INSO
10825-3
1st. Edition
May.2013

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۱۰۸۲۵-۳
چاپ اول
اردیبهشت ۱۳۹۲

فناوری اطلاعات – فنون امنیتی- احراز هویت هستار قسمت ۳: سازوکارهای استفاده کننده از فنون امضای رقمی (دیجیتال)

Information Technology - Security Techniques — Entity Authentication Part3: Mechanisms Using Digital Signature Techniques

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-احراز هویت هستار

قسمت ۳: سازوکارهای استفاده از فنون امضای رقمی (دیجیتال) »

رئیس :	**سمت و یا نمایندگی**
فولادیان، مجید (فوق لیسانس مهندسی برق مخابرات)	مشاور سازمان فناوری اطلاعات
دبیر :	
میراسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم افزار)	مدیر کل خدمات ارزش افزوده سازمان فناوری اطلاعات
اعضا: (اسامی به ترتیب حروف الفبا)	
امیریان، احسان (کارشناس ارشد مهندسی کامپیوتر - نرم‌افزار)	مدیرعامل شرکت هوشمندی تجاری تالی
بختیاری، شیرین (کارشناسی مهندسی برق)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
جمیل پناه، ناصر (فوق لیسانس مدیریت)	کارشناس سازمان فناوری اطلاعات
خوشنویسان، نازنین (لیسانس مهندسی نرم‌افزار)	نماینده دانشگاه شهید بهشتی
سعیدی، عذرا (فوق لیسانس مهندسی برق مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
سلطانی حقیقت، الهه (لیسانس مهندسی برق مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
فرهاد شیخ احمد، لیلا (فوق لیسانس مهندسی کامپیوتر نرم افزار)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات

فیاضی، مهدی (لیسانس مهندسی برق مخابرات)	کارشناس مسئول تدوین استاندارد و امنیت شبکه سازمان فناوری اطلاعات
قسمتی، سیمین (فوق لیسانس فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فنـاوری اطلاعات
مزینی، ناصر (دکتری کامپیوتر)	استادیار دانشگاه علم و صنعت ایران
معروف، سینا (لیسانس مهندسی کامپیوتر)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
موجبی، محمود (فوق لیسانس مخابرات)	کارشناس تدوین استاندارد سازمان فنـاوری اطلاعات
میرزایی رضایی، طیبه (فوق لیسانس فیزیک)	رئیس اداره تدوین استانداردها و نظـارت بـر امنیت سرویس‌ها سازمان فناوری اطلاعات
ناظمی، اسلام (دکتری کامپیوتر)	استادیار دانشگاه شهید بهشتی
نیسی مینایی، آصف (لیسانس مهندسی فناوری اطلاعات)	نماینده دانشگاه شهید بهشتی

فهرست مندرجات

پیش‌گفتار

استاندارد « فناوری اطلاعات – فنون امنیتی – احراز هویت هستار - قسمت ۳: سازوکارهای استفاده کننده از فنون امضای رقمی (دیجیتال) » که پیش نویس آن درکمیسیون‌های مربوط توسط سازمان فناوری اطلاعات تهیه و تدوین شده و در دویست و نوزدهمین اجلاس کمیتهٔ ملی استاندارد رایانه و فرآوری داده مورخ ۹۱/۹/۲۷ 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 پیشرفت‌های 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.

منابع و ماخذی که برای تهیهٔ این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 9798-3: 1998, Information technology — Security techniques — Entity authentication — Part 3: Mechanisms using digital signature techniques+ Technical Corrigendum 1: 2009 + Technical Corrigendum 2: 2010 + Amendment 1:2010

فناوری اطلاعات – فنون امنیتی- احراز هویت هستار
قسمت ۳: سازوکارهای استفاده کننده از فنون امضای رقمی (دیجیتال)

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین مشخصات سازوکارهای احراز هویت هستار با استفاده از امضای رقمی(دیجیتال) بر پایه‌ی فنون نامتقارن است. دو سازوکار براساس احراز هویت تک هستار (احراز هویت یک جانبه) وجود دارد، در حالیکه باقی سازوکارها برای احراز هویت دوجانبه از دو هستار می‌باشند. امضای رقمی برای تایید هویت یک هستار استفاده می‌شود. بهره‌گیری از یک طرف سوم مورد اعتماد نیز مجاز است.
سازوکارهای معرفی شده در این استاندارد از پارامترهای زمان مانند مهرهای زمانی، اعداد دنباله‌ای یا اعداد تصادفی، برای جلوگیری از پذیرش اطلاعات معتبر یک عمل احراز هویت در یک زمانی دیرتر استفاده می‌کنند.
اگر از یک مهر زمانی یا یک عدد دنباله‌ای استفاده شود آنگاه برای احراز هویت یک جانبه، یک مرحله لازم است در حالی که برای دست‌یابی به احراز هویت‌های متقابل به دو مرحله نیاز است. اگر یک روش چالش و پاسخ که از اعداد تصادفی بهره می‌گیرد مورد استفاده قرار گیرد، دو مرحله برای احراز هویت یک جانبه لازم خواهد بود، در حالی که برای احراز هویت متقابل، سه یا چهار مرحله (که با توجه به سازوکار استفاده شده تعیین می‌شود) لازم خواهد بود.

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 می شود.
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 تاریخ تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است .
استفاده از مرجع زیر برای این استاندارد الزامی است:

۲-۱ استاندارد ملی شماره ۱-۹۷۹۸ : سال ۱۳۹۱ فناوری اطلاعات – فنون امنیتی – احراز هویت هستار – قسمت ۱ : کلیات

۳ اصطلاحات و تعاریف

در این استاندارد، تعارف و علائم توصیف شده در استاندارد ملی شماره ۱-۹۷۹۸ : ۱۳۹۱و آنچه در زیر آورده شده به‌کار می‌رود:

IA هویت هستار A، که می‌تواند A و یا CertA باشد.

IB هویت هستار B، که می‌تواند B و یا CertB باشد.

ResX نتیجه وارسی هستار کلید عمومی X و یا گواهینامه آن کلید عمومی

همان‌طور که در استاندارد ملی شماره ۱-۹۷۹۸ : ۱۳۹۱ تعریف شده، X||Y برای تعریف نتیجه الحاق تکه‌های داده X و Y طبق دستور مشخص شده مورد استفاده قرار می‌گیرد. در مواردی که نتیجه الحاق دو یا چند داده به‌عنوان بخشی از مکانیزم مشخص شده در این استاندارد تعیین شده باشد، این نتیجه باید ترکیب شود تا بتواند به طور یکتا با بخش اصلی رشته‌های داده خود، یکپارچه شود، به این معنی که امکان ابهام در تفسیر داده‌ها وجود نداشته باشد. این مشخصه با توجه به برنامه مورد استفاده به راه‌های گوناگونی قابل دسترسی است. به طور مثال، این مشخصه (الف) با تنظیم طول هر کدام از زیر رشته‌ها در کل محدوده استفاده از مکانیزم و یا (ب) به وسیله رمزگذاری ترتیب رشته‌های اضافه شده با استفاده از روشی که رمزگشایی منحصر به فرد را تضمین می‌کند، قابل انجام است. به طور مثال استفاده از قوانین متمایز رمزگذاری در استاندارد ISO/IEC 8825-1 [1].

۴ الزامات

در سازوکارهای احراز هویت مورد بحث در این استاندارد، هستاری که مورد احراز هویت قرار خواهد گرفت، با نشان دادن دانش خود از کلید امضای خصوصی خود، هویت خود را تایید می‌کند. این به وسیله هستاری که از کلید امضای خصوصی خود برای امضا نمودن اطلاعات مشخصی استفاده می‌کند، به دست می‌آید. امضای هستار به وسیله هر کس که کلید عمومی هستار را در اختیار داشته باشد، می‌تواند مورد پذیرش و تایید قرار گیرد.

سازوکارهای تشخیص هویت نیازمندی‌های زیر را دارند:

الف- یک تایید کننده باید کلید عمومی معتبر هستار خواهان، یعنی هستاری که خواهان اظهار به بودن می‌کند، را در اختیار داشته باشد.

ب- یک هستار خواهان، باید یک کلید امضای خصوصی که فقط خودش از آن اطلاع دارد و استفاده می‌کند، داشته باشد.

پ- کلید امضای خصوصی که برای پیاده‌سازی هر یک از سازوکارهای مشخص‌شده در این استاندارد، باید از کلیدهایی که با اهداف دیگری استفاده شده‌اند جدا شود.

ت- رشته داده‌هایی که در سازوکار احراز هویت در چندین نقطه امضا شده‌اند نباید دستکاری شوند تا بتوان آن‌ها را ارسال کرد.

یادآوری- برای رعایت این مورد می‌توان عناصر زیر را به هر رشته داده امضا شده اضافه کرد:

- شناساگر شیء که در پیوست ب مشخص شده است. به طوری خاصی که در استاندارد آمده، شماره بخش و سازوکار احراز هویت؛

- ثابتی که به‌طور منحصر به فرد برای شناسایی رشته در سازوکار به کار برود. برای سازوکارهایی که فقط یک رشته را امضا می‌کنند این ثابت قابل حذف است.

گیرنده امضا باید شناساگر شیء و ثابت شناسایی امضا را که در سازوکار قرار گرفته تصدیق کند که همانی باشد که انتظار می‌رود.
اگر هرکدام از این موارد برآورده نشود، ممکن است فرایند احراز هویت لو برود یا به طور کامل موفق نباشد.

یادآوری ۱- یک راه برای به‌دست آوردن کلید عمومی معتبر، استفاده از گواهی است. (پیوست پ از استاندارد ISO/IEC 9798-1 را مشاهده فرمایید). تولید، پخش، و لغو گواهی‌ها از دامنه بررسی استاندارد ISO/IEC 9798-1 خارج است. ممکن است طرف سوم قابل اعتمادی به این منظور وجود داشته باشد. راه دیگر برای به دست آوردن کلید عمومی معتبر استفاده از پیک‌های مورد اعتماد است.

یادآوری ۲- مراجع به طرح‌واره‌های امضای رقمی در کتاب‌نامه همین استاندارد آورده شده‌اند.

۵ سازوکارها

سازوکارهای احراز هویت هستار مشخص شده، از پارامترهای متغیر با زمان مانند مهرهای زمانی، اعداد دنباله‌ای و اعداد تصادفی استفاده می‌کنند. (به پیوست ب از استاندارد ISO/IEC9798-1[1] و یادآوری ۱ زیر این بند مراجعه شود.)
در این استاندارد، نشانه‌ها فرم زیر را خواهند داشت:

$$Token = X_1 || \dots ||X_t||sS_A(Y_1|| \dots ||Y_j)$$

در این قسمت از استاندارد ملی اصطلاح داده‌ی امضا شده به "$Y_1|| \dots ||Y_j$" اشاره دارد که به عنوان ورودی طرح‌واره امضا استفاده شده و اصطلاح "داده‌ی امضا نشده" به "$X_1||\dots||X_i$" اشاره دارد. اگر اطلاعات داده‌ی امضا شده‌ی نشانه بتواند از امضا بازیافت شود، آنگاه دیگر نیازی نخواهد بود تا این اطلاعات در داده امضا نشده‌ی نشانه وجود داشته باشد (برای مثال استاندارد ISO/IEC 9796 را مراجعه شود).
اگر اطلاعات موجود در فیلد متنی داده امضا شده‌ی نشانه را نتوان از امضا بازیافت کرد، آنگاه باید این داده‌ها در فیلد متنی امضا نشده‌ی نشانه وجود داشته باشد. اگر اطلاعات موجود در داده‌های امضا شده‌ی نشانه (مانند یک عدد تصادفی) از قبل برای تایید کننده، مشخص باشد، آنگاه نیازی نیست این داده‌ها توسط هستار خواهان در اطلاعات امضا نشده‌ی نشانه فرستاده شود. همه‌ی فیلدهای متنی مشخص شده در سازوکارهای زیر برای استفاده در کاربردهای بیرون از حوزه این استاندارد در دسترس است. (ممکن است

[1] - معادل استاندارد شماره ۱-۹۷۹۸ : سال ۱۳۹۱ موجود می‌باشد

خالی باشند.) وابستگی و محتوای این فیلدها به کاربرد خاص آن‌ها بستگی دارد. پیوست الف را برای آشنایی بیشتر با نحوه استفاده از فیلدهای متنی مراجعه شود.

یادآوری ۱- می‌توان از امضا شدن بسته داده یک هستار که این بسته داده توسط یک هستار دومی و به دلایلی مورد تغییر قرار گرفته، به وسیله هستار اول و با وارد کردن عدد تصافی موجود در بسته داده امضا شده توسط آن جلوگیری کرد. در این مورد، در حقیقت این غیر قابل پیش‌بینی بودن است که جلوی امضای یک داده از قبل تعریف شده را می‌گیرد.

یادآوری ۲- به دلیل اینکه توزیع گواهی‌ها خارج از حوزه این استاندارد است، فرستادن گواهی‌ها نیز برای تمام سازوکارها اختیاری است.

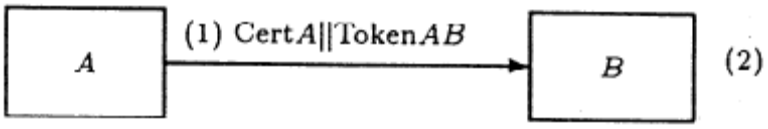
۵-۱ احراز هویت یک جانبه

احراز هویت یک جانبه به معنی احراز هویت یکی از دو هستار با استفاده از سازوکار است.

۵-۱-۱ احراز هویت یک مرحله‌ای

در این سازوکار تشخیص هویت، خواهان A روند احراز هویت را شروع کرده و توسط تاییدکننده B احراز هویت می‌شود. یکتایی یا جدول زمانی، به‌وسیله تولید و وارسی‌کردن یک مهر زمانی و یا یک عدد دنباله‌ای کنترل می‌شود. (پیوست ب از استاندارد ISO/IEC 9798-1 مراجعه شود)

سازوکار احراز هویت در شکل ۱ خلاصه شده است:



شکل ۱: احراز هویت یک مرحله‌ای

فرم نشانه (نشانهAB) که از طرف خواهان A به تاییدکننده B فرستاده شده به صورت زیر است :

$$TokenAB = \frac{T_A}{N_A}||B||Text2||sS_A\left(\frac{T_A}{N_A}||B||Text1\right)$$

جایی که خواهان A از یک عدد دنباله‌ای N_A یا یک مهر زمانی T_A به عنوان پارامتر زمان استفاده کرده است. انتخاب بین N_A و T_A به قابلیت‌های فنی خواهان و تاییدکننده و همچنین محیط اجرا بستگی دارد.

یادآوری ۱- وجود شناساگرB در داده امضا شده‌ی نشانه AB برای جلوگیری از مورد پذیرش قرار گرفتن آن به وسیله فرد دیگری غیر از تایید کننده تعیین شده، ضروری است.

یادآوری ۲- به‌طور کلی، Text2 با این فرآیند احراز هویت نمی‌شود.

یادآوری ۳- یک کاربرد از این سازوکار می‌تواند توزیع کلید باشد (به پیوست الف از استاندارد ملی شماره ۱-۹۷۹۸ : ۱۳۹۱مراجعه شود)

ساز و کار احراز هویت یک مرحله‌ای به شرح است:

(۱) A نشانه AB و به صورت اختیاری گواهی آن را برای B می‌فرستد.

(۲) در دریافت پیام حاوی نشانه AB که از طرف A فرستاده شده بود، B مراحل زیر را انجام می‌دهد:

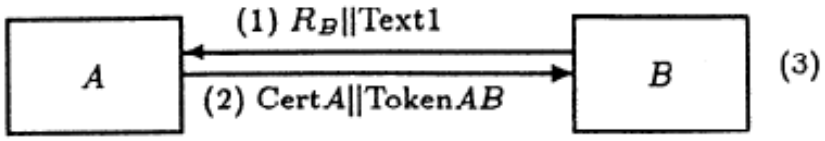
(الف) مطمئن می‌شود که یک کلید عمومی معتبر از A دارد. این کار را با وارسی گواهی فرستاده شده از طرف A و یا راه‌های دیگر انجام می‌دهد.

(ب) نشانه AB را با وارسی امضای A که در نشانه قرار گرفته، با وارسی کردن مهر زمانی یا عدد دنباله‌ای و یا با وارسی کردن اینکه شناساگرB که در داده امضا شده‌ی نشانه AB قرار گرفته با شناساگر متمایز کننده هستار B برابر است، تایید می‌کند.

۵-۱-۲ احراز هویت دو مرحله‌ای

در این سازوکار احراز هویت، خواهان A توسط تاییدکننده B که فرآیند را شروع می‌کند، احراز هویت می‌شود. یکتایی یا جدول زمانی، با تولید و وارسی‌کردن یک عدد تصادفی R_B کنترل می‌شود. (به پیوست ب از استاندارد ISO/IEC 9798-1 مراجعه شود.)

سازوکار احراز هویت دو مرحله‌ای در شکل ۲ خلاصه شده است.



شکل ۲: احراز هویت دو مرحله‌ای

فرم نشانه (نشانه AB) که از طرف خواهان A به تاییدکننده B فرستاده شده به صورت زیر است :

$$\mathrm{Token}AB = R_A||R_B||B||Text3||sS_A(R_A||R_B||B||Text2)$$

وجود شناساگر B در نشانه AB اختیاری بوده و به محیطی که این سازوکار در آن استفاده می‌شود، بستگی دارد.

یادآوری۱- گنجایش شناساگر B در داده امضا شده‌ی نشانه AB می‌تواند سبب جلوگیری از پذیرفته شدن نشانه توسط شخصی غیر از شناساگر مورد نظر شود (مانند حمله از طریق شخصی در میان[1]).

یادآوری ۲- گنجایش عدد تصادفی R_A در قسمت امضا شده‌ی نشانه AB، قبل از شروع سازوکار احراز هویت از دسترسی B به امضای A در داده انتخاب شده توسط B جلوگیری می‌کند. این اندازه‌گیری ممکن است لازم باشد؛ برای مثال زمانی که همان کلید توسط A برای اهدافی غیر از احراز هویت سازوکار زیر مورد استفاده قرار می‌گیرد.

ساز و کار احراز هویت دو مرحله‌ای به شرح است:

(۱) B عدد تصادفی R_B و به صورت اختیاری یک فیلد متن Text1 را برای A می‌فرستد.

[1]-Person-in-the-middle attack

(۲) A نشانهAB و به صورت اختیاری گواهی آن‌را به B می‌فرستد.

(۳) B در دریافت پیام شامل نشانه AB، گام‌های زیر را انجام می‌دهد:

(الف) مطمئن می‌شود که یک کلید عمومی معتبر از A دارد. این کار را با وارسی گواهی فرستاده شده از طرف A یا راه‌های دیگر انجام می‌دهد.

(ب) نشانهAB را با وارسی امضای A که در نشانه قرارگرفته، با وارسی‌کردن اینکه عدد تصادفی RB که در گام ۱ به A فرستاده شده بود، با عدد تصادفی موجود در داده امضا شده‌ی نشانهAB موافق است و یا با وارسی‌کردن اینکه شناساگر B که در داده امضا شده‌ی نشانه AB قرار گرفته با شناساگر متمایز کننده B برابر است، تایید می‌کند.

۵-۲ احراز هویت متقابل

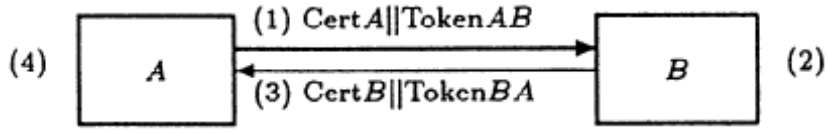
احراز هویت متقابل یعنی دو هستار مرتبط، بتوانند توسط طرف دیگر احراز هویت شوند.

دو سازوکار توصیف شده در بندهای ۵-۱-۱ و ۵-۱-۲، به ترتیب در بندهای ۵-۲-۱ و ۵-۲-۲ برای دستیابی به احراز هویت متقابل گسترش یافته‌اند. این کار با فرستادن یک پیام بیشتر که منجر به انجام دو گام اضافی می‌شود، صورت می‌گیرد. سازوکار بررسی شده در بند ۵-۲-۳ از ۴ پیام استفاده می‌کند که البته نیازی به فرستادن متوالی همه آنها نیست. با این کار ممکن است عملیات احراز هویت با سرعت بیشتری انجام شود.

۵-۲-۱ احراز هویت دو مرحله‌ای

در این سازوکار احراز هویت یکتایی یا جدول زمانی به‌وسیله تولید و وارسی کردن یک مهر زمانی و یا یک عدد دنباله‌ای کنترل می‌شود. (به پیوست ب از استاندارد ملی شماره ۱-۹۷۹۸ :۱۳۹۱ مراجعه شود.)

سازوکار احراز هویت در شکل ۳ خلاصه شده است:



شکل ۳: احراز هویت دو مرحله‌ای

فرم نشانه (نشانه AB) که از طرف A به B فرستاده شده، شبیه فرم مشخص شده در بند ۵-۱-۱ است.

$$TokenAB = \frac{T_A}{N_A}||B||Text2||sS_A\left(\frac{T_A}{N_A}||B||Text1\right)$$

فرم نشانه (نشانه BA) که از طرف B به A فرستاده می‌شود، به صورت زیر است:

$$TokenBA = \frac{T_B}{N_B}||A||Text4||sS_B\left(\frac{T_B}{N_B}||A||Text3\right)$$

انتخاب استفاده از مهرهای زمانی یا اعداد دنباله‌ای به قابلیت‌های فنی خواهان و تاییدکننده و همچنین محیط اجرا بستگی دارد.

یادآوری ۱- وارد کردن شناساگرهای A و B به ترتیب در نشانه‌های BA و AB برای جلوگیری از دریافت نشانه‌ها توسط افرادی غیر از تاییدکننده‌ی مشخص شده ضروری است.

در ساز و کار احراز هویت دو مرحله‌ای گام‌های ۱ و ۲ کاملاً همانند بند ۵-۱-۱ هستند که در قسمت احراز هویت یک مرحله‌ای بررسی شدند.

(۳) نشانهBA و به صورت اختیاری گواهی آن را به A می‌فرستد.

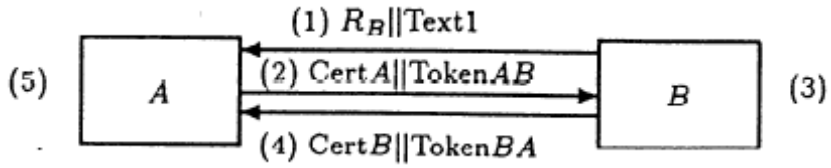
(۴) پیام در مرحله ۳ به صورت مرحله ۲ کنترل می‌شود.

یادآوری ۲- دو پیام از این سازوکار به همدیگر وصل نمی‌شوند مگر به وسیله جدول زمانی و البته به صورت ضمنی. این سازوکار در حقیقت شامل دو بار استفاده مستقل از سازوکار بند. ۵-۱-۱ است. اتصال بیشتر پیام‌ها در این سازوکار می‌تواند با استفاده مناسب از فیلدهای متنی حاصل شود.

۵-۲-۲ احراز هویت سه مرحله‌ای

در این سازوکار احراز هویت یکتایی یا جدول زمانی به‌وسیله تولید و وارسی کردن یک مهر زمانی و یا یک عدد دنباله‌ای کنترل می‌شود. (به پیوست ب از استاندارد ملی شماره ۱-۹۷۹۸ :۱۳۹۱ مراجعه شود.)

سازوکار احراز هویت در شکل ۴ خلاصه شده است:



شکل ۴: احراز هویت سه مرحله‌ای

فرم نشانه‌ها در این سازوکار، به صورت زیر است:

$$\text{Token}AB = R_A||R_B||B||Text3||sS_A(R_A||R_B||B||Text2)$$
$$\text{Token}BA = R_B||R_A||A||Text5||sS_B(R_B||R_A||A||Text4)$$

وارد کردن پارامتر B در نشانه AB و همچنین A در نشانه BA اختیاری بوده و بستگی به محیطی دارد که این سازوکار در آن مورد استفاده قرار می‌گیرد.

یادآوری- وارد کردن عدد تصادفی R_A در قسمت امضا شده‌ی نشانه AB از به دست آوردن امضای A به وسیله B در داده‌ی انتخاب شده توسط B قبل از شروع سازوکار جلوگیری می‌کند. این اندازه‌گیری ممکن است لازم باشد. برای مثال، در زمانی که همان کلید به وسیله A برای هدف دیگری غیر از احراز هویت مورد استفاده قرار می‌گیرد. در هر صورت وارد کردن R_B در نشانه BA بنا به دلایل امنیتی که وارسی یکی بودن مقدار ارسال شده و مقدار اولیه را به A دیکته می‌کند، لازم می‌باشد؛ از آنجایی که R_B از ابتدا توسط A و تعیین R_A معلوم می‌باشد، چنین امنیتی برای B ممکن است در نظر گرفته نشود. اگر همچین حفاظتی مورد نیاز باشد، B می‌تواند یک عدد تصادفی اضافی R_B^t را در فیلدهای متنی Text4 و Text5 از نشانه BA اضافه کند.

ساز و کار احراز هویت سه مرحله‌ای به شرح است:

(۱) B یک عدد تصادفی R_B و به صورت اختیاری یک فیلد متن Text1 را به A می‌فرستد.

(۲) A نشانه AB و به صورت اختیاری گواهی آن‌را به B می‌فرستد.

(۳) B مراحل زیر را انجام می‌دهد:

(الف) مطمئن می‌شود که یک کلید عمومی معتبر از A دارد. این کار را با وارسی گواهی فرستاده شده از طرف A و یا راه‌های دیگر انجام می‌دهد.

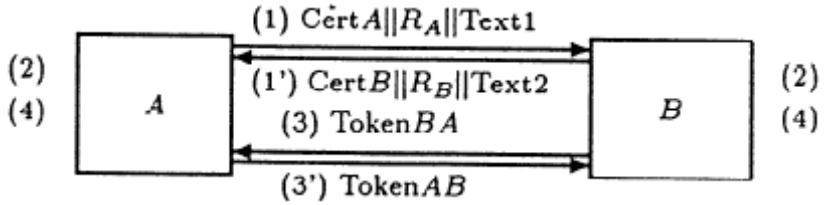
(ب) او نشانهAB را با وارسی امضای A که در نشانه قرار گرفته، با وارسی‌کردن اینکه عدد تصادفی R_B که در گام ۱ به A فرستاده شده بود، با عدد تصادفی موجود در داده امضا شده‌ی نشانهAB موافق است و یا با وارسی کردن اینکه شناساگر B که در داده امضا شده‌ی نشانه AB قرار گرفته (اگر فرستاده شده باشد) با شناساگر متمایز کننده B برابر است، تایید می‌کند.

(ت) B نشانه BA و به صورت اختیاری گواهی آن‌را به A می‌فرستد.

(ث) در جواب پیام شامل نشانه BA، A شبیه گام‌های الف و ب فهرست شده در مرحله ۳ عمل می‌کند. علاوه بر آن وارسی می‌کند تا مطمئن شود که عدد تصادفی R_B موجود در داده‌های امضا شده‌ی نشانه BA با عدد تصادفی R_B که در گام الف دریافت شده برابر است.

۵-۲-۳ احراز هویت موازی دو مرحله‌ای

در این سازوکار احراز هویت به صورت موازی انجام می‌شود. یکتایی و یا جدول زمانی به‌وسیله تولید و وارسی کردن اعداد تصادفی کنترل می‌شود. (به پیوست ب از استاندارد ملی شماره ۱-۹۷۹۸ : ۱۳۹۱ مراجعه شود.) سازوکار احراز هویت در شکل ۵ خلاصه شده است:



شکل ۵: احراز هویت موازی دو مرحله‌ای

فرم نشانه‌ها در این سازوکار، شبیه فرم مشخص شده در بند ۵-۱-۲ است.

$$\mathrm{Token}AB = R_A||R_B||B||Text4||sS_A(R_A||R_B||B||Text3)$$
$$TokenBA = R_B||R_A||A||Text6||sS_B(R_B||R_A||A||Text5)$$

وارد کردن پارامتر B در نشانه AB و همچنین A در نشانه BA اختیاری بوده و بستگی به محیطی دارد که این سازوکار در آن مورد استفاده قرار می گیرد.

یادآوری ۱- عدد تصادفی R_A به دلیل جلوگیری از کسب شدن امضا A توسط B، از طریق داده انتخابی از طرف B پیش از شروع سازوکار احراز هویت، در نشانه AB وجود دارد. این جلوگیری ممکن است لازم باشد؛ برای مثال، زمانی که همان کلید

توسط A برای اهداف دیگری جز احراز هویت هستار نیز مورد استفاده است. بنا به دلایلی مشابه عدد تصادفی R_B نیز در نشانه BA وجود دارد. وابسته به زمان نسبی رسید پیام‌های ارسال شده در گام‌های (۱) و (۱')، یکی از طرفین در زمان تعیین عدد تصادفی خود، مجاز به دانستن عدد تصادفی طرف دیگر است. در صوزتیکه این عمل مطلوب نباشد، هر دو طرف می‌توانند به ترتیب اعداد تصادفی اضافی R'_A و R'_B را در فیلدهای متنی Text3 و Text4 از نشانه AB و Text5 و Text6 از نشانه BA اضافه کنند.

ساز و کار احراز هویت موازی دو مرحله‌ای به شرح است:

(۱) A ، R_A و به صورت اختیاری گواهی آن و یک فیلد متنی Text1 را به B می‌فرستد.

(۱') B، R_B و به صورت اختیاری گواهی آن و فیلد متنی Text2 را به A می‌فرستد.

(۲) A و B مطمئن می‌شوند که یک کلید عمومی از هستار دیگر در اختیار دارند. این کار را یا از طریق وارسی گواهی‌های مرتبط یا با راه‌هایی دیگر انجام می‌دهند.

(۳) A، نشانه AB را به B می‌فرستد.

(۳') B، نشانه BA را به A می‌فرستد.

(۴) A و B گام‌های زیر را انجام می‌دهند.

هر کدام از آنها با وارسی‌کردن امضا موجود در نشانه و با وارسی‌کردن اینکه عدد تصادفی که قبلاً به هستار دیگر فرستاده شده بود با عدد تصادفی موجود در داده‌ی امضا شده از نشانه رسیده موافق است، نشانه دریافت شده را تصدیق می‌کند.

یادآوری ۲- یک جایگزین برای سازوکار ۵-۲-۳ اجرای سازوکار ۲-۱-۵ در هر دو حالت است. وجود گواهی‌ها در پیام‌های اول سازوکار ۵-۲-۳ اجازه می‌دهد تا وارسی گواهی زودتر انجام شود که این کار ممکن است سبب افزایش سرعت عملیات احراز هویت شود.

۶ سازوکارهایی که با یک طرف سوم مورد اطمینان برخط سروکار دارند.

۶-۱ مقدمه

سازوکارهای احراز هویت در این بند به دو هستار A و B برای تائید اعتبار کلیدهای عمومی یکدیگر با استفاده از طرف سوم مورد اطمینان برخط، نیاز دارند. (با شناساگر اختصاصی TP) این طرف سوم مورد اطمینان باید رونوشت‌هایی قابل اطمینان از کلیدهای عمومی A و B را در اختیار داشته باشد. هستارهای A و B باید رونوشت قابل اطمینانی از کلید عمومی TP را در اختیار داشته باشند.

این بخش، دو سازوکار پنج مرحله‌ای احراز هویت را مشخص می‌کند که هر دو به اصالت متقابل بین هستارهای A و B دست می‌یابند.

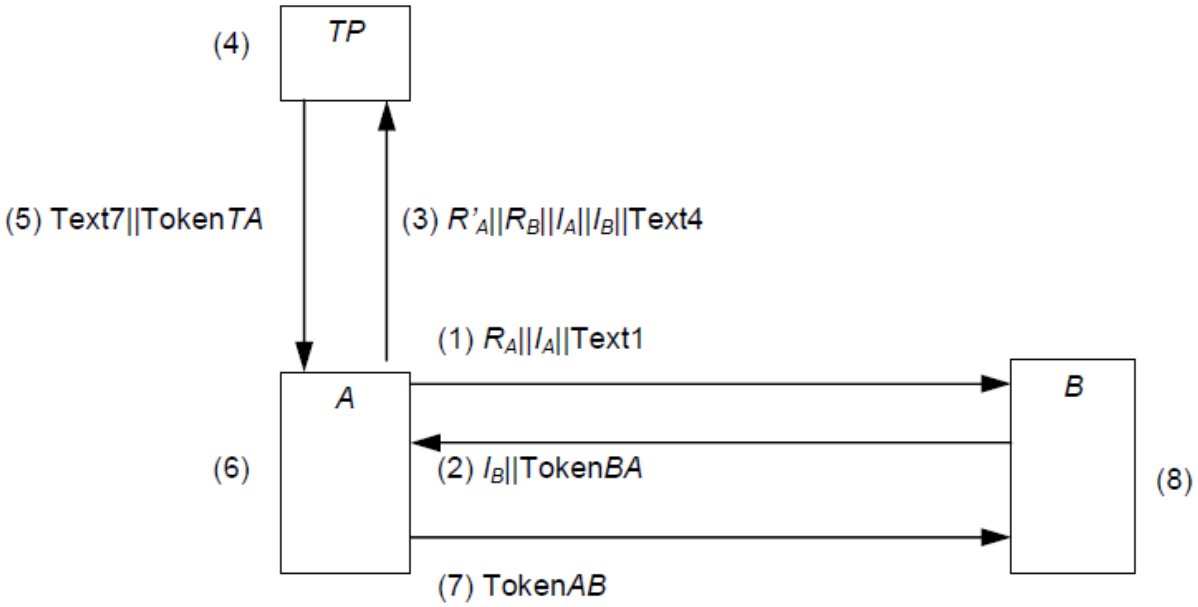
در مشخصات دو سازوکار، قالب نشانه‌ها و فیلدهای متنی از توضیحات ارائه شده در ابتدای بند ۵ پیروی می‌کنند. به عنوان مثال تمامی پاراگراف‌های بند ۵، قبل از ۵-۱.

پیاده‌سازی سازوکارها باید از یکی از روش‌های امضا مشخص شده در استانداردهای ISO/IEC 14888 و یا ISO/IEC 9796 استفاده کنند.

۶-۲ احراز هویت پنج مرحله‌ای (شروع شده توسط A)

در این سازوکار احراز هویت، یکتایی یا جدول زمانی، با ایجاد و وارسی یک عدد تصادفی کنترل می‌شود. (به پیوست ب در استاندارد ملی شماره ۱-۹۷۹۸ : ۱۳۹۱ مراجعه شود.)

این سازوکار احراز هویت در شکل ۶ به تصویر کشیده شده است.



شکل ۶: احراز هویت پنج مرحله‌ای(شروع شده توسط A)

نشانه باید مطابق با یکی از دو گزینه‌ی زیر ایجاد شود.

گزینه ۱:

$TokenAB= Text9||ResA||sS_T(R_B||ResA||Text5)||sS_A(R_B||R_A||B||A||Text8)$

$TokenBA= R_A||R_B||Text3||sS_B(B||R_A||R_B||A||Text2)$

$TokenTA= ResA||ResB||sS_T(R'_A||ResB||Text6)||sS_T(R_B||ResA||Text5)$

گزینه ۲:

$TokenAB= TokenR'_A||Text9||TA||sS_A(R_B||R_A||B||A||Text8)$

$TokenBA= R_A||R_B||Text3||sS_B(B||R_A||R_B||A||Text2)$

$TokenTA= ResA||ResB||sS_T(R'_A||R_B||ResA||ResB||Text5)$

ارزش‌های فیلدهای I_A ، I_B، ResA، ResB، Status و Failure باید قالب‌های زیر را داشته باشند:

I_A=A یا CertA

I_B=B یا CertB

ResA=(CertA||Status), (A||P_A) یا Failure

ResB=(CertB||Status), (B||P_B) یا Failure

Status= درست یا غلط. اگر لغو شدن گواهینامه معلوم باشد، ارزش این فیلد باید غلط باشد؛ درغیر این‌صورت باید درست نشانده شود.

Failure: ارزش ResX (دراینجا X={A,B})، درصورتیکه کلید عمومی و یا گواهینامه هستار X توسط TP پیدا نشود، Failure خواهد بود.

در این سازوکار، اگر TP نگاشت میان هویت X و P_x (دراینجا X={A,B}) را بداند، بنابراین باید I_X را برابر X قراردهد؛ درغیر این‌صورت باید I_x=CertX قرار دهد و X باید برابر با مقدار هویت فیلدهای موجود در CertX قرار داده شود. درصورتیکه X یا CertX مجاز به استفاده شدن به عنوان هویت در نظر گرفته شوند، آنگاه بهتر است تا برای اجازه دادن به TP برای تشخیص دو نوع نشانه‌های هویت، یک واسط از پیش سازماندهی شده وجود داشته باشد. ارزش ResX (در اینجا X={A,B}) باید با توجه به جدول ۱ تعیین شود.

جدول۱- ارزش ResX

فیلد	انتخاب ۱	انتخاب۲
Ix	X	CertX
ResX	Failure یا (X||Px)	Failure یا (CertX||Status)

سازوکار مطابق روند زیر اجرا می‌شود:

۱- A یک عدد تصادفی R_A، هویت آن I_A و بصورت اختیاری یک فیلد متنی Text1 را به B ارسال می‌کند.

۲- B نشانه BA و I_B را به A ارسال می‌کند.

۳- A یک عدد تصادفی R'_A را به‌همراه R_B، I_A، I_B و به‌صورت اختیاری یک فیلد متنی Text4 را به TP ارسال می‌کند.

۴- در دریافت پیـام گام (۳) از A، TP گام‌های زیر را اجـرا می‌کند. اگـر I_A=A و I_B=B باشد آنگاه TP، P_A و P_B را اصلاح می‌کند؛ اگر I_A=CertA و I_B=CertB باشد، TP درست بودن CertA و CertB را وارسی می‌کند. روند تائید گواهینامه توسط TP مجاز به داشتن حفاظت در مقابل بندآوری خدمات است. ویژگی‌های سازوکارهایی که برای ایجاد چنین امنیتی مورد استفاده قرار می‌گیرند از دامنه بررسی این استاندارد خارج است.

۵- سپس TP، نشانه TA و به‌صورت اختیاری یک فیلد متنی Text7 را به A ارسال می‌کند. فیلدهای ResA و ResB در نشانه TA باید گواهینامه‌های A و B و همچنین وضعیت آن‌ها، هویت‌های اختصاصی A و B و کلیدهای عمومی آن‌ها، یا یک نشانه از Failure باشند.

۶- در دریافت پیام گام (۵) از TP، A گام‌های زیر را اجرا می‌کند:

(الف) تائید نشانه TA با استفاده از وارسی امضا TP که در نشانه وجود دارد و همچنین با وارسی عدد تصادفی R'_A که در گام (۳) به TP ارسال شده و تطبیق آن با عدد تصادفی R'_A که در اطلاعات امضا شده‌ی نشانه TA نگه‌داری می‌شود، تائید انجام می‌شود.

(ب) بازیابی کلید عمومی B از روی پیام، تائید نشانه BA با وارسی امضا B که در نشانه‌ای که در گام (۲) دریافت شد وجود دارد و همچنین وارسی کردن برابر بودن ارزش فیلد شناساگر (A) در اطلاعات امضا شده از نشانه BA با شناساگر اختصاصی A و در پایان وارسی یکسان بودن عدد تصادفی R_A که در گام (۱) به B ارسال شده است با عدد تصادفی R_A موجود در نشانه BA انجام می‌شود.

(ت) A نشانه AB را به B ارسال می‌کند.

(ث) B در دریافت پیام گام (۷) از A، گام‌های زیر را انجام می‌دهد:

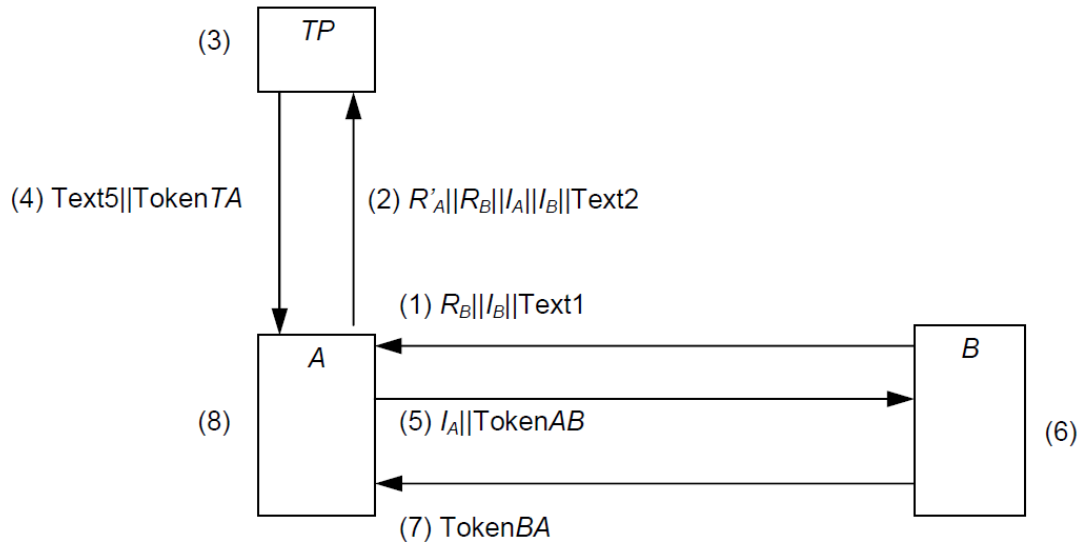
۱- تائید نشانه TA با استفاده از وارسی امضا TP که در نشانه وجود دارد و همچنین با وارسی عدد تصادفی R_B که در گام (۲) به A ارسال شده و تطبیق آن با عدد تصادفی R_B که در اطلاعات امضا شده‌ی نشانه TA نگه‌داری می‌شود، تائید انجام می‌شود.

۲- بازیابی کلید عمومی A از روی پیام، تائید نشانه AB با وارسی امضا A که در نشانه وجود دارد و همچنین وارسی کردن برابر بودن ارزش فیلد شناساگر (B) در اطلاعات امضا شده از نشانه AB با شناساگر اختصاصی B و در پایان وارسی یکسان بودن عدد تصادفی R_B که در گام (۲) به B ارسال شده است با عدد تصادفی R_B موجود در نشانه AB انجام می‌شود.

۳-۶ احراز هویت پنج مرحله‌ای (شروع شده توسط B)

در این سازوکار احراز هویت، یکتایی یا جدول زمانی، با ایجاد و وارسی یک عدد تصادفی کنترل می‌شود. (به پیوست ب در استاندارد ملی شماره ۱-۹۷۹۸ : ۱۳۹۱ مراجعه کنید.)

این سازوکار احراز هویت در شکل ۷ به تصویر کشیده شده است.



شکل ۷ – احراز هویت پنج مرحله‌ای(شروع شده توسط B)

نشانه باید مطابق با یکی از دو گزینه‌ی زیر ایجاد شود.

گزینه ۱:

Token*AB* = Text7||*RA*||Res*A*||*sST*(*RB*||Res*A*||Text3)||*sSA*(*RB*||*RA*||*B*||*A*||Text6)

Token*BA* = *RA*||*RB*||Text9||*sSB*(*A*||*RA*||*RB*||*B*||Text8)

Token*TA* = Res*A*||Res*B*||*sST*(*R'A*||Res*B*||Text4)||*sST*(*RB*||Res*A*||Text3)

گزینه ۲:

Token*AB* = *R'A* ||Text7||Token*TA*||*sSA*(*RB*||*RA*||*B*||*A*||Text6)

Token*BA* = *RA*||*RB*||Text9||*sSB*(*RA*||*RB*||*A*||*B*||Text8)

Token*TA* = Res*A*||Res*B*||*sST*(*R'A*||*RB*||Res*A*||Res*B*||Text3)

ارزش فیلدهای I_A ، I_B، ResA، ResB، Status و Failure باید قالب‌های زیر را داشته باشند:

I_A=A یا CertA

I_B=B یا CertB

ResA=(CertA||Status) ،(A||P_A) یا Failure

ResB=(CertB||Status) ،(B||P_B) یا Failure

Status= درست یا غلط. اگر لغو شدن گواهینامه معلوم باشد، ارزش این فیلد باید غلط باشد؛ درغیر این‌صورت باید درست نشانده شود.

Failure: ارزش ResY (دراینجا Y={A,B})، درصورتیکه هیچ‌کدام از کلید عمومی و یا گواهینامه هستار Y توسط TP پیدا نشود، Failure خواهد بود.

در این سازوکار، اگر TP نگاشت میان هویت Y و P_Y (دراینجا Y={A,B}) را بداند، بنابراین باید I_Y را برابر Y قراردهد؛ درغیر این‌صورت باید I_Y=CertY قرار دهد و Y باید برابر با مقدارهویت فیلدهای موجود در CertY قرار داده شود. درصورتیکه Y و یا CertY مجاز به استفاده شدن به عنوان هویت درنظر گرفته شوند، آنگاه بهتر است تا برای اجازه دادن به TP برای تشخیص دو نوع نشانه‌های هویت، یک واسط از پیش سازماندهی شده وجود داشته باشد. ارزش ResY (در اینجا Y={A,B}) باید با توجه به جدول ۲ تعیین شود.

جدول۲- ارزش ResY

فیلد	انتخاب ۱	انتخاب۲
IY	Y	CertY
ResY	Failure یا (Y||PY)	Failure یا (CertY||Status)

سازوکار مطابق روند زیر اجرا می‌شود:

۱- B یک عدد تصادفی R_B، هویت آن I_B و به‌صورت اختیاری یک فیلد متنی Text1 را به A ارسال می‌کند.

۲- A یک عدد تصادفی R'_A را به‌همراه R_B، I_A، I_B و به‌صورت اختیاری یک فیلد متنی Text2 را به TP ارسال می‌کند.

۳- TP در دریافت پیام گام (۲) از A، گام‌های زیر را اجرا می‌کند. اگر I_A=A و I_B=B باشد آنگاه TP، P_A و P_B را اصلاح می‌کند؛ اگر I_A=CertA و I_B=CertB باشد، TP درست بودن CertA و CertB را وارسی می‌کند. روند تائید گواهینامه توسط TP مجاز به داشتن حفاظت در مقابل بندآوری خدمات است. ویژگی‌های سازوکارهایی که برایی ایجاد چنین امنیتی مورد استفاده قرار می‌گیرند از دامنه وارسی این استاندارد خارج است.

۴- سپس TP، نشانهTA و به‌صورت اختیاری یک فیلد متنی Text5 را به A ارسال می‌کند. فیلدهای ResA و ResB در نشانهTA باید گواهینامه‌های A و B و همچنین وضعیت آن‌ها، هویت‌های اختصاصی A و B و کلیدهای عمومی آن‌ها، یا یک نشانه از Failure باشند.

۵- نشانه A، نشانه AB و I_A را به B ارسال می‌کند.

۶- B در دریافت پیام گام (۵) از A، گام‌های زیر را اجرا می‌کند:

(الف) تائید امضا TP در نشانه AB با وارسی امضا TP که در نشانه وجود دارد و همچنین با وارسی عدد تصادفی R_B که در گام (۱) به A ارسال شده و تطبیق آن با عدد تصادفی R_B که در اطلاعات امضا شده‌ی TP که در نشانهAB نگه‌داری می‌شود، تائید انجام می‌شود.

(ب)بازیابی کلید عمومی A از روی پیام، تائید نشانه AB با وارسی امضا A که درنشانه وجود دارد و همچنین وارسی کردن برابر بودن ارزش فیلد شناساگر (B) در اطلاعات امضا شده از نشانه AB با شناساگر اختصاصی B و در پایان وارسی یکسان بودن عدد تصادفی R_B که در گام (۱) به A ارسال شده است با عدد تصادفی R_B موجود در نشانه AB انجام می‌شود.

(ت)B نشانه BA را به A ارسال می‌کند.

(ث)A در دریافت پیام گام (۷) از B، گام‌های زیر را انجام می‌دهد:

۱- تائید نشانه TA با استفاده از وارسی امضا TP که در نشانه وجود دارد و همچنین با وارسی عدد تصادفی R'_A که در گام (۲) به TP ارسال شده و تطبیق آن با عدد تصادفی R'_A که در اطلاعات امضا شده‌ی نشانهTA نگه‌داری می‌شود، تائید انجام می‌شود.

۲- بازیابی کلید عمومی B از روی پیام، تائید نشانه BA با وارسی امضا B که در نشانه وجود دارد و همچنین وارسی کردن برابر بودن ارزش فیلد شناساگر (A) در اطلاعات امضا شده از نشانه BA با شناساگر اختصاصی A و در پایان وارسی یکسان بودن عدد تصادفی R_A موجود در نشانه BA با عدد تصادفی R_A که در گام (۵) به B ارسال شده است انجام می‌شود.

پیوست الف

(اطلاعاتی)

استفاده از فیلدهای متنی

نشانه‌های مشخص شده در بخش ۵ و بخش ۶ شامل فیلدهای متنی است. استفاده‌ی واقعی و همچنین رابطه بین فیلدهای متنی مختلف در یک مرحله بستگی به کاربردی دارد که در آن مورد استفاده قرار می‌گیرند. چند مثال در زیر آمده است. برای اطلاعات بیشتر به پیوست الف از استاندارد ملی شماره ۱-۹۷۹۸ : ۱۳۹۱را نیز مراجعه شود. اگر یک طرح‌واره امضا بدون بازیافت پیام استفاده شود و اگر فیلد متن امضا شده خالی نباشد، آنگاه تایید کننده نیاز دارد تا متن را از قبل برای تایید امضا داشته باشد. در این پیوست، «فیلد متنی امضا شده» اشاره به فیلدهای متنی در داده‌های امضا شده دارند و «فیلد متنی امضا نشده» به فیلدهای متنی با داده امضا نشده اشاره می‌کنند.

برای مثال اگر یک طرح‌واره امضای رقمی بدون بازیابی پیام استفاده شود، آنگاه هر اطلاعاتی که نیاز به احراز هویت دارد باید از فیلد متنی امضا شده و (به‌عنوان بخشی از) فیلد متنی امضا نشده از نشانه قرار گیرد. اگر نشانه (به اندازه کافی) افزونگی نداشته باشد، فیلدهای متنی امضا شده ممکن است برای فراهم کردن افزونگی بیشتر مورد استفاده قرار گیرند.

فیلدهای متنی امضا شده برای مشخص کردن معتبر بودن نشانه، فقط به هدف احراز هویت هستار، مجاز است تا مورد استفاده قرار گیرد. بهتر است این نگرانی وجود داشته باشد که ممکن است یک هستار مقداری هم‌تراز را با نیت سو و به قصد به‌دست آوردن امضا هستار دیگر اختیار کند و لذا هستار دیگر مجاز به اختیار یک عدد تصادفی در فیلد متنی می‌باشد.

در شرایطی که این امکان وجود داشته باشد که راه‌اندازی حمله‌ها بر پایه‌ی این حقیقت که یک خواهان مشخصی با استفاده از کلید یکسانی که خواهان برای ارتباط از آن استفاده می‌کند، برای تمامی تاییدکننده‌ها استفاده کند، بهتر است که یک الگوریتم مورد استفاده قرار گیرد. همچنین اگر چنین حمله‌های به‌صورت یک تهدید تلقی شود، توصیه می‌شود که شناساگر تاییدکننده موردنظر در فیلد متنی امضا شده و در صورت لزوم در فیلد متنی امضا نشده قرار گیرد.

همچنین فیلدهای متنی امضا نشده می‌توانند برای یک تایید کننده، اطلاعات بیانگر (غیر احراز هویت شده) شناساگرای که خواهان بر آن ادعا می‌کند را فراهم کند. اگر ابزارهایی غیر از گواهی‌ها برای توزیع کلیدهای عمومی مورد استفاده قرار گیرد، این اطلاعات مجاز است تا برای احراز هویت یک خواهان، به تائیدکننده اجازه دهد تا از میان کلیدهای عمومی مقدار لازم را تعیین کند.

پیوست ب

(الزامی)

شناسانه شی و دستورهای ASN.1

ب-۱ تعریف رسمی

```
EntityAuthenticationMechanisms-3 {
iso(1) standard(0) e-auth-mechanisms(9798) part3(3)
asn1-module(0) object-identifiers(0) }
DEFINITIONS EXPLICIT TAGS ::= BEGIN
-- EXPORTS All; --
-- IMPORTS None; --
OID ::= OBJECT IDENTIFIER -- alias
-- Synonyms --
is9798-3 OID ::= { iso(1) standard(0) e-auth-mechanisms(9798) part3(3)
}
mechanism OID ::= { is9798-3 mechanisms(1) }
-- mechanisms not involving a trusted third party --
ua-one-pass OID ::= { mechanism 1 }
ua-two-pass OID ::= { mechanism 2 }
ma-two-pass OID ::= { mechanism 3 }
ma-three-pass OID ::= { mechanism 4 }
ma-two-pass-Parallel OID ::= { mechanism 5 }
-- mechanisms involving a trusted third party --
ttp-ma-five-pass-by-A OID ::= { mechanism 6 }
ttp-ma-five-pass-by-B OID ::= { mechanism 7 }
END -- EntityAuthenticationMechanisms-3 –
```

ب-۲ استفاده از شناسانه‌های شی پی در پی

بلافاصله بعد از اینکه یک شناسانه شی، سازوکار را شناسایی کرد، یک شناسانه شی دیگر که الگوریتم امضا رقمی را شناسایی می‌کند باید روند را دنبال کند. (یعنی، یکی از الگوریتم‌هایی که در استانداردهای ISO/IEC 14888 یا ISO/IEC9796 آمده است.)

ب-۳ مثال‌های کدگزاری در مطابقت با کدبندی پایه

در مطابقت با استاندارد ISO/IEC 8825-1، یک شناسانه شی شامل یک یا چند سری از هشت تایی‌ها است. هر سری، یک عدد را کدگذاری می‌کند.

- بیت ۸ (مهمترین بیت)، در هشت تایی آخر سری مقدار صفر نشانده می‌شود و درصورتیکه سری بیش از یک هشت تایی داشته باشد، در هشت تایی‌های قبلی مقدار آن یک خواهد بود.
- سلسله‌بندی بیت‌های ۷ تا ۱ در هشت تایی‌های یک سری، یک عدد را کدگذاری می‌کنند. هر عدد باید با کمترین تعداد هشت تایی ممکن کدگذاری شود؛ یعنی در اولین جایگاه یک سری، هشت تایی ’80‘ بی‌اعتبار است.

- اولین عدد، عدد استاندارد است؛ عدد دوم، درصورت وجود، بخشی از یک استاندارد چند بخشی است.

یک شناسانه شی می‌تواند به هر یک از سازوکارهای تعریف شده در این استاندارد مراجعه کند.

- برای شناسایی یک استاندارد ISO، هشت تایی اول مقدار ’28‘(در مبنای شانزده) قرار می‌گیرد که عدد ۴۰ در مبنای ده است. (به استاندارد ISO/IEC 8825-1 مراجعه کنید.)
- دو هشت تایی بعدی برابر با ’CC46‘ قرار می‌گیرند. ۹۷۹۸ در مبنای شانزده برابر ’2646‘ است یعنی 0110 0100 0110 0010 که به معنی دو بخش هفت بیتی: 1001100 و 1000110 است. بعد از جای‌دهی مقدار مناسب بیت هشتم در هر هشت تایی، کدگذاری مناسب سری 11001100 01000110 است که همان ’CC46‘ است.
- هشت تایی بعدی برای شناسایی بخش ۳، برابر با ’03‘ مقداردهی می‌شود.
- هشت تایی بعدی یک سازوکار احراز هویت را مشخص می‌کند.

- ’01‘، سازوکار احراز هویت یک مرحله‌ای و یک‌طرفه را که یک طرف سوم برخط مورد اطمینان را شامل نمی‌شود، مشخص می‌کند.
- ’02‘، سازوکار احراز هویت دو مرحله‌ای و یک‌طرفه را که یک طرف سوم برخط مورد اطمینان را شامل نمی‌شود، مشخص می‌کند.
- ’03‘، سازوکار احراز هویت دو مرحله‌ای و دوطرفه را که یک طرف سوم برخط مورد اطمینان را شامل نمی‌شود، مشخص می‌کند.
- ’04‘، سازوکار احراز هویت سه مرحله‌ای و دوطرفه را که یک طرف سوم برخط مورد اطمینان را شامل نمی‌شود، مشخص می‌کند.
- ’05‘، سازوکار احراز هویت موازی دو مرحله‌ای و دوطرفه را که یک طرف سوم برخط مورد اطمینان را شامل نمی‌شود، مشخص می‌کند.
- ’06‘، سازوکار احراز هویت پنج مرحله‌ای، دوطرفه و شروع شده توسط A را که یک طرف سوم برخط مورد اطمینان را شامل می‌شود، مشخص می‌کند.
- ’07‘، سازوکار احراز هویت پنج مرحله‌ای، دوطرفه و شروع شده توسط B را که یک طرف سوم برخط مورد اطمینان را شامل می‌شود، مشخص می‌کند.

مثال : عنصر اطلاعات ’28 CC 46 03 04‘ {iso standard 9798 3 4} یعنی سازوکار چهارم در این استاندارد، سازوکار احراز هویت سه مرحله‌ای و دوطرفه را که یک طرف سوم برخط مورد اطمینان را شامل نمی‌شود را باز می‌خواند. عنصر اطلاعاتی فوق مجاز است که از طریق اطلاعات شی‌ای BER-TLV ذکر شده در زیر منتقل شود (به قوانین پایه‌ای کدبندی در ASN.1، ISO/IEC 8825-1، برچسب طبقه عمومی ’06‘ مراجعه کنید.) که در آن خط‌های تیره و کروشه‌ها برای فهم بهتر اضافه شده‌اند و اهمیت ندارند.

داده شی = {’28 CC 46 03 04‘-’05‘-’06‘}

کتاب‌نامه

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

[2] ISO/IEC 9796 (all parts), Information technology — Security techniques — Digital signature scheme giving message recovery

[3] ISO/IEC 14888 (all parts), Information technology — Security techniques — Digital signatures with appendix