INSO
10825-2
1st. Edition
Jan.2013

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

استاندارد ملی ایران
۱۰۸۲۵-۲
چاپ اول
دی ۱۳۹۱

فناوری اطلاعات – فنون امنیتی- احراز هویت هستار قسمت ۲: سازوکارهای استفاده‌کننده از الگوریتم-های پوشیده سازی متقارن

Information technology - Security Techniques — Entity authentication part2: Mechanisms using symmetric encipherment algorithms

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 ۲: سازوکارهای استفاده‌کننده‌ی الگوریتم‌های پوشیده سازی متقارن »

	سمت و/ یا نمایندگی
رئیس:	
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 (فوق لیسانس فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
عباسپور، مقصور (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

پیش‌گفتار

استاندارد «فناوری اطلاعات- فنون امنیتی- احراز هویت هستار - قسمت ۲: سازوکارهای استفاده‌کننده‌ی الگوریتم‌های پوشیده سازی متقارن » که پیش نویس آن درکمیسیون‌های مربوطه توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده و دردویست و یکمین اجلاس کمیتهٔ ملی استاندارد رایانه و فرآوری داده مورخ ۹۱/۸/۹ 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 می-شود.

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

ISO/IEC 9798-2: 2008, Information technology — Security techniques — Entity authentication — Part 2: Mechanisms using symmetric encipherment algorithms +Technical Corrigendum 1:2010+ Technical Corrigendum 2:2012

فناوری اطلاعات – فنون امنیتی- احراز هویت هستار
قسمت ۲: سازوکارهای استفاده‌کننده‌ی الگوریتم‌های پوشیده سازی متقارن

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، بیان سازوکارهای احراز هویت هستاری است که از الگوریتم‌های پوشیده سازی متقارن استفاده می‌کند. چهار مورد از سازوکارها، احراز هویت هستار را بین دو هستار بدون دخالت طرف سوم مورد اعتماد[۱] فراهم می‌سازند؛ دو مورد از این سازوکارها برای احراز هویت یک جانبه[۲] یک هستار به دیگری است در حالی که دو سازوکار دیگر برای احراز هویت دو جانبه[۳] دو هستار مورد استفاده قرار می‌گیرند. سازوکار-های باقیمانده به طرف سوم مورد اعتمادی برای ایجاد یک کلید سری[۴] مشترک و تشخیص یک یا دو جانبه بودن احراز هویت، نیاز دارند.

سازوکارهای مشخص شده در این قسمت از این مجموعه استاندارد ملی از پارامترهای متغیر با زمان، مانند مهرهای زمانی[۵]، اعداد دنباله‌ای یا عددهای تصادفی، برای جلوگیری از پذیرفته‌شدن اطلاعات احراز هویت معتبر در بعدی یا دیگر دفعات استفاده می‌کنند.

اگر هیچ طرف سوم مورد اعتمادی درگیر نباشد و از یک مهر زمانی یا عدد دنباله استفاده شود، برای احراز هویت یک جانبه به یک گذر نیاز است. اگر هیچ طرف سوم مورد اعتمادی درگیر نباشد و یک چالش یا روش پاسخ شامل عددهای تصادفی استفاده شود، برای احراز هویت یک جانبه به دو گذر نیاز است، در حالی که برای دستیابی به احراز هویت دو جانبه نیاز به سه گذر وجود دارد. اگر طرف سوم مورد اعتمادی درگیر باشد، هرگونه ارتباط اضافی بین هستار و طرف سوم مورد اعتماد نیازمند دو گذر اضافه در مبادله‌ی ارتباطی خواهد بود.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی به آن‌ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی محسوب می شود.

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

---

1 -Trusted third party
2 - Unilaterally
3 - Mutual
4 - Secret Key
5 - Time stamps

استفاده از مراجع زیر برای این استاندارد الزامی است :

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

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به کار می‌رود:

۱-۳

رمزبندی احراز هویت شده[۱]

تبدیل (برگشت‌پذیر) داده با یک الگوریتم رمزنگاشتی[۲] برای تولید متن رمزی[۳] که هستار غیرمجاز بدون آنکه تشخیص داده شود قادر به تغییر آن نخواهد بود، به عبارت دیگر این رمزنگاری محرمانگی[۴] داده، یکپارچگی[۵] داده و احراز هویت منشأ داده را فراهم می‌سازد.

[ISO/IEC 19772:-1]

۲-۳

متن رمز

داده‌ای که با هدف مخفی نمودن، محتویات اطلاعاتی آن تبدیل[۶] شده است.

[مطابق استاندارد ملی ایران شماره ۹۶۰۰: سال ۱۳۸۶]

۳-۳

خواهان[۷]

هستاری که هویت آن قابل احراز هویت بوده وشامل توابع و داده‌ی خصوصی لازم برای ارائه در مبادلات احراز هویت به نیابت از طرف اصلی[۸] است.

[ISO/IEC 9798-5:2004]

۴-۳

کد احراز هویت پیام (MAC)[۹]

رشته‌ای از بیت‌ها که خروجی یک الگوریتم MAC است.

1- Authenticated encryption
2 -Cryptographic
3- Ciphertext
4- Confidentiality
5- integrity
6- Transformation
7 -Claimant
8- On behalf of a principal
9- Message authentication code (MAC)

یادآوری- از MAC گاهی با عنوان مقدار وارسی رمزنگاشتی یاد می‌شود.

[ISO/IEC 9797-1:1999]

۵-۳

الگوریتم کد احراز هویت پیام[1]

الگوریتمی برای محاسبه‌ی یک تابع که رشته‌هایی از بیت‌ها و یک کلید سرّی را به رشته‌هایی از بیت‌ها با طول ثابت نگاشت کرده و دارای دو خصوصیت زیر است:

- برای هر کلید و هر رشته‌ی ورودی، تابع به صورت کارآمد می‌تواند محاسبه شود.
- برای هر کلید ثابت و بدون هیچ آگاهی قبلی از کلید، محاسبه‌ی مقدار تابع برای یک رشته ورودی جدید حتی با آگاهی از یک مجموعه رشته‌های ورودی و مقادیر متناظر تابع که مقدار iامین رشته‌ی ورودی ممکن است بعد از مشاهده‌ی مقدار اولین i-1 مقدار تابع انتخاب شده باشد، به‌طور محاسباتی غیر عملی است.

یادآوری۱- از الگوریتم MAC گاهی با عنوان تابع وارسی رمزنگاشتی یاد می‌شود (به مثال‌های ISO 7498-2 مراجعه شود).

یادآوری۲- عملی بودن به طور محاسباتی به محیط و الزامات امنیتی خاص کاربر بستگی دارد.

[ISO/IEC 9797-1:1999]

۶-۳

مهر زمانی

پارامتر متغیر با زمان که نشان دهنده‌ی نقطه‌ای در زمان، با توجه به زمان مرجع مشترک است.

[استاندارد ملی ایران شماره ۱۳۸۷:۱۱۳۱۰-۱]

۷-۳

طرف سوم قابل اعتماد (TPP)[2]

یک مرجع امنیتی یا عامل[3] آن، که توسط دیگر هستارها با توجه به فعالیت‌های مرتبط با امنیت مورد اعتماد قرارگرفته باشد.

[استاندارد ملی ایران شماره ۱۳۸۷:۱۱۳۱۰-۱]

۴ نمادها و نشانه گذاری

A , B	برچسب‌هایی برای هستارهای شرکت‌کننده در سازوکار
d_k	فرایند ناپوشیده سازی احراز هویت شده با استفاده از کلید سرّی K
e_k	فرایند پوشیده سازی احراز هویت شده با استفاده از کلید سرّی K

1- Message authentication code (MAC) algorithm
2- Trusted Third Party
3- Agent

$e_k(X)$	نتیجه‌ی فرایند ساخت رمز برای داده X با الگوریتم پوشیده سازی متقارن با استفاده از کلید K
I_U	شناسه‌ی تشخیص‌دهنده‌ی هستار U
K	کلید سرّی مورد استفاده در فرایندهای پوشیده سازی و واپوشیده‌سازی
K_{UV}	کلید سرّی مشترک بین هستار U و V، تنها برای استفاده در فنون پوشیده سازی متقارن
N_U	عدد دنباله‌ی صادره توسط هستار U
P	نمادی برای نمایش طرف سوم مورد اعتماد
R_U	عدد تصادفی صادره توسط هستار U
TN_U	پارامتر متغیر با زمان، که منشا آن هستار U است که مهر زمانی T_U و یا عدد ترتیب N_U است
$Token_{UV}$	نشانه‌ی فرستاده شده توسط هستار U به V
T_U	مهر زمانی صادره توسط هستار U
TVP_U	پارامتر متغیر با زمان ساخته شده توسط هستار U که یا مهر زمانی T_U و یا عدد دنباله N_U یا عدد تصادفیR_U است.
$X\|\|Y$	نتیجه الحاق[1] فقره‌های داده ای X و Y طبق ترتیب مشخص است. در مواردی که نتیجه الحاق دو یا چند فقره داده‌ای به‌عنوان قسمتی از سازوکار مشخص شده در این قسمت از این مجموعه استاندارد ملی، رمزنگاری شده باشد، این نتیجه باید ترکیب شود تا بتواند به طور یکتا با قسمت اصلی رشته‌های داده خودش یکپارچه شود، به این معنی که امکان ابهام در تفسیر داده‌ها وجود نداشته باشد. این مشخصه با توجه به برنامه مورد استفاده به طرق گوناگونی قابل دسترسی است. به طور مثال، این مشخصه الف - با تنظیم طول هر کدام از زیر رشته‌ها در کل محدوده استفاده از سازوکار و یا ب - به وسیله کدبندی دنباله‌ای از رشته‌های اضافه شده با استفاده از روشی که رمزگشایی منحصر به فرد را تضمین می کند، قابل انجام است. به طور مثال استفاده از قواعد متمایز شده کدبندی در ISO/IEC 8825-1 [1].
یادآوری- برای این‌کار نه تنها رشته‌های الحاق شده بلکه چندتایی‌های مرتب شده نیاز است. به طور طبیعی نماد چندتایی مرتب شده به صورت $[X_1,X_2,...,X_n]$ است.	

۵ الزامات

در سازوکارهای احراز هویت مشخص شده در این قسمت از این مجموعه استاندارد ملی، یک هستار برای احراز هویت، شناسه‌ی خود را با اثبات آگاهی از کلید احراز هویت سرّی تقویت می‌نماید. این مهم توسط هستاری که از کلید سرّی‌اش برای پوشیده‌سازی یک داده مشخص استفاده می‌کند تحقق می‌یابد. هر کسی که اشتراک گذارنده‌ی کلید احراز هویت سرّی هستار باشد قادر است داده پوشیده‌شده را واپوشیده‌سازی نماید. داده‌ی واپوشیده‌سازی شده باید شامل یک پارامتر متغیر با زمان باشد. این پارامتر به یکی از طرق زیر قابل درستی‌سنجی می‌باشد:

۱- اگر آن عددی تصادفی باشد، آنگاه گیرنده باید اطمینان یابد که با چالش تصادفی فرستاده‌شده به خواهان یکی است. برای آگاهی از ایجاد و استفاده از اعداد تصادفی، به ISO/IEC 18031 مراجعه شود.

2- Concatenation

۲- اگر آن مهری زمانی باشد، آنگاه توصیه می‌شود که گیرنده اعتبار مهر زمانی را درستی‌سنجی کند.
۳- اگر آن عددی دنباله باشد، آنگاه گیرنده باید قادر به مقایسه‌ی آن با عدد با عددهای قبلی رسیده یا ذخیره شده باشد تا اطمینان یابد که این عدد بازپخش نیست.

سازوکارهای احراز هویت دارای الزامات زیر است. در صورت برآورده نشدن هر یک از این موارد، فرایند احراز هویت بی‌اعتبار و قابل پیاده‌سازی نمی‌باشد.

الف) خواهانی که خود را به یک درستی‌سنج شناسانده است باید یک کلید احراز هویت سرّی مشترک با آن درستی‌سنج، به اشتراک بگذارد، یعنی با به‌کارگیری سازوکارهای بند ۶، هر هستار باید یک کلید احراز هویت سرّی با یک طرف سوم مورد اعتماد را به اشتراک بگذارد، یا با به‌کارگیری سازوکارهای بند۷- چنین کلیدهایی باید قبل از شروع هر رخداد خاص در یک سازوکار احراز هویت، به طرف‌های درگیر شناسانده شوند. روش دستیابی به این مهم فراتر از دامنه‌ی این قسمت از این استاندارد ملی می‌باشد. راهنمایی‌های لازم راجع به مدیریت کلیدهای احراز هویت سرّی در ISO/IEC 11770-1 و ISO/IEC 11770-2 قرار دارد.

ب) در صورت وجود یک طرف سوم مورد اعتماد، خواهان و درستی سنج هر دو باید قابل اطمینان باشند.

پ) کلید احراز هویت سرّی مشترک بین یک خواهان و درستی‌سنج، یا یک هستار و یک طرف سوم مورد اعتماد، تنها لازم است به آن دو طرف شناسانده شود و احتمالا هستار دیگری که هر دو به آن اعتماد دارند که از کلید سوء استفاده نمی‌کند، مثلا ظاهرسازی به بودن یکی از طرفین نمی‌کند.

یادآوری- توصیه می‌شود الگوریتم پوشیده سازی و طول عمر کلید انتخاب شوند تا به طور محاسباتی، استنتاج یک کلید در طول مدت عمر آن غیر عملی باشد. به علاوه، انتخاب طول عمر کلید به منظور جلوگیری از حملات شناخته شده و انتخابی متن ساده، توصیه می‌شود.

ت) نشانه‌های مورد استفاده در سازوکارها باید، حتی با آگاهی از نشانه‌های قدیمی، غیرقابل جعل باشند. به عبارت دیگر، نشانه‌های قدیمی نباید به هیچ طریقی (بخشی یا به صورت کامل) مجدداً برای ساخت نشانه‌های جدید استفاده شوند. هر کلید سرّی ممکن K، تابع پوشیده سازی e_K و تابع واپوشیده‌ساز وابسته آن d_K، باید دارای ویژگی ذیل باشند. فرایند واپوشیده سازی d_K، وقتی به یک رشته‌ی $e_K(X)$ اعمال می‌شود، باید گیرنده‌ی رشته را قادر به شناسایی داده‌ی جعلی یا دستکاری شده نماید، به عبارت دیگر، تنها صاحب کلید سرّی K باید قادر به تولید رشته‌هایی باشد که وقتی تحت فرایند واپوشیده‌سازی d_K قرار می‌گیرند «پذیرفته» خواهند شد.

یادآوری- در عمل، این مهم به طرق گوناگونی قابل دستیابی است. رویکرد پیشنهادی استفاده از کلید سرّی K و یک فن رمزبندی تأیید شده است که هر دو محافظت یکپارچگی و محرمانگی را، همانگونه که در ISO/IEC 19772 استانداردسازی شده است، فراهم می‌آورد.

ث) سازوکارهای این قسمت از این مجموعه استاندارد ملی نیازمند استفاده از پارامترهای متغیربا زمان مانند

مهرهای زمانی، اعداد دنباله‌ای یا عددهای تصادفی هستند. ویژگی‌های این پارامترها برای امنیت این سازوکارها دارای اهمیت است، به خصوص که برای آن‌ها تکرار در طول عمر یک کلید احراز هویت سرّی بعید است. برای اطلاعات بیشتر به پیوست ب در استاندارد ملی ایران شماره ۱-۹۷۹۸: سال ۱۳۹۱مراجعه شود.

ج) کلید احراز هویت سرّی استفاده شده در پیاده‌سازی برای هر سازوکار مشخص شده در این قسمت از مجموعه استاندارد ملی باید از هر کلید استفاده شده برای هر یک از اهداف دیگر تشخیص داده شود.

د)رشته‌های داده پوشیده شده در نقاط مختلف در سازوکار احراز هویت نباید به‌طوری تلفیق شوند که قابل تبادل نباشند.

یادآوری- این امر با اضافه کردن عناصر زیر در هر رشته داده پوشانده‌شده اجرا می‌شود.

شیء شناسه‌گر مشخص شده در پیوست الف، به ویژه شناسایی استاندارد ISO، عدد قسمت و مکانیزم احراز هویت

۶ سازوکارهای بدون طرف سوم مورد اعتماد

در این سازوکارهای احراز هویت، هستارهای A و B باید قبل از شروع هر رخداد خاص در این سازوکارها، یک کلید احراز هویت سرّی مشترک K_{AB} یا دو کلید سرّی یک طرفه K_{AB} و K_{BA} به اشتراک بگذارند. در مورد آخر، کلیدهای سرّی یک طرفه K_{AB} و K_{BA} به ترتیب برای احراز هویت A توسط B و B به وسیله A استفاده می‌شوند.

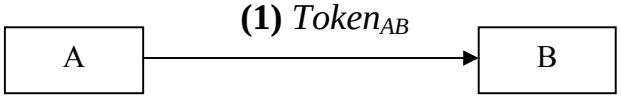
تمام فیلدهای متنی[1] بیان شده در سازوکارهای ذیل برای استفاده، در برنامه‌های کاربردی خارج از دامنه‌ی این قسمت از این مجموعه استاندارد ملی در دسترس هستند (ممکن است خالی باشند). ارتباط و محتوای آنها به آن برنامه‌ی کاربردی مشخص وابسته می‌باشد. برای اطلاع از کاربرد فیلدهای متنی به پیوست ب - مراجعه شود.

۶-۱ احراز هویت یک جانبه

احراز هویت یک جانبه به این معناست که تنها یکی از دو هستار با استفاده از سازوکار احراز هویت می‌شود.

۶-۱-۱ سازوکار ۱ – احراز هویت یک گذره

در این سازوکار احراز هویت، خواهان A فرایند را آغاز و توسط درستی‌سنج B، احراز هویت می‌شود. یکتایی/ جدول زمانی توسط تولید و وارسی یک مهر زمانی یا یک عدد دنباله، کنترل می‌شود (به پیوست ب) استاندارد ملی ایران شماره ۱-۹۷۹۸: سال ۱۳۹۱ از مراجعه شود). سازوکار احراز هویت در شکل ۱ نمایش داده شده است.



1 - Text-Field

شکل ۱- سازوکار ۱- احراز هویت یک گذره

قالب نشانه‌ی ($Token_{AB}$)، فرستاده شده از خواهان A به درستی‌سنج B :

$$Token_{AB} = Text_2 \,||\, e_{K_{AB}}(TN_A \,||\, I_B \,||\, Text_1)$$

که در آن خواهان A از پارامتر متغیر با زمان TN_A که مهر زمانی T_A یا عدد دنباله N_Aاست استفاده می‌کند. گنجاندن شناسه تشخیص‌دهنده‌ی I_B در $Token_{AB}$ اختیاری است.

یادآوری- شناسه تشخیص‌دهنده‌ی I_B در $Token_{AB}$ گنجانده شده است تا از استفاده مجدد $Token_{AB}$ در هستار A با رقیبی که تظاهر می‌کند هستار B است جلوگیری نماید. این گنجاندن اختیاری است تا در صورت لزوم، در محیط‌هایی که چنین حملاتی نمی‌تواند رخ دهد، حذف شود. اگر یک کلید یک طرفه استفاده شود نیز شناسه تشخیص‌دهنده I_B قابل حذف خواهد بود.

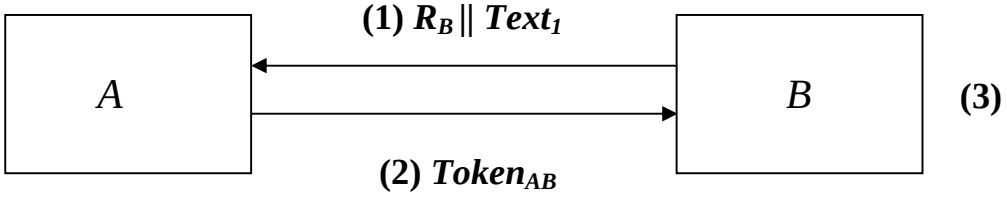
شرح سازوکار ۱- احراز هویت یک گذره، در ادامه آمده است:

(۱) A، $Token_{AB}$ را تولید و به B می‌فرستد.

(۲) B با دریافت پیام شامل $Token_{AB}$، و با ناپوشیده سازی قسمت پوشیده سازی شده [در اینجا رمزگشایی مستلزم آن است که الزاماتی که در بند ۵ ت - آمده است برآورده شوند] و سپس وارسی صحت شناسه تشخیص‌دهنده‌ی I_B، در صورت وجود، به علاوه‌ی مهر زمانی و عدد دنباله، $Token_{AB}$ را درستی‌سنجی می‌کند.

۶-۱-۲ سازوکار ۲ – احراز هویت دو گذره

در این سازوکار احراز هویت، خواهان A توسط درستی‌سنج B که آغازکننده‌ی فرایند است احراز هویت می‌شود. یکتایی/ جدول زمانی توسط تولید و وارسی یک عدد تصادفی R_B، کنترل می‌شود. (به پیوست ب) از استاندارد ملی ایران شماره ۱-۹۷۹۸: سال ۱۳۹۱مراجعه شود). سازوکار احراز هویت در شکل ۲ نمایش داده شده است.



شکل ۲- سازوکار ۲- احراز هویت دو گذره

قالب نشانه‌ی ($Token_{AB}$)، فرستاده شده از خواهان A به درستی‌سنج B:

$$Token_{AB} = Text_3 \,||\, e_{K_{AB}}(R_B \,||\, I_B \,||\, Text_2)$$

گنجاندن شناسه تشخیص‌دهنده‌ی I_B در $Token_{AB}$ اختیاری است.

یادآوری ۱- برای جلوگیری از احتمال پذیری یک حمله‌ی متن ساده‌ی انتخابی، برای مثال یک حمله‌ی رمز تحلیلی[1] که در آن رمز تحلیلگر، متن ساده‌ی کامل برای یک یا چند رشته‌ی متن رمز را می‌داند، هستار A شاید شامل یک عدد تصادفی R_A در $Text_2$ باشد.

یادآوری۲- شناسه تشخیص‌دهنده I_B در $Token_{AB}$ گنجانده شده است تا از استفاده هر یک از طرفین از $Token_{AB}$ به عنوان $Token_{BA}$ جلوگیری نماید. این گنجاندن اختیاری است تا در صورت لزوم، در محیط‌هایی که چنین حملاتی نمی‌تواند رخ دهد، حذف شود. اگر یک کلید یک طرفه استفاده شود نیز شناسه تشخیص‌دهنده I_B قابل حذف خواهد بود.

شرح سازوکار ۲- احراز هویت دو گذره، در ادامه آمده است:

(۱) B یک عدد تصادفی R_B را تولید و با یک فیلد متنی $Text_2$، به صورت اختیاری، برای A می‌فرستد.

(۲) A، $Token_{AB}$ را تولید و به B می‌فرستد.

(۳) B با دریافت پیام شامل $Token_{AB}$، و با واپوشیده‌سازی قسمت پوشیده‌شده [در اینجا واپوشیده‌سازی مستلزم آن است که الزاماتی که در بند ۵ ت - آمده است برآورده شوند] و سپس وارسی صحت شناسه تشخیص‌دهنده I_B، در صورت وجود، و اینکه عدد تصادفیR_B فرستاده شده به A در مرحله‌ی (۱) با عدد تصادفی موجود در $Token_{AB}$ مطابقت دارد، آن را درستی‌سنجی می‌کند.

۶-۲ احراز هویت دو جانبه

احراز هویت دو جانبه به این معناست که هر دو هستار مرتبط با استفاده از سازوکار یکدیگر را احراز هویت می-کنند.

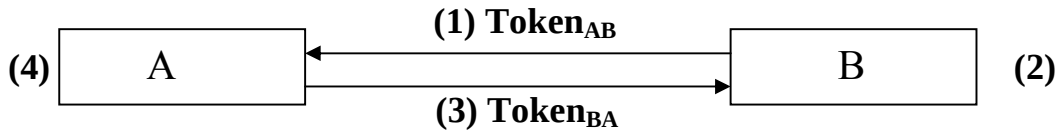
دو سازوکار توصیف شده در ۶-۱-۱ و ۶-۱-۲، برای احراز هویت دو جانبه، به ترتیب در ۶-۲-۱ و ۶-۲-۲ اقتباس شده‌اند. در هر دو حالت یک گذر و در نتیجه دو مرحله نیاز خواهد بود.

یادآوری- سازوکار سومی برای احراز هویت دو جانبه از دو نمونه سازوکار مشخص شده در ۶-۱-۲ یکی با شروع از هستار A و دیگری با هستار B قابل ساخت است.

۶-۲-۱ سازوکار ۳ – احراز هویت دو گذره

در این سازوکار احراز هویت یکتایی/ جدول زمانی توسط تولید و وارسی مهر زمانی یا اعداد دنباله‌ای، کنترل می‌شود (به پیوست ب از استاندارد ملی ایران شماره ۱-۹۷۹۸: سال ۱۳۹۱مراجعه شود).

سازوکار احراز هویت در شکل۳ نمایش داده شده است.



شکل ۳- سازوکار ۳- احراز هویت دو گذره

1- Cryptanalytic attack

قالب نشانه‌ی ($Token_{AB}$)، فرستاده شده از خواهان A به درستی‌سنج B، با آنکه در ۶-۱-۱ بیان شد یکسان است:

$$Token_{AB} = Text_2 \parallel e_{K_{AB}}(TN_A \parallel I_B \parallel Text_1)$$

قالب نشانه‌ی ($Token_{BA}$)، فرستاده شده از خواهان A به درستی‌سنج B:

$$Token_{BA} = Text_4 \parallel e_{K_{AB}}(TN_B \parallel I_A \parallel Text_3)$$

گنجاندن شناسه تشخیص‌دهنده I_B در $Token_{AB}$ و I_A در $Token_{BA}$ (به صورت مستقل) اختیاری است.

یادآوری- شناسه تشخیص‌دهنده I_B در $Token_{AB}$ گنجانده شده است تا از استفاده مجدد $Token_{AB}$ در هستار A با رقیبی که تظاهر می‌کند هستار B است جلوگیری نماید. به دلایل مشابه شناسه تشخیص‌دهنده I_A در $Token_{BA}$ قرار دارد. این گنجاندن‌ها اختیاری شده است تا در صورت لزوم، در محیط‌هایی که چنین حملاتی نمی‌تواند رخ دهد، یک یا هر دو حذف شوند. اگر کلیدهای یک طرفه استفاده شوند نیز شناسه‌های تشخیصی I_B و I_A قابل حذف خواهند بود (به زیر مراجعه شود).

شرح سازوکار ۳- احراز هویت دو گذره، در ادامه آمده است:

(۱) A، $Token_{AB}$ را تولید و به B می‌فرستد.

(۲) B با دریافت پیام شامل $Token_{AB}$، و با واپوشیده‌سازی قسمت پوشیده‌شده [در اینجا واپوشیده‌سازی مستلزم آن است که الزاماتی که در بند ۵ ت - آمده است برآورده شوند] و سپس وارسی صحت شناسه تشخیص‌دهنده I_B، در صورت وجود، به علاوه‌ی مهر زمانی و عدد دنباله، $Token_{AB}$ را درستی‌سنجی می‌کند.

(۳) B، $Token_{BA}$ را تولید و به A می‌فرستد.

(۴) با پیام مرحله‌ی (۳) به روشی مشابه مرحله‌ی (۲) در ۶-۱-۱ برخورد می‌شود.

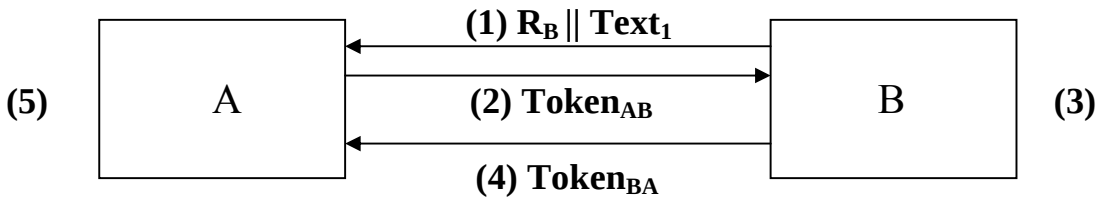
یادآوری- دو پیام این سازوکار به هیچ طریقی محدود به یکدیگر نیستند، جز به صورت خاص، به موقع بودن؛ این سازوکار به صورت مستقل دو بار از سازوکار ۶-۱-۱ استفاده می‌کند. پیوند بیشتر این پیام‌ها از طریق استفاده از فیلدهای متنی مناسب محقق خواهد شد.

اگر از کلیدهای یک طرفه استفاده شود آنگاه کلید K_{AB} در $Token_{BA}$ با کلید K_{BA} جایگزین شده و کلید مناسب در مرحله‌ی (۴) استفاده می‌شود.

۶-۲-۲ سازوکار ۴ – احراز هویت سه گذره

در این سازوکار احراز هویت، یکتایی/ جدول زمانی توسط تولید و وارسی اعداد تصادفی کنترل می‌شود (به پیوست ب از استاندارد ملی ایران شماره ۱-۹۷۹۸: سال ۱۳۹۱ مراجعه شود).

سازوکار احراز هویت در شکل ۴ نمایش داده شده است.



شکل ۴- سازوکار ۴- احراز هویت سه گذره

قالب نشانه‌ها به صورت زیر است:

$$Token_{AB} = Text_3 \,||\, e_{K_{AB}}(R_A \,||\, R_B \,||\, I_B \,||\, Text_2)$$

$$Token_{BA} = Text_5 \,||\, e_{K_{AB}}(R_B \,||\, R_A \,||\, Text_4)$$

گنجاندن شناسه تشخیص‌دهنده I_B در $Token_{AB}$ اختیاری است.

یادآوری- در صورت وجود، شناسه تشخیص‌دهنده I_B در $Token_{AB}$ گنجانده شده است تا از حمله‌ی به اصطلاح بازتاب جلوگیری نماید. چنین حمله‌ای به این صورت است که یک مهاجم، که تظاهر می‌کند A است، چالش R_B را به B، « بازتاب می‌کند». گنجاندن I_B اختیاری شده است تا در صورت لزوم، در محیط‌هایی که چنین حملاتی نمی‌تواند رخ دهد، یک یا هر دو حذف شوند. اگر یک کلید یک طرفه استفاده شود نیز شناسه‌های تشخیصدهنده‌ی I_B قابل حذف خواهد بود (به زیر مراجعه شود).

شرح سازوکار ۴ - احراز هویت سه گذره، در ادامه آمده است:

(۱) B یک عدد تصادفی R_B تولید و با یک فیلدی متنی $Text_2$، اختیاری، برای A می‌فرستد.

(۲) A یک عدد تصادفی R_A تولید و با یک فیلدی متنی $Text_2$، اختیاری، برای B می‌فرستد.

(۳) B با دریافت پیام شامل $Token_{AB}$، و با واپوشیده سازی قسمت پوشیده‌شده [در اینجا واپوشیده‌سازی مستلزم آن است که الزاماتی که در بند ۵ ت - آمده است برآورده شوند] و سپس وارسی صحت شناسه تشخیص‌دهنده I_B، در صورت وجود، و اینکه عدد تصادفی R_B فرستاده شده به A در مرحله‌ی (۱) با عدد تصادفی موجود در $Token_{AB}$ مطابقت دارد، آن را درستی‌سنجی می‌کند.

(۴) B، $Token_{BA}$ را تولید و به A می‌فرستد.

(۵) A با دریافت پیام شامل $Token_{BA}$، و با واپوشیده سازی قسمت پوشیده‌شده [در اینجا واپوشیده‌سازی مستلزم آن است که الزاماتی که در بند ۵ ت - آمده است برآورده شوند] و سپس وارسی صحت شناسه تشخیص‌دهنده I_B، در صورت وجود، و اینکه عدد تصادفی R_B دریافتی از B در مرحله‌ی (۱) و عدد تصادفی R_A فرستاده شده به B در مرحله‌ی (۲) با عدد تصادفی موجود در $Token_{BA}$ مطابقت دارد، $Token_{BA}$ را درستی‌سنجی می‌کند.

اگر از کلیدهای یک طرفه استفاده شود آنگاه کلید K_{AB} در $Token_{BA}$ با کلید K_{BA} جایگزین شده و کلید مناسب در مرحله‌ی (۵) استفاده می‌شود.

۷ سازوکارها شامل طرف سوم مورد اعتماد

سازوکارهای احراز هویت این بند از کلید سرّی مشترکی بین دو هستار، قبل از فرایند احراز هویت، استفاده نمی‌کنند. بلکه آنها از یک طرف سوم مورد اعتماد (که با P نمایش داده می‌شود) استفاده می‌کنند که با آن هر یک از هستارهای A و B یک کلید محرمانه، به ترتیب K_{AP} و K_{BP}، به اشتراک گذاشته‌اند. در هر دو سازوکار یکی از هستارها، یک کلید K_{AB} از طرف سوم مورد اعتماد درخواست می‌کند. این فرایند با اقتباسی از سازوکار-های مشروح در، به ترتیب، ۶-۲-۱ و ۶-۲-۲ دنبال می‌شود.

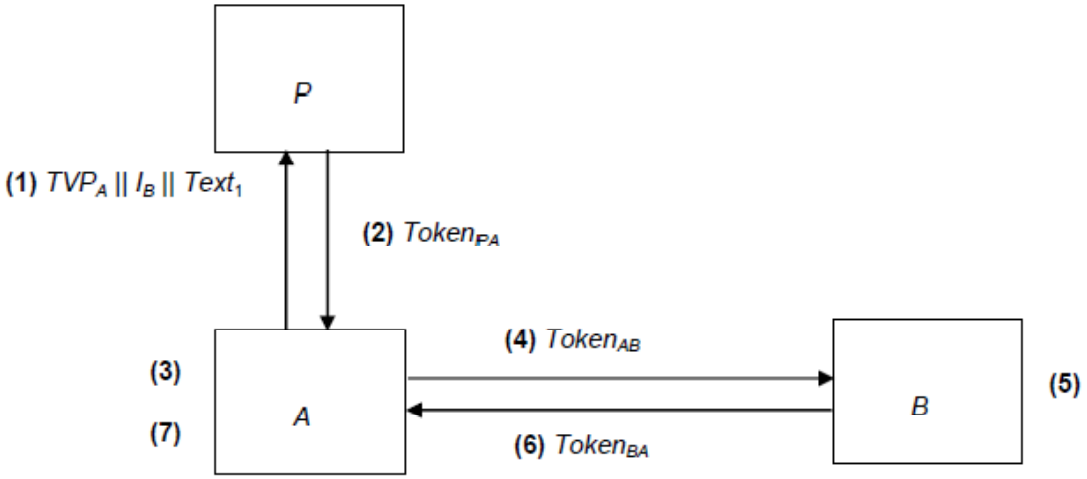
همان‌گونه که قبلاً شرح داده شد، اگر تنها احراز هویت یک جانبه مورد نیاز باشد، گذرهای معینی از هر سازوکار قابل حذف هستند.

تمام فیلدهای متنی مشخص‌شده در سازوکارهای ذیل برای استفاده، در برنامه‌های کاربردی خارج از دامنه‌ی این قسمت از این مجموعه استاندارد ملی در دسترس هستند (ممکن است خالی باشند). ارتباط و محتوای آنها به آن کاربرد مشخص وابسته می‌باشد. برای اطلاع از کاربرد فیلدهای متنی به پیوست ب - مراجعه شود.

۷-۱ سازوکار ۵ – احراز هویت چهار گذره

این سازوکار معادل با سازوکار ایجاد کلید ۸ در ISO/IEC 11770-2 :2008 می‌باشد.

سازوکار احراز هویت در شکل۵ نمایش داده شده است.



شکل ۵- سازوکار ۵- احراز هویت چهار گذره

قالب نشانه‌ی ($Token_{PA}$) فرستاده شده از P به A :

$$Token_{PA} = Text_4 \| e_{K_{AP}}(TVP_A \| K_{AB} \| I_B \| Text_3) \| e_{K_{BP}}(TN_P \| K_{AB} \| I_A \| Text_2)$$

قالب نشانه‌ی ($Token_{AB}$) فرستاده شده از A به B :

$$Token_{AB} = Text_6 \,||\, e_{K_{BP}}(TN_P \,||\, K_{AB} \,||\, I_A \,||\, Text_2) \,||\, e_{K_{AB}}(TN_A \,||I_B|| \, Text_5)$$

قالب نشانه‌ی ($Token_{BA}$) فرستاده شده از B به A :

$$Token_{BA} = Text_8 \,||\, e_{K_{AB}}(TN_B \,||\, I_A \,||\, Text_7)$$

انتخاب استفاده از مهرهای زمانی یا اعداد دنباله‌ای در این سازوکار، به قابلیت‌های هستارهای درگیر و همچنین محیط وابسته است.

استفاده از پارامتر متغیر با زمان TVP_A در مراحل (۱) تا (۳) از شکل ۵، همانگونه که در زیر بیان شده، تا اندازه‌ای از استفاده‌ی معمول آن متفاوت است. این کار به A اجازه می‌دهد که پیام پاسخ (۲) را به پیام درخواست (۱) پیوند دهد. ویژگی مهم پارامتر متغیر با زمان در اینجا تکرارنشدنی بودن آن، برای محدودیت استفاده‌ی مجدد از نشانه‌ی قبلا مصرف شده‌ی $Token_{PA}$ ، است.

یادآوری- پارامتر متغیر با زمان TVP_A می‌تواند یک عدد تصادفی باشد. با این حال، برخلاف اعداد تصادفی مورد استفاده در برخی سازوکارهای این قسمت از مجموعه استاندارد ملی، لازم نیست TVP_A برای طرف سوم غیر قابل پیش‌بینی باشد و یک مقدار شمارنده‌ی تکرارنشدنی نیز مناسب خواهد بود.

شرح سازوکار ۵ - احراز هویت چهار گذره، در ادامه آمده است:

(۱) A یک پارامتر متغیر با زمان TVP_A تولید کرده و آن را به همراه شناسه‌ی تشخیص‌دهنده‌ی I_B و یک فیلدی متنی $Text_1$، به صورت اختیاری، به طرف سوم مورد اعتماد P می‌فرستد.

(۲) طرف سوم مورد اعتماد P، $Token_{PA}$ را تولید و به A می‌فرستد.

(۳) A با دریافت پیام شامل $Token_{PA}$، و با واپوشیده‌سازی قسمت پوشیده‌سازی شده [در اینجا واپوشیده‌سازی مستلزم آن است که الزاماتی که در بند ۵ ت - آمده است برآورده شوند] و سپس وارسی صحت شناسه تشخیص‌دهنده‌ی I_B، و اینکه پارامتر متغیر با زمان فرستاده شده به P در مرحله‌ی (1) با پارامتر متغیر با زمان موجود در $Token_{PA}$ مطابقت دارد، آن را درستی‌سنجی می‌کند. به علاوه، A کلید احراز هویت محرمانه K_{AB} را بازیابی می‌کند. A سپس

$$e_{K_{BP}} = (TN_p \,||K_{AB}||I_A|| \, Text_2)$$

را از $Token_{PA}$ استخراج کرده و از آن برای ساخت $Token_{AB}$ استفاده می‌کند.

(۴) A، $Token_{AB}$ را تولید و به B می‌فرستد.

(۵) B با دریافت پیام شامل $Token_{AB}$، و با واپوشیده‌سازی قسمت پوشیده‌سازی شده [در اینجا واپوشیده‌سازی مستلزم آن است که الزاماتی که در بند ۵ ت - آمده است برآورده شوند] و سپس وارسی صحت شناسه‌های تشخیصی I_B و I_A به علاوه‌ی مهر زمانی(ها) یا عدد دنباله(ها)، $Token_{AB}$ را درستی‌سنجی می‌کند. B کلید احراز هویت سرّی K_{AB} را بازیابی می‌کند.

(۶) B، $Token_{BA}$ را تولید و به A می‌فرستد.

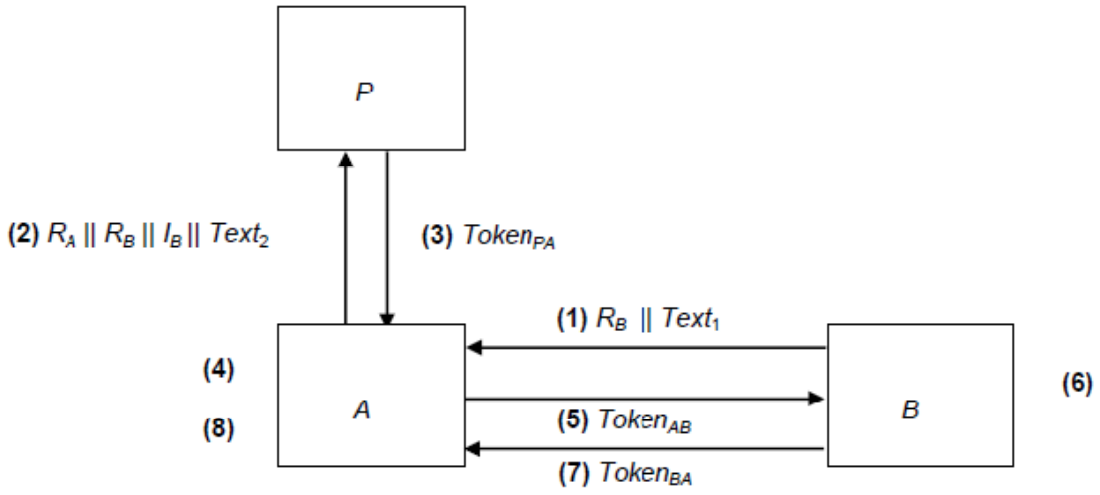
(۷) A با دریافت پیام شامل $Token_{BA}$، و با واپوشیده‌سازی قسمت پوشیده‌سازی شده [در اینجا واپوشیده‌سازی مستلزم آن است که الزاماتی که در بند ۵ ت - آمده است برآورده شوند] و سپس وارسی صحت شناسه تشخیص‌دهنده I_A به علاوه‌ی مهر زمانی یا عدد دنباله، $Token_{BA}$ را درستی‌سنجی می‌کند.

اگر فقط احراز هویت یک جانبه از A به B نیاز باشد،مراحل (۶) و (۷) قابل حذف خواهند بود.

۲-۷ سازوکار ۶ – احراز هویت پنج گذره

در این سازوکار احراز هویت دو جانبه، یکتایی/ به موقع بودن توسط اعداد تصادفی کنترل می‌شود. (به پیوست ب از استاندارد ملی ایران شماره ۱-۹۷۹۸: سال ۱۳۹۱ مراجعه شود). این سازوکار معادل با سازوکار ایجاد کلید ۹ در ISO/IEC 11770-2 :2008 می‌باشد.

سازوکار احراز هویت در شکل ۶ نمایش داده شده است.



شکل ۶- سازوکار ۶- احراز هویت پنج گذره

قالب نشانه‌ی ($Token_{PA}$) فرستاده شده از P به A :

$$Token_{PA} = Text_5 \| e_{K_{AP}}(R_A \| K_{AB} \| I_B \| Text_4) \| e_{K_{BP}}(R_B \| K_{AB} \| I_A \| Text_3)$$

قالب نشانه‌ی ($Token_{AB}$) فرستاده شده از A به B:

$$Token_{AB} = Text_7 \| e_{K_{BP}}(R_B \| K_{AB} \| I_A \| Text_3) \| e_{K_{AB}}(R'_A \| R_B \| Text_6)$$

قالب نشانه‌ی ($Token_{BA}$) فرستاده شده از B به A :

$$Token_{BA} = Text_9 \,||\, e_{K_{AB}}(R_B \,||\, R'_A \,||\, Text_8)$$

شرح سازوکار ۶ - احراز هویت پنج گذره، در ادامه آمده است:

(۱) B یک عدد تصادفی R_B تولید و با یک فیلدی متنی $Text_1$، اختیاری، برای A می‌فرستد.

(۲) A یک عدد تصادفی R_A تولید کرده و آن را به همراه عدد تصادفی R_B، شناسه‌ی تشخیص‌دهنده I_B و یک فیلدی متنی $Text_2$، به صورت اختیاری، به طرف سوم مورد اعتماد P می‌فرستد.

(۳) طرف سوم مورد اعتماد P، $Token_{PA}$ را تولید و به A می‌فرستد.

(۴) A با دریافت پیام شامل $Token_{PA}$، و با واپوشیده‌سازی قسمت پوشیده‌شده [در اینجا واپوشیده‌سازی مستلزم آن است که الزاماتی که در بند ۵ ت - آمده است برآورده شوند] و سپس وارسی صحت شناسه تشخیص‌دهنده I_B، و اینکه عدد تصادفی R_A فرستاده شده به P در مرحله‌ی (۲) با عدد تصادفی موجود در $Token_{PA}$ مطابقت دارد، آن را درستی‌سنجی می‌کند. به علاوه، A کلید احراز هویت سرّی K_{AB} را بازیابی می‌کند. A سپس

$$e_{K_{BP}} = (R_B \,||K_{AB}||I_A||\, Text_3)$$

را از $Token_{PA}$ استخراج کرده و از آن برای ساخت $Token_{AB}$ استفاده می‌کند.

(۵) A، عدد تصادفی ثانویه R'_A را تولید و سپس $Token_{AB}$ را تولید و به B می‌فرستد.

(۶) B با دریافت پیام شامل $Token_{AB}$، و با واپوشیده‌سازی قسمت پوشیده‌شده [در اینجا واپوشیده‌سازی مستلزم آن است که الزاماتی که در بند ۵ ت - آمده است برآورده شوند] و سپس وارسی صحت شناسه‌ی تشخیص‌دهنده I_A و اینکه عدد تصادفی R_A فرستاده شده به A در مرحله‌ی (۱) با هر دو کپی موجود در $Token_{AB}$ مطابقت دارد، آن را درستی‌سنجی می‌کند. B کلید احراز هویت سرّی K_{AB} را بازیابی می‌کند.

(۷) B، $Token_{BA}$ را تولید و به A می‌فرستد.

(۸) A با دریافت پیام شامل $Token_{BA}$ و با واپوشیده‌سازی قسمت پوشیده‌شده [در اینجا رمزگشایی مستلزم آن است که الزاماتی که در بند ۵ ت - آمده است برآورده شوند] و سپس وارسی اینکه عدد تصادفی R_B دریافتی از B در مرحله‌ی (۱) و عدد تصادفی R'_A فرستاده شده به B در مرحله‌ی (۵) هر کدام با عدد تصادفی موجود در $Token_{BA}$ مطابقت دارد، آن را درستی‌سنجی می‌کند.

اگر فقط احراز هویت یک جانبه از A به B نیاز باشد، مراحل (۷) و (۸) قابل حذف خواهند بود.

پیوست الف

(الزامی)

OIDها و ASN.1syntax

الف-۱ تعریف رسمی

```
EntityAuthenticationMechanisms-2    {

     iso (1)  standard (0)  e-auth-mechanisms (9798)  part (2)

         Ans1-module (0)  object-identifiers (0)    }

     DEFINITION  EXPLICIT  TAGS  : := BEGIN

-- EXPORTS ALL; --

-- IMPORTS None; --

OID : :=OBJECT  IDENTIFIER -- alias

-- Synonyms --

is9798-2 OID : := {   iso (1)  standard (0)  e-auth-mechanisms (9798)  part2
(2)  }

mechanism OID : := {   is9798-2 mechanism (1)   }


--   Unilateral  and  mutual  entity  authentication  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   }

--   Mutual  entity  authentication  mechanisms  involving  a trusted  third
 party   --

ttp-four-pass  OID  : :=  {   mechanism  5   }

ttp-five-pass  OID  : :=  {   mechanism  6   }

END  --  EntityAuthenticationMechanisms-2    --
```

الف-۲ استفاده از شناسه‌های شی بعدی

هر یک از سازوکارهای احراز هویت هستار از یک فن رمزبندی متقارن استفاده می‌کنند. بنابراین، شناسه‌ی شی سازوکار احراز هویت هستار ممکن است بوسیله‌ی یک شناسه‌ی شیء، که فن رمزبندی مورد استفاده را بیان می‌کند، دنبال شود، مثلا شناسه‌ای برای سازوکارهای بیان شده در ISO/IEC 19772.

الف-۳ مثال‌های کدنویسی مطابق با قواعد بنیادی کدبندی ASN.1

طبق ISO/IEC 8825-1، یک شناسه‌ی شیء شامل یک یا چند ردیف از گروه‌های هشت‌تایی است. هر ردیف یک عدد را کدگذاری می‌کند.

- اگر بیش از یک گروه هشت‌تایی موجود باشد، بیت ۸ (با ارزش‌ترین بیت) در آخرین گروه هشت‌تایی هر ردیف را صفر و در گروه‌های هشت‌تایی قبلی یک قرار می‌دهیم.
- توالی بیت‌های ۷ تا ۱ گروه‌های هشت‌تایی هر ردیف یک عدد را کدگذاری می‌کند. هر عدد باید با کمترین مقدار عدد در گروه‌های هشت‌تایی کدگذاری شود، به عبارت دیگر، ′80 در اولین جایگاه یک ردیف، فاقد اعتبار است.
- اولین عدد، شماره‌ی استاندارد است؛ عدد دوم، در صورت وجود، شماره‌ی قسمت در استانداردهای چندقسمتی است.

یک شناسه ممکن است به هر سازوکاری که در این سند تعریف شده ارجاع نماید.

- برای شناسایی یک استاندارد ISO، اولین گروه هشت‌تایی برابر ′28 قرار داده می‌شود، یعنی ۴۰ در مقیاس دهدهی (به ISO/IEC 8825-1 مراجعه کنید).
- دو گروه هشت‌تایی بعدی را برابر ′CC46 قرار می‌دهیم. ۹۷۹۸ برابر ′2646 در مقیاس ۶۰تایی، یعنی، 0110 0100 0110 0010 به عبارت دیگر، دو بلوک بیت هفت:10011001000110 .بعد از افزودن مقدار مناسب از بیت ۸ به هر گروه هشت‌تایی، کدبندی ردیف‌ها برابر 1100110001000110 ،یعنی، ′CC46 است.
- گروه هشت‌تایی بعدی را برای شناسایی قسمت ۲ برابر ′02 قرار داده می‌شود.
- گروه هشت‌تایی بعدی سازوکار احراز هویت را شناسایی می‌کند.
- ′01 یک سازوکار احراز هویت یک جانبه یک گذره، بدون طرف سوم مورد اعتماد را شناسایی می‌کند.
- ′02 یک سازوکار احراز هویت یک جانبه دو گذره، بدون طرف سوم مورد اعتماد را شناسایی می‌کند.
- ′03 یک سازوکار احراز هویت دو جانبه دو گذره، بدون طرف سوم مورد اعتماد را شناسایی می‌کند.
- ′04 یک سازوکار احراز هویت دو جانبه سه گذره، بدون طرف سوم مورد اعتماد را شناسایی می‌کند.
- ′05 یک سازوکار احراز هویت دو جانبه چهار گذره، شامل طرف سوم مورد اعتماد را شناسایی می‌کند.

- ′06′ یک سازوکار احراز هویت دو جانبه پنج گذره، شامل طرف سوم مورد اعتماد را شناسایی می‌کند.

برای مثال عنصر داده ′28 CC 46 02 05′ به صورت {iso standard 9798 2 5} خوانده می‌شود، به طور مثال، پنجمین سازوکار در این قسمت از این استاندارد ملی، به عبارت دیگر، سازوکار احراز هویت دو جانبه چهار گذره شامل طرف سوم مورد اعتماداست. این جزء داده ممکن است در شیء داده BER-TLV فرستاده شود که در آن خط فاصله‌ها و کروشه‌ها اهمیت خاصی ندارند و تنها برای وضوح بیشتر اضافه شده‌اند (به قواعد بنیادی کد بندی ASN.1، ISO/IEC 8825-1، برچسب کلاس عمومی ′06′ مراجعه کنید).

Data object = {′06′ – ′05′ - ′28 CC 46 02 05′ }

پیوست ب

(اطلاعاتی)

استفاده از فیلدهای متنی

نشانه‌های مشخص شده در بندهای ۶ و ۷ از این قسمت از این استاندارد ملی شامل فیلدهای متنی است. استفاده‌ی واقعی و ارتباط بین فیلدهای متنی متنوع، در یک گذر معین، وابسته به کاربرد می‌باشد. مثالی در ذیل آمده است؛ به پیوست الف از استاندارد ملی ایران شماره ۱-۹۷۹۸: سال ۱۳۹۱نیز مراجعه شود.

- هرگونه اطلاعات که نیاز به محرمانگی و احراز هویت اصلی دارد باید در قسمت پوشیده سازی شده‌ی هر نشانه قرار داده شود.

پیوست پ

(اطلاعاتی)

ویژگی‌های سازوکارهای احراز هویت هستار

جدول پ-۱ خصوصیات اصلی سازوکار احراز هویت هستار بیان شده در این استاندارد ملی را خلاصه می‌نماید. موارد اختیاری در پرانتز نمایش داده شده‌اند، برای مثال سازوکار ۵ یک مدل اختیاری سه گذره از پروتکل، برای احراز هویت یک جانبه، دارا می‌باشد.

جدول پ-۱- ویژگی‌های سازوکارها

سازوکار	۱	۲	۳	۴	۵	۶
تعداد گذرها	۱	۲	۲	۲	۴ (یا به صورت اختیاری۳)	۵ (یا به صورت اختیاری۴)
یک جانبه/ دوجانبه بین درستی‌سنج و خواهان	یک جانبه	یک جانبه	دوجانبه	دو جانبه	دو جانبه (یک جانبه)	دو جانبه (یک جانبه)
متغیر(ها)ی ضمانت‌کننده تازگی(یادآوری۱)	TN_A	R_B	TN_A و TN_B	R_A و R_B	TVP_A, TN_B و TN_P	R_A و R_B
هستار آغازکننده‌ی سازوکار (احراز هویت)	A	B	A	B	A	B
آگاهی خواهان از موفقیت (یادآوری۲)	خیر	خیر	فقط برایA	فقط برایA	فقط برایA	فقط برایA

یادآوری‌های زیر برای جدول به کار برده می‌شود:

یادآوری۱- برای سازوکارهای ۲، ۴ و ۶ که از عدد(ها)ی تصادفی برای ضمانت تازگی[1] استفاده می‌کنند، نیازی به نگهداری ساعت‌های همزمانی یا اعداد دنباله‌ای بین دو هستار وجود ندارد.

یادآوری۲- در سازوکارهای احراز هویت توصیف شده در این استاندارد، خواهان، اثبات هویت را در قالب یک نشانه‌ی رمزبندی شده می‌فرستد. در برخی موارد هیچ پاسخی از هستارهای دیگر برای نشان دادن اینکه اثبات هویت با موفقیت پذیرفته شده بود، وجود ندارد. آخرین ردیف از جدول پ-۱ نشان می‌دهد که کجا پروتکل به طور ذاتی آگاهی از احراز هویت موفق را ضمانت می‌کند. در تمامی موارد دیگر، در صورت نیاز، سامانه باید شرط آگاهی از موفقیت را برای خواهان قرار دهد.

1- Freshness

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 9797-1:1999, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher

[3] ISO/IEC 9798-5:2004, Information technology — Security techniques — Entity authentication — Part 5: Mechanisms using zero-knowledge techniques

[۴] استاندارد ملی ۹۶۰۰: سال ۱۳۸۶ فناوری اطلاعات - روشهای امنیتی – حالت‌های عملیاتی یک الگوریتم رمزنگاری قطعه ای N بیتی

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

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

[۷] استاندارد ملی ۱-۱۱۳۱۰: سال ۱۳۸۷ فناوری اطلاعات- فنون امنیتی-خدمت های مهرزمانی- قسمت اول: چارچوب

[8] ISO/IEC 18031, Information technology — Security techniques — Random bit generation

[9] ISO/IEC 19772:—2), Information technology — Security techniques — Authenticated encryption