به اثبات می‌رساند. سازوکارها به عنوان مبادلات اطلاعات بین هستارها، و در صورت نیاز با یک طرف سوم مورد اعتماد، تعریف می‌شوند.

جزئیات سازوکارها و محتوای مبادلات احراز هویت در قسمت‌های بعدی ISO/IEC 9798 آورده شده است.

۲ مراجع الزامی

برای این استاندارد مراجع الزامی وجود ندارد.

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به‌کار می‌رود:

۳-۱

فن رمزنگاشتی نامتقارن[۱]

رمزنگاشتی از دو تبدیل مرتبط استفاده می‌کند: یک تبدیل عمومی (تعریف شده با کلید عمومی) و یک تبدیل خصوصی (تعریف شده با کلید خصوصی)

یادآوری- دو تبدیل دارای این خاصیت هستند که با در نظر گرفتن تبدیل عمومی، تبدیل خصوصی از لحاظ محاسباتی امکان پذیر نمی باشد.

۳-۲

سامانه رمز بندی نامتقارن[۲]

سامانه مبتنی بر فنون رمزنگاشتی نامتقارن که عملیات عمومی آن برای رمزبندی و عملیات خصوصی‌اش برای رمزگشایی استفاده می‌شود.

۱- Asymmetric cryptographic technique

2- Asymmetric encryption system

۳-۳

جفت کلید نامتقارن[1]

جفتی از کلیدهای مرتبط که در آن کلید خصوصی، تبدیل خصوصی وکلید عمومی، تبدیل عمومی را مشخص می‌کند.

۴-۳

سامانه امضای نامتقارن[2]

سامانه‌ای بر اساس فنون رمزنگاشتی نامتقارن که تبدیل خصوصی آن برای امضا و تبدیل عمومی آن برای درستی سنجی استفاده می‌شود.

۵-۳

چالش[3]

قلم داده‌ای به صورت تصادفی انتخاب و توسط درستی سنج برای خواهان فرستاده می‌شود تا خواهان به همراه اطلاعات سری که در اختیار دارد از آن استفاده کرده و پاسخی را برای درستی سنج ایجاد کند.

۶-۳

خواهان[4]

هستار[5] اصلی (یا نماینده آن) که برای مقاصد احراز هویت مورد استفاده قرار می گیرد.

یادآوری- یک خواهان، محتوای توابع و داده خصوصی مورد نیاز برای درگیری در تبادلات احراز هویت را شامل می‌شود.

۷-۳

متن رمز[6]

داده‌ای که برای پنهان ساختن محتوای اطلاعاتی خود تبدیل یافته است.

۸-۳

تابع وارسی رمزنگاشتی[7]

تبدیل رمزنگاشتی که یک کلید سرّی و یک رشته‌ی اختیاری را به عنوان ورودی دریافت نموده و یک مقدار وارسی رمزنگاشتی به عنوان خروجی برمی‌گرداند.

یادآوری- محاسبه مقدار وارسی صحیح بدون آگاهی از کلید سرّی[8] امکان‌پذیر نخواهد بود.

1- Asymmetric key pair
2- Asymmetric signature system
3- Challenge
4- Claimant
5- Entity
6- Cipher text
7- Cryptographic check function
8- secret key

۹-۳

مقدار وارسی رمزنگاشتی[1]

اطلاعاتی که با انجام دادن یک تبدیل رمزنگاشتی بر روی واحد داده‌ای بدست می‌آید.

۱۰-۳

رمزگشایی[2]

عملیات معکوس متناظر با رمز بندی است.

۱۱-۳

امضای دیجیتال[3]

داده الحاقی به یک واحد داده یا به تبدیل رمزنگاشتی شده آن، که به گیرنده واحد داده اجازه می‌دهد که منبع و صحت واحد داده را اثبات و از آن در برابر جعل، به طور مثال توسط گیرنده، محافظت نماید.

۱۲-۳

شناسه تشخیص دهنده[4]

اطلاعاتی که یک هستار را در متن یک مبادله احراز هویت، به وضوح تشخیص می‌دهد.

۱۳-۳

رمزبندی [5]

عملیاتی برگشت‌پذیر توسط یک الگوریتم رمزنگاشتی که جهت پنهان کردن محتوای اطلاعاتی داده، آن را به متن رمز تبدیل می‌کند.

۱۴-۳

احراز هویت هستار[6]

تأیید آنکه یک هستار همان چیزی است که ادعا می‌شود.

۱۵-۳

حمله جای‌دهی [7]

ظاهرسازی با استفاده از اطلاعاتی که از یک یا چند مبادله احراز هویت جاری یا قبلی به دست می‌آید.

1- Cryptographic check value
2- Decryption
3- Digital signature(signature)
4- Distinguishing identifier
5- Encryption
6- Entity authentication
7- Interleaving attack

۳-۱۶

کلید[1]

دنباله‌ای از نمادها که عملیات یک تبدیل رمزنگاشتی را کنترل می‌کند.

یادآوری- به عنوان مثال رمز بندی، رمزگشایی، محاسبه تابع وارسی رمزنگاشتی، تولید امضا، یا درستی‌سنجی امضا.

۳-۱۷

دگرنمایی[2]

تظاهر یک هستار به یک هستار متفاوت است.

۳-۱۸

احراز هویت دو جانبه[3]

احراز هویت هستاری که دو هستار را از هویت یکدیگر مطمئن می‌سازد.

۳-۱۹

متن ساده[4]

اطلاعات پوشانده نشده[5] است.

۳-۲۰

اصلی[6]

هستاری که هویت آن قابل احراز هویت باشد.

۳-۲۱

کلید رمزگشایی خصوصی[7]

کلید خصوصی که تبدیل رمزگشایی خصوصی را مشخص می‌کند.

۳-۲۲

کلید خصوصی[8]

کلید مربوط به جفت کلید نامتقارن یک هستار که رمز آن را حفظ کرده و تنها باید توسط آن هستار استفاده شود.

1- Key
2- Masquerade
3- Mutual authentication
4- Plaintext
5- Unenciphered
6- Principal
7- Private decryption key
8- Private key

۲۳-۳

کلید امضای خصوصی[1]

کلید خصوصی که تبدیل امضای خصوصی را تعریف می‌کند.

یادآوری- این کلید گاهی، کلید امضای رمز نامیده می‌شود.

۲۴-۳

کلید رمز بندی عمومی[2]

کلید عمومی که تبدیل رمز بندی عمومی را تعریف می‌کند.

۲۵-۳

کلید عمومی[3]

کلید مربوط به جفت کلید نامتقارن یک هستار که می‌تواند عمومی شود.

۲۶-۳

گواهینامه کلید عمومی[4]

اطلاعات کلید عمومی یک هستار که توسط مرجع صدور گواهی[5]، امضا شده و به این طریق قابل جعل نخواهد بود.

یادآوری- به پیوست پ نیز مراجعه شود.

۲۷-۳

اطلاعات کلید عمومی[6]

اطلاعات مختص به یک هستار منفرد که حداقل شامل محتوی شناسه تشخیص‌دهنده و کلید عمومی آن هستار باشد.

یادآوری- سایر اطلاعات در خصوص مرجع صدور گواهی، هستار و کلید عمومی، از جمله مدت زمان اعتبار کلید عمومی، مدت زمان اعتبار کلید خصوصی وابسته، یا شناسه‌ی درگیر در الگوریتم‌ها، احتمالا در گواهی کلید عمومی گنجانده شده‌اند (به پیوست پ نیز مراجعه شود).

۲۸-۳

کلید درستی‌سنجی عمومی[7]

کلید عمومی که تبدیل درستی‌سنجی عمومی را مشخص می‌کند.

1- Private signature key
2- Public encryption key
3- Public key
4- Public key certificate (certificate)
5- Certification authority
6- public key information
7- Public verification key

۲۹-۳

عدد تصادفی[1]

پارامتر متغیر با زمان که مقدار آن قابل پیش‌بینی نیست (به پیوست ب نیز مراجعه شود).

۳۰-۳

حمله‌ی بازتاب[2]

ظاهرسازی که شامل برگرداندن پیامی از پیش فرستاده شده به فرستنده آن است.

۳۱-۳

حمله‌ی بازپخش[3]

ظاهرسازی باز ارسال پیام های از پیش فرستاده شده است.

۳۲-۳

عدد دنباله‌ای[4]

پارامتر متغیر با زمان که مقدار آن از طریق یک دنباله مشخص است که در هر بازه‌ی زمانی معین تکرارنشدنی به دست می‌آید.

یادآوری- به پیوست ب نیز مراجعه شود.

۳۳-۳

فن رمزنگاشتی متقارن[5]

فن رمزنگاشتی که از یک کلید سری یکسان برای تبدیل در سازنده و گیرنده استفاده می‌کند.

یادآوری- بدون آگاهی از کلید سرّی، محاسبه تبدیل سازنده یا گیرنده امکان‌پذیر نیست.

۳۴-۳

الگوریتم رمزبندی متقارن[6]

الگوریتم رمز بندی که از یک کلید سری یکسان برای تبدیل در سازنده و گیرنده استفاده می‌کند.

۳۵-۳

مهر زمانی[7]

پارامتر متغیر با زمان که نشان‌دهنده‌ی یک نقطه‌ی زمانی نسبت به یک مرجع مشترک است.

یادآوری- به پیوست ب نیز مراجعه شود.

1- Random number
2- Reflection attack
3- Replay attack
4- Sequence number
5- Symmetric cryptographic technique
6- Symmetric encryption algorithm
7- Time stamp

۳۶-۳

پارامتر متغیر با زمان[1]

قلم داده‌ای که برای درستی‌سنجی بازپخش نبودن یک پیام استفاده می‌شود، مانند عدد تصادفی، مهر زمانی یا عدد دنباله‌ای

یادآوری- به پیوست ب نیز مراجعه شود.

۳۷-۳

نشانه[2]

پیامی که از تعدادی فیلد داده[3] مرتبط با یک ارتباط[4] ویژه تشکیل شده و با استفاده از فن رمزنگاشتی تبدیل می‌شود.

۳۸-۳

طرف سوم قابل اعتماد[5]

متولی امنیت یا نماینده‌ی آن که با توجه به فعالیت‌های مرتبط امنیتی، مورد اعتماد سایر هستارها باشد.

یادآوری- بر اساس استاندارد ISO/IEC 9798، یک طرف سوم قابل اعتماد، در جهت اهداف احراز هویت، مورد اعتماد خواهان و / یا درستی سنج است.

۳۹-۳

احراز هویت یک جانبه[6]

احراز هویت هستاری که یک هستار را از هویت دیگری مطمئن می‌سازد اما نه برعکس می‌باشد.

۴۰-۳

درستی‌سنج[7]

هستاری که نیاز به یک هویت احراز هویت شده دارد، یا آن را نمایندگی می‌کند.

یادآوری- یک درستی‌سنج محتوی توابع لازم برای درگیری در مبادلات احراز هویت را در بر دارد.

1- Time variant parameter
2- token
3- Data Field
4- Communication
5- Trusted third party
6- Unilateral authentication
7- Verifier

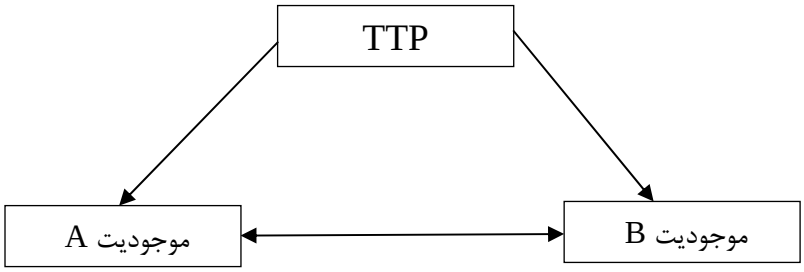
۴ نمادها و کوته نوشت

A	شناسه تشخیص‌دهنده‌ی هستار A
B	شناسه تشخیص‌دهنده‌ی هستار B
TP	شناسه تشخیص‌دهنده هستار طرف سوم قابل اعتماد
TTP[1]	طرف سوم قابل اعتماد
Kxy	کلید سری مشترک بین هستارهای X و Y، مورد استفاده در فنون رمزنگاشتی متقارن
Px	کلید درستی‌سنجی عمومی هم‌بسته به هستار X، مورد استفاده در فنون رمزنگاشتی نامتقارن
Sx	کلید امضای عمومی هم‌بسته به هستار X، مورد استفاده در فنون رمزنگاشتی نامتقارن
Nx	عدد دنباله‌ی صادر شده توسط هستار X
Rx	عدد تصادفی صادر شده توسط هستار X
Tx	مهر زمان صادر شده توسط هستار X
Tx/Nx	پارامتر متغیر با زمان ایجاد شده توسط هستار X که یا مهر زمان Tx است یا عدد دنباله‌ای Nx
Y||Z	نتیجه الحاق[2] اقلام داده‌ای Y و Z به ترتیب مشخص شده است. در مواردی که دو یا چند مورد داده‌ای الحاقی ورودی یک الگوریتم رمزنگاشتی، به عنوان قسمتی از یک سازوکار احراز هویت هستند، این نتیجه به گونه‌ای ترکیب خواهد شد که بتوان منحصرا آن را به رشته‌های داده‌ای سازنده‌اش تجزیه نمود، یا به عبارت دیگر هیچ‌گونه احتمال ابهام در تفسیر وجود نداشته باشد. می‌توان به این ویژگی پایانی، بسته به برنامه کاربردی، از راه‌های گوناگون دست یافت. به عنوان مثال، این ویژگی را می‌توان به دو طریق تضمین نمود: (الف) تثبیت طول هرکدام از زیررشته‌ها در کل دامنه‌ی استفاده از سازوکار؛ (ب) کد بندی زنجیره‌ی رشته‌های متوالی با استفاده از روشی که کدگشایی یکتایی را ضمانت کند، مثلاً استفاده از قوانین برجسته‌ی کد بندی که در ISO/IEC 8825-1[3] بیان شده است.
$e_K(Z)$	نتیجه‌ی رمز بندی داده Z با یک الگوریتم رمز بندی متقارن با استفاده از کلید K.
$d_K(Z)$	نتیجه‌ی رمزگشایی داده Z با یک الگوریتم رمزبندی متقارن با استفاده از کلید K.
$f_K(Z)$	یک مقدار وارسی رمزنگاشتی که نتیجه‌ی اعمال تابع وارسی رمزنگاشتی f با ورودی کلید سرّی K و رشته داده‌ی دلخواه Z می‌باشد.
CertX	گواهی یک طرف سوم قابل اعتماد برای هستار X.
TokenXY	یک نشانه که از هستار X به هستار Y فرستاده می‌شود.
TVP	یک پارامتر متغیر با زمان

1- Trusted Third Party
2- Concatenation

$sSX(Z)$ امضای حاصل از اعمال تبدیل امضای خصوصی بر داده‌ی Z با استفاده از کلید امضای خصوصی S_X

۵ مدل احراز هویت



شکل ۱- مدل احراز هویت

مدل کلی برای سازوکار احراز هویت هستار در شکل ۱ نشان داده شده است. نمایش تمامی هستارها و مبادلات در هر سازوکار احراز هویت ضروری نیست.

برای سازوکارهای احراز هویت مشخص‌شده در دیگر قسمت‌های ISO/IEC 9798 و برای احراز هویت یک جانبه، هستار A خواهان و هستار B درستی‌سنج در نظر گرفته شده‌اند. برای احراز هویت دوجانبه A و B هردو نقش خواهان و درستی‌سنج را با هم ایفا می‌کنند.

به منظور احراز هویت، هستارها پیام‌های استاندارد به نام نشانه‌ها، تولید و مبادله می‌کنند. برای احراز هویت یک جانبه، مبادله‌ی حداقل یک نشانه و برای احراز هویت دوجانبه، مبادله‌ی حداقل دو نشانه لازم است. در صورتی که برای آغاز یک مبادله‌ی احراز هویت نیاز به ارسال یک چالش باشد، احتمالا به یک گذر اضافه نیاز خواهد بود. در صورت درگیری یک طرف سوم قابل اعتماد نیز احتمال نیاز به گذرهای اضافی وجود خواهد داشت.

خطوط موجود در شکل ۱ نشان‌دهنده‌ی جریان احتمالی اطلاعات هستند. هستارهای A و B ممکن است به طور مستقیم یا از طریق طرف سوم قابل اعتماد به ترتیب با B یا A در تعامل بوده و یا از اطلاعات صادره از طرف سوم استفاده کنند.

جزئیات سازوکارهای احراز هویت ISO/IEC 9798 در قسمت‌های بعدی بیان می‌شوند.

۶ الزامات کلی و محدودیت‌ها

برای اینکه یک هستار بتواند هستار دیگری را احراز هویت کند، هر دو باید از مجموعه‌ی مشترکی از فنون و پارامترهای رمزنگاشتی استفاده نمایند.

در طول عمر یک کلید، مقادیر تمامی پارامترهای متغیر زمان که بر روی آن‌ها عمل می‌کند (یعنی مهر زمان‌ها، عددهای دنباله‌ای و عددهای تصادفی) با احتمال قوی، باید تکرارنشدنی باشند.

فرض بر آن است که طی استفاده از یک سازوکار احراز هویت، هستارهای A و B از هویت‌های ادعایی یکدیگر آگاه هستند. این امر با گنجاندن شناسه‌ها در مبادلات اطلاعات بین دو هستار و یا به وضوح از بافت استفاده از سازوکار قابل دستیابی خواهد بود.

اعتبار هستار تنها می‌تواند در لحظه‌ی مبادله احراز هویت محقق شود. بنابراین به منظور تضمین اعتبار داده-های مرتبط بعدی، مبادله‌ی احراز هویت باید به همراه یک شیوه‌ی امنیتی ارتباطی استفاده گردد.

پیوست الف
(اطلاعاتی)
استفاده از فیلد متنی

نشانه‌های بیان شده در قسمت‌های بعدی استاندارد ISO/IEC 9798 شامل فیلدهای متنی هستند. استفاده‌ی واقعی و ارتباط بین دسته های متنی متنوع، در یک گذر معین، وابسته به نوع کاربرد است.

فیلد متنی ممکن است شامل پارامترهای اضافی متغیر زمان باشد. برای مثال، یک مهر زمانی، در صورت استفاده‌ی سازوکار از عددهای دنباله‌ای، در فیلد(ها)ی متن یک نشانه گنجانده خواهد شد. این مسئله با الزام گیرنده پیام به درستی‌سنجی هر مهر زمانی موجود در پیام، در یک پنجره‌ی زمانی پیش معین وجود دارد، موجب تشخیص تأخیرهای تحمیلی می‌شود (به پیوست ب نیز مراجعه شود).

اگر بیش از یک کلید معتبر وجود دارد، آنگاه می‌توان یک شناسه برای کلید، در فیلدهای متنی درون متن ساده قرار داد. اگر بیش از یک طرف سوم مورد اعتماد وجود دارد، آنگاه می‌توان از فیلدهای متنی برای دربرگرفتن شناسه‌ی تشخیص دهنده‌ی طرف سوم مورد نظر استفاده نمود.

فیلدهای متنی برای توزیع کلیدها نیز قابل استفاده هستند (به ISO/IEC 11770-2 و ISO/IEC 11770-3 مراجعه شود).

اگر هرکدام از سازوکارهای بیان شده در قسمت‌های بعدی استاندارد ISO/IEC 9798 در یک برنامه کاربردی نهفته باشند که به هر هستار اجازه می‌دهد احراز هویت را از طریق یک پیام اضافه شده قبل از شروع سازوکار آغاز کند، حمله‌ی نفوذی[1] مسلم خواهد بود. فیلدهای متنی مشخص می‌کنند کدام هستار احراز هویت برای مقابله با حملاتی را که نشانه‌ی بارز امکان استفاده مجدد یک نفوذی از یک نشانه‌ی غیرقانونی هستند، درخواست می‌نماید (به استاندارد ملی۲-۱۰۱۸۱مراجعه شود).

مثال‌های بالا جامع[2] نیستند.

1- Intruder attack
2 - Exhaustive

پیوست ب
(اطلاعاتی)
پارامترهای متغیر زمان

ب-۱ پارامترهای سه‌تایی متغیر با زمان

پارامترهای متغیر با زمان برای کنترل یکتایی/ جدول زمانی[1] استفاده می‌شوند. این پارامترها برای شناسایی، امکان بازپخش پیام‌های ارسالی قبلی را فراهم می‌آورند. بدین منظور، اطلاعات احراز هویت باید از یک مبادله به مبادله‌ی بعدی تغییر نماید.

برخی از انواع پارامترهای متغیر زمان مجاز به تشخیص «تأخیرهای تحمیلی» (تأخیرهای وارد شده در رسانه‌ی ارتباطی توسط یک رقیب) نیز هستند. در سازوکارهای در برگیرنده‌ی بیش از یک گذر، تاخیرهای تحمیلی، به شیوه‌های دیگر نیز قابل شناسایی خواهند بود (ازجمله پالس زمان پایانی[2] برای اعمال وقفه‌های زمانی مجاز بین پیام‌های معین)

پارامترهای سه‌تایی متغیر با زمان که در قسمت‌های بعدی ISO/IEC 9798 مورد استفاده قرار می‌گیرند، شامل مهر زمانی، عددهای دنباله‌ای و عددهای تصادفی هستند. بسته به الزامات پیاده‌سازی، انواع گوناگون پارامترهای متغیر با زمان در کاربردهای گوناگون ارجح می‌گردد. در برخی موارد نیز استفاده بیش از یک نوع پارامتر متغیر با زمان مناسب خواهد بود (مانند مهر زمانی و عددهای دنباله‌ای با هم). جزئیات انتخاب این پارامترها فراتر از دامنه‌ی این قسمت از ISO/IEC 9798 می‌باشد.

ب-۲ مهر زمانی

سازوکارهای محتوی مهر زمانی‌ها از یک مرجع زمانی رایج ستفاده می‌کنند که خواهان و درستی‌سنج را به صورت منطقی به هم مرتبط می‌سازد. ساعت مرجع پیشنهادی، زمان هماهنگ جهانی[3] (CTU) است. یک پنجره تأیید، در اندازه‌های ثابت، توسط درستی‌سنج استفاده می‌شود. درستی‌سنج با محاسبه اختلاف بین مهر زمانی، در یک نشانه‌ی دریافتی مجاز، و زمانی که نشانه را دریافت می‌کند، می‌تواند به موقع بودن پیام را کنترل نماید. اگر این اختلاف در بازه‌ی زمانی پنجره باشد، پیام پذیرفته خواهد شد. یکتایی پیام از طریق ورود تمامی پیام‌ها در پنجره کنونی، و رد کردن پیشامدهای بعدی پیام‌های مشابه در آن پنجره، تایید می‌شود.

برخی از سازوکارها برای اطمینان از همزمانی ساعت– زمان‌های[4] هستارهای مرتبط باید به کار برده شود. به علاوه، ساعت- زمان‌ها باید به خوبی باهم همزمان شوند تا احتمال جعل هویت از طریق بازپخش به طور قابل قبولی کاهش یابد. همچنین تمامی اطلاعات مربوط به درستی‌سنجی مهر زمانی، در هستارهای مرتبط، باید در برابر تغییر یا استفاده حفاظت شوند.

سازوکارهایی که از مهر زمانی استفاده می‌کنند، تشخیص تأخیرهای تحمیلی را مجاز می‌دانند.

1- Uniqueness/ Timelines
2- Timeout clocks
3- Coordinated Universal Time
4- Time clocks

ب-۳ عددهای دنباله‌ای

یکتایی پیام را می‌توان از طریق عددهای دنباله‌ای کنترل کرد زیرا این عددها درستی‌سنج را قادر به تشخیص بازپخش پیام‌ها می‌سازند. خواهان و درستی‌سنج ابتدا به گونه‌ای خاص بر سر یک سیاست برای شماره‌گذاری پیام‌ها توافق می‌کنند، ایده‌ی کلی آن است که پیامی با یک شماره‌ی خاص تنها یک بار (یا در یک بازه‌ی زمانی معین تنها یک بار) پذیرفته شود. سپس پیام‌های دریافتی از درستی‌سنج بررسی می‌شوند تا مشخص شود شماره فرستاده شده به همراه پیام، بر اساس سیاست توافقی، قابل قبول است. اگر عدد دنباله-ی همراه مطابق با سیاست توافقی نباشد، پیام پذیرفته نخواهد شد.

استفاده از عددهای دنباله‌ای نیازمند کار اضافی[1] خواهد بود. خواهان باید سوابق عدد دنباله‌های استفاده شده‌ی قبلی یا آن‌هایی که برای استفاده بعدی معتبرند را نگه‌داری کند. خواهان نیاز خواهد داشت این سوابق را برای تمامی درستی‌سنج‌های احتمالی به منظور ارتباط، نگه‌داری نماید. به صورت مشابه، درستی-سنج نیز باید چنین سوابقی را برای تمامی خواهان‌های احتمالی نگه‌داری کند. همچنین روش اجرایی خاصی برای تنظیم یا شروع مجدد شمارنده‌های عددهای دنباله‌ای، وقتی موقعیت‌هایی (مانند خرابی‌های سامانه) توالی معمول را برهم می‌زند، مورد نیاز است. استفاده‌ی خواهان از عددهای دنباله‌ای، توانایی درستی‌سنج برای تشخیص تأخیرهای تحمیلی را تضمین نمی‌کند. برای سازوکارهایی شامل دو یا چند پیام، اگر فرستنده‌ی پیام وقفه‌ی زمانی بین ارسال یک پیام و دریافت جواب مورد انتظار را اندازه‌گیری کند، تأخیرهای تحمیلی قابل تشخیص خواهند بود، و اگر این تأخیر بیشتر از مدت زمان از پیش مشخص شده باشد، آن پیام پذیرفته نخواهد شد.

ب-۴ اعداد تصادفی

اعداد تصادفی مورد استفاده در سازوکارهای بیان شده در قسمت‌های بعدی استاندارد ISO/IEC 9798، از حملات بازپخش و تفکیک‌کننده جلوگیری می‌کنند. بنابراین تمامی عددها تصادفی مورد استفاده در استاندارد ISO/IEC 9798 باید از محدوده‌ی به اندازه‌ی کافی بزرگی انتخاب شوند تا احتمال تکرار هنگام استفاده از کلید یکسان و همچنین احتمال پیش‌بینی یک مقدار معین توسط طرف سوم بسیار کاهش یابد. بر اساس استاندارد ISO/IEC 9798، استفاده از اصطلاح عددهای تصادفی، شامل عددهای شبه- تصادفی که الزامات یکسانی را برآورده می‌سازند نیز می‌شود.

به منظور جلوگیری از حملات بازپخش یا تفکیک‌کننده، درستی‌سنج یک عدد تصادفی برای ارسال به خواهان فراهم می‌آورد و خواهان با گنجاندن این عداد تصادفی در قسمت محافظت‌شده‌ی نشانه‌ی بازگشتی خود به درستی‌سنج پاسخ می‌دهد (معمولا به آن چالش-پاسخ اطلاق می‌شود). این روش اجرایی[2] دو پیام شامل با عددهای تصادفی خاص را به هم پیوند می دهد . اگر عددها تصادفی یکسانی باید مجددا توسط درستی‌سنج استفاده شود، طرف سومی که مبادله‌ی احراز هویت اصلی را ضبط کرده می‌تواند نشان ضبط

1- Book keeping
2 Procedure

شده را برای درستی‌سنج فرستاده و به دروغ خود را به عنوان خواهان بشناساند. بنابراین برای جلوگیری از چنین حملاتی، عددها تصادفی باید با احتمال بالایی تکرارنشدنی باشد.

استفاده‌ی خواهان از عددها تصادفی، توانایی درستی‌سنج برای تشخیص تأخیرهای تحمیلی را تضمین نمی‌کند.

استاندارد ISO/IEC 18031 فنونی برای تولید عددها تصادفی، برای برنامه‌های کاربردی رمزنگاشتی، مشخص‌می‌کند.

پیوست پ
(اطلاعاتی)

گواهی‌نامه‌ها

در برخی از سازوکارهای مشخص‌شده در قسمت‌های بعدی ISO/IEC 9798، گواهی‌نامه‌های کلید عمومی (گواهی‌نامه‌ها) را می‌توان برای اطمینان از اعتبار کلیدهای عمومی استفاده کرد. در این حالت یک گواهی‌نامه، اطلاعات کلید عمومی یک هستار را، که حداقل شامل شناسه تشخیص هستار و کلید عمومی است، در برمی‌گیرد. احتمالا اطلاعات دیگری در اطلاعات کلید عمومی در مورد طرف سوم قابل اعتماد، هستار و کلید عمومی وجود دارد، از جمله مدت زمان اعتبار کلید عمومی، مدت زمان اعتبار کلید خصوصی وابسته، یا شناسه‌های الگوریتم‌های درگیر. گواهی‌نامه شامل اطلاعات کلید عمومی است که به وسیله طرف سوم مورد اعتماد امضا شده است.

درستی‌سنجی یک گواهی‌نامه شامل درستی‌سنجی امضای طرف سوم مورد اعتماد، وارسی و دیگر شرایط مربوط به اعتبار گواهی‌نامه، مانند مدت زمان اعتبار یا ابطال در صورت لزوم است.

گواهی‌نامه‌ها تنها راه ضمانت اعتبار کلیدهای عمومی نیستند. برای اینکه یک هستار، مجاز به دستیابی به کلیدهای عمومی دیگرهستارها به شیوه‌های دیگر باشد، استفاده از گواهی‌نامه‌ها در تمامی سازوکارها در قسمت‌های بعدی استاندارد ISO/IEC 9798 اختیاری است. سایر روش‌های ضمانت اعتبار کلیدهای عمومی شامل طرح‌های امضای هویت محور می‌باشد، مانند موارد بیان شده در استاندارد ISO/IEC 14888-2.

کتاب‌نامه

[1] ISO/IEC 7498-1:1994, *Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*

[2] ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic*
Reference Model — Part 2: Security Architecture

[3] ISO/IEC 8825-1:2002, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

[۴] استاندارد ملی۸-۱۱۰۸۷: سال ۱۳۸۷ فناوری اطلاعات - اتصال سامانه های باز - دایرکتوری : چارجوب های گواهینامه کلید عمومی وگواهینامه نشان

[5] ISO/IEC 9796-2:2002, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*

[6] ISO/IEC 10181-1:1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview*

[۷] استاندارد ملی۲-۱۰۱۸۱: سال ۱۳۸۸ فناوری اطلاعات- اتصال متقابل سامانه های باز- چارچوب های کاری امنیتی برای سامانه های باز: چارچوب کاری احراز هویت

[8] ISO/IEC 11770-1:1996, *Information technology — Security techniques — Key management — Part 1: Framework*

[9] ISO/IEC 11770-2:2008, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*

[۱۰] استاندارد ملی۳-۱۰۸۲۲: سال ۱۳۸۷فناوری اطلاعات-فنون امنیتی-مدیریت کلید-قسمت ۳-ساز و کارهای مبتنی بر فنون نامتقارن

[11] ISO/IEC 13888-1:2009, *Information technology — Security techniques — Non-repudiation — Part 1: General*

[۱۲] استاندارد ملی ۱-۱۱۴۹۴: سال ۱۳۸۷ فناوری اطلاعات-فنون امنیت- امضاهای دیجیتال با پیوست- قسمت ۱-کلیات

[13] ISO/IEC 14888-2:2008, *Information technology — Security techniques — Digital signatures with appendix — Part 2: Integer factorization based mechanisms*

[14] ISO/IEC 14888-3:2006, *Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms*

[15] ISO/IEC 18031:2005, *Information technology — Security techniques — Random bit generation*