ISIRI
10825-4
1st. edition

جمهوری اسلامی ایران
Islamic Republic of Iran
مؤسسه استاندارد وتحقیقات صنعتی ایران
Institute of Standards and Industrial Research of Iran

استاندارد ملی ایران
۱۰۸۲۵-۴
چاپ اول

فن‌آوری اطلاعات - فنون امنیتی - تشخیص هویت نهاد - قسمت چهارم: مکانیزم‌های استفاده‌کننده از یک تابع‌مقابله رمزنگاری

Information technology – Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function

ICS:35.040

به‌نام خدا

آشنایی با مؤسسهٔ استاندارد و تحقیقات صنعتی 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.

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان مؤسسه* صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فن‌آوری 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 می‌شود .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 می‌شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذیصلاح 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 می‌شود .بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که مؤسسه استاندارد تشکیل می‌دهد به تصویب رسیده باشد.

مؤسسهٔ استاندارد و تحقیقات صنعتی 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 پیشرفتهای علمی، فنی و صنعتی جهان و استانداردهای بینالمللی بهره‌گیری می‌شود.

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران می‌تواند 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 کشو ر و / یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. مؤسسه می‌تواند 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 سا زمانها 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 ، مؤسسهٔ استاندارد 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 آنها 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 مؤسسه است.

---

* موسسهٔ استاندارد و تحقیقات صنعتی ایران

1 - International organization for Standardization
2 - International Electro technical Commission
3 - International Organization for Legal Metrology (Organization International de Metrology Legal)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« فن‌آوری اطلاعات - فنون امنیتی - تشخیص هویت نهاد - »

« قسمت چهارم: مکانیزم‌های استفاده‌کننده از یک تابع‌مقابله رمزنگاری »

	سمت و/ یا نمایندگی
رئیس:	
حسینی خیاط ، سعید	عضو هیات علمی دانشکده مهندسی
(دکترای مهندسی برق)	دانشگاه فردوسی مشهد
دبیر:	
خانیکی ، رضا	اداره کل استاندارد و تحقیقات صنعتی
(لیسانس مهندسی برق - مخابرات)	خراسان رضوی
اعضاء: (اسامی به ترتیب حروف الفبا)	
اثنی عشری ، امیر مهدی	موسسه تحقیقات و فن آوری پارس
(لیسانس مهندسی برق - کنترل)	
ارومیه‌چی‌ها ، محمدعلی	شرکت صنایع الکترونیک زعیم
(فوق لیسانس مهندسی مخابرات- رمز)	(سهامی خاص)
رضایی ، امید	شرکت مهندسی ایمن رایانه شرق
(فوق لیسانس مهندسی مخابرات- رمز)	(سهامی خاص)
سهی زاده ابیانه ، محمد رضا	شرکت صنایع الکترونیک زعیم
(فوق لیسانس مهندسی مخابرات- رمز)	(سهامی خاص)
طوماریان ، سهیلا	مؤسسهٔ استاندارد و تحقیقات صنعتی
(لیسانس مهندسی برق- الکترونیک)	ایران
فرزاد ، پویان	گروه مهندسین فن‌آوری نوین ۵۲
(فوق لیسانس ریاضی‌کاربردی)	

میرمطهری ، نوید
(فوق لیسانس مهندسی برق- مخابرات)
اداره مخابرات و ارتباطات رادیویی
آستان قدس رضوی

فهرست مندرجات

پیش گفتار

استاندارد " فن‌آوری اطلاعات - فنون امنیتی - تشخیص هویت نهاد -- قسمت چهارم: مکانیزم‌های استفاده-کننده از یک تابع‌مقابله رمزنگاری" که پیش نویس آن درکمیسیون های مربوط توسط (مؤسسهٔ استاندارد و تحقیقات صنعتی ایران) تهیه و تدوین شده و در پنجاه و چهارمین اجلاس کمیتهٔ ملی استاندارد رایانه و فرآوری داده‌ها مورخ ۸۷/۸/۱۲ مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ 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.

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

1- ISO/IEC 9798-4:1999, 2nd Ed.: Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function

۲ - کلیه واژگان مصوب فرهنگستان علوم, سایت اینترنتی فرهنگستان زبان و ادبیات پارسی
http://www.persianacademy.ir/

فن‌آوری اطلاعات - فنون امنیتی – تشخیص هویت نهاد[1] --
قسمت چهارم: مکانیزم‌های استفاده‌کننده از یک تابع‌مقابله رمزنگاری[2]

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، مشخص کردن مکانیزم هایی است که برای تشخیص‌هویت نهاد از یک تابع‌مقابله[3] رمزنگاری استفاده می‌کنند. دو مکانیزم مربوط به تشخیص هویت یک نهاد (تشخیص هویت یک‌جانبه[4]) بوده و بقیه مکانیزم ها برای تشخیص‌هویت دوطرفه[5] دونهاد مورد استفاده قرار می‌گیرند.

مکانیزم های مشخص شده در این قسمت از مجموعه استاندارد ملی ایران به شماره ۱۰۸۲۵، از پارامترهای متغیر با زمان مانند تمبرهای زمانی[6]، شماره‌های توالی[7] و یا اعداد تصادفی[8] استفاده می کنند تا از پذیرفته پذیرفته شدن اطلاعات تشخیص هویت معتبر در آینده یا برای بیش از یک بار جلوگیری کنند.

اگر از یک تمبر زمانی یا یک شماره توالی استفاده شود، یک‌مرحله تبادل اطلاعات برای تشخیص هویت یک‌جانبه مورد نیاز است، در حالی‌که برای تشخیص هویت دوطرفه دو مرحله تبادل اطلاعات تشخیص‌هویت مورد نیاز است. اگر از یک روش چالش - پاسخ[9] که اعداد تصادفی را بکار می‌گیرد، استفاده شود؛ دو مرحله تبادل اطلاعات برای تشخیص‌هویت یک‌جانبه مورد نیاز است، در حالیکه برای تشخیص‌هویت دوطرفه سه‌مرحله تبادل اطلاعات تشخیص‌هویت مورد نیاز است.

نمونه هایی از توابع مقابله رمزنگاری در مجموعه استاندارد ISO/IEC 9797 ذکر شده‌اند.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی هستند که در متن این استاندارد به آن‌ها ارجاع شده است، و به این ترتیب جزئی از این استاندارد محسوب می‌شوند.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن موردنظر این استاندارد نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

2-1 ISO/IEC 9797 (all parts), Information technology - Security Techniques - Message Authentication Codes (MACs)

---

1 - Entity Authentication
2 - Cryptographic check function
3 - Check function
4 - Unilateral authentication
5 - Mutual authentication
6 - Time stamps
7 - Sequence numbers
8 - Random numbers
9 - Challenge and response method

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

۳ اصطلاحات و نمادها[1]

در این قسمت از مجموعه استاندارد ملی ایران به شماره ۱۰۸۲۵، اصطلاحات و نمادهای بیان شده در ISO/IEC 9798-1 مورد استفاده قرار می‌گیرند.

۴ الزامات

در مکانیزم های تشخیص‌هویتی که در این قسمت از مجموعه استاندارد ملی ایران به شماره ۱۰۸۲۵ مشخص شده‌اند، نهادی که قرار است هویت آن تشخیص داده شود، هویت خود را با نشان دادن دانش خود درباره یک کلید تشخیص‌هویت محرمانه[2]، اثبات می‌کند. نهاد برای این کار، با استفاده از کلیدمحرمانه[3] خود، خود، یک تابع‌مقابله رمزنگاری را روی یک داده مشخص اعمال کرده و یک مقدارمقابله[4] رمزنگاری بدست می‌آورد. این مقدارمقابله رمزنگاری می‌تواند توسط هر فردی که کلیدمحرمانه تشخیص‌هویت نهاد با او به اشتراک گذاشته شده‌است، بررسی شود؛ این فرد می‌تواند مقدارمقابله رمزنگاری را مجدداً محاسبه نموده و با مقدار دریافتی مقایسه کند.

مکانیزم های تشخیص‌هویت دارای الزامات زیر هستند. اگر هر یک از این الزامات برآورده نشوند، امکان دارد که امنیت فرایند تشخیص‌هویت به خطر بیافتد[5] و یا پیاده‌سازی فرایند تشخیص‌هویت امکان‌پذیر نباشد.

الف- یک نهادمدعی[6] که قصد دارد تا هویت خود را به یک نهادتاییدکننده[7] اثبات کند، یک کلید تشخیص‌هویت محرمانه را با آن نهاد به اشتراک می‌گذارد. طرفین باید هر بار قبل از آغاز اجرای مکانیزم ویژه تشخیص‌هویت، از این کلید آگاه باشند. روش توزیع کلید بین نهادها، خارج از دامنه کاربرد این استاندارد است.

ب- کلید تشخیص‌هویت محرمانه به اشتراک گذاشته شده بین نهادمدعی و نهادتاییدکننده باید تنها در اختیار این دو نهاد و درصورت‌امکان طرف‌های دیگری که هر دو نهاد به آنها اعتماد دارند، باشد.

پ- قدرت مکانیزم ها به طول و محرمانه بودن کلید، طبیعت توابع مقابله رمزنگاری و طول مقدارمقابله وابسته است. این پارامترها باید به گونه ای انتخاب شوند که سطح امنیتی مورد نیاز را که ممکن است در سیاست امنیتی[8] مشخص شده باشد، تامین کنند.

---

1 - Notation
2 - Secret authentication key
3 - Secret key
4 - Check value
5 - Compromise : به خطر افتادن، خطر کشف رمز، تسخیر
6 - Claimant
7 - Verifier
8 - Security policy

۵ مکانیزم‌ها

در این مکانیزم‌های تشخیص‌هویت، نهادهای A و B باید هر بار قبل از آغاز اجرای مکانیزم تشخیص‌هویت بصورت خاص، یک کلید تشخیص‌هویت محرمانه K_{AB} یا دو کلیدمحرمانه یک‌سویه[1] K_{AB} و K_{BA} را به اشتراک بگذارند. در حالت دوم، کلیدهای محرمانه یک‌سویه K_{AB} و K_{BA} به ترتیب برای تشخیص‌هویت A توسط B و B توسط A مورد استفاده قرار می‌گیرند.

این مکانیزم‌ها نیازمند استفاده از پارامترهای متغیر با زمان مانند تمبرهای زمانی، شماره‌های توالی و یا اعداد تصادفی هستند. خصوصیات پارامترهای متغیر با زمان، برای امنیت این مکانیزم‌ها مهم هستند. بویژه، پارامترها باید به گونه ای انتخاب شوند که تکرار آنها در طول عمر کلید تشخیص‌هویت، دارای کمترین احتمال باشد. برای اطلاعات بیشتر به پیوست ب از استاندارد ISO/IEC 9798-1 رجوع کنید.

استفاده از قسمت های متنی مشخص شده در مکانیزم های زیر، خارج از دامنه کاربرد این استاندارد است (این قسمت‌ها می‌توانند تهی باشند)، و به کاربرد خاص بستگی خواهد داشت. برای دستیابی به اطلاعات بیشتر در مورد شیوه استفاده از قسمت های متنی، به پیوست الف رجوع کنید.

یک قسمت متنی تنها در صورتی می‌تواند در ورودی تابع‌مقابله رمزنگاری مورد استفاده قرار گیرد که نهادتاییدکننده اعتبار بتواند آن را به طور مستقل تعیین کند، به عنوان مثال، اگر از قبل معلوم باشد، بصورت پرنشده ارسال شده باشد و یا از طریق یک یا هر دو منبع قابل دریافت[2] باشد.

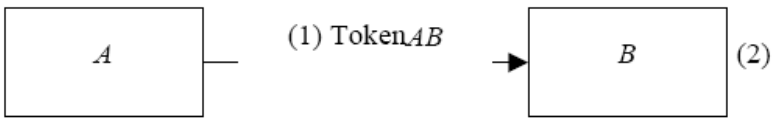
۵-۱ تشخیص‌هویت یک‌جانبه

تشخیص‌هویت یک‌جانبه به این معنی است که با استفاده از مکانیزم، تنها هویت یکی از دو نهاد تشخیص داده می شود.

۵-۱-۱ تشخیص‌هویت یک‌مرحله‌ای[3]

در این مکانیزم تشخیص‌هویت، نهادمدعی A فرایند را آغاز می کند و توسط نهادتاییدکننده B مورد تشخیص‌هویت قرار می گیرد. یکتا بودن / بهنگام بودن با تولید و بررسی یک تمبر زمانی یا یک شماره توالی کنترل می‌شود (به پیوست ب از استاندارد ISO/IEC 9798-1 رجوع کنید).

مکانیزم تشخیص‌هویت، در شکل ۱ نمایش داده شده است.



شکل ۱- تشخیص هویت یک مرحله‌ای

قالب نشانه (TokenAB) که از نهاد مدعی A به B ارسال می‌شود، بصورت زیر است:

---

9 - Unidirectional
1 - Derived
2- One pass authentication

$$TokenAB = \overset{T_A}{N_A} \| Text2 \| f_{K_{AB}}(\overset{T_A}{N_A} \| B \| Text1)$$

که در آن، نهاد مدعی A از یک شماره توالی N_A یا یک تمبر زمانی T_A به عنوان پارامتر متغیر با زمان استفاده می‌کند. انتخاب پارامتر متغیر با زمان، به امکانات فنی نهادمدعی و نهادتاییدکننده و همچنین محیط اجرا بستگی دارد. همانگونه که در استاندارد ISO/IEC 9798-1 تعریف شده است، $f_K(X)$ نشاندهنده مقدارمقابله رمزنگاری است که با اعمال تابع‌مقابله رمزنگاری f روی داده X با استفاده از کلید K محاسبه شده است.

گنجاندن شناسه متمایزکننده B در TokenAB اختیاری است.

یادآوری – شناسه متمایز کننده B در TokenAB گنجانده می‌شود تا از استفاده مجدد از TokenAB برای نهاد A توسط دشمنی که خود را به عنوان نهاد B معرفی می کند، جلوگیری شود. گنجاندن شناسه متمایز کننده B اختیاری قرار داده شده است تا در محیط هایی که امکان چنین حمله هایی وجود ندارد، بتوان شناسه متمایز کننده B را حذف کرد.

همچنین شناسه متمایزکننده B را نیز در صورت استفاده از کلید یک‌سویه، می‌توان حذف کرد.

(۱) A، TokenAB را تولید کرده و آن را برای B ارسال می‌کند.

(۲) با دریافت پیامی که شامل TokenAB است، B با بررسی تمبر زمانی یا شماره توالی و محاسبه

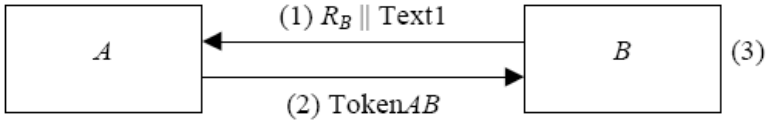
$$f_{K_{AB}}(\overset{T_A}{N_A} \| B \| Text1)$$

و مقایسه نتیجه با مقدارمقابله رمزنگاری نشانه، درستی‌یا نادرستی TokenAB را بررسی کرده و بدین ترتیب، صحیح بودن شناسه متمایزکننده B، در صورت وجود، و تمبر زمانی یا شماره توالی را مورد بررسی قرار می-دهد.

۵-۱-۲ تشخیص‌هویت دو مرحله‌ای[1]

در این مکانیزم تشخیص‌هویت، هویت نهادمدعی A از طریق نهادتاییدکننده B که آغاز کننده فرایند است، بررسی می‌شود. یکتا بودن / بهنگام بودن با تولید و بررسی یک عدد تصادفی R_B کنترل می‌شود (به پیوست ب از استاندارد ISO/IEC 9798-1 رجوع کنید).

مکانیزم تشخیص‌هویت در شکل ۲ نمایش داده شده است.



شکل ۲- تشخیص هویت دو مرحله‌ای

قالب نشانه (TokenAB) که توسط نهادمدعی A به نهادتاییدکننده B ارسال می‌شود، به صورت زیر است:

$$TokenAB = Text3 \| f_{K_{AB}}(R_B \| B \| Text2)$$

1- Two pass authentication

گنجاندن شناسه متمایزکننده B در TokenAB اختیاری است.

یادآوری – شناسه متمایز کننده B در TokenAB گنجانده می‌شود تا از نوعی حمله که اصطلاحا حمله بازتابی نامیده می‌شود، جلوگیری شود. در این حمله مهاجم با بازگرداندن چالش R_B به B، وانمود می‌کند که A است. گنجاندن شناسه متمایز کننده B اختیاری قرار داده شده است تا در محیط هایی که امکان چنین حمله هایی وجود ندارد، بتوان شناسه متمایز کننده B را حذف کرد.

همچنین شناسه متمایزکننده B را نیز در صورت استفاده از کلید یک‌سویه، می توان حذف کرد.

(۱) B یک عدد تصادفی R_B را تولید کرده و آن را، بصورت اختیاری، به همراه یک قسمت متنی Text1، برای A ارسال می‌کند.

(۲) A، TokenAB را تولید کرده و آن را برای B ارسال می‌کند.

(۳) با دریافت پیامی که شامل TokenAB است، B با محاسبه

$$f_{K_{AB}}(R_B \| B \| Text2)$$

و مقایسه نتیجه با مقدارمقابله رمزنگاری نشانه، درستی‌یا نادرستی TokenAB را بررسی کرده و بدین‌ترتیب، صحیح بودن شناسه متمایزکننده B (در صورت وجود) و اینکه از عدد تصادفی R_B (که در گام (۱) به A فرستاده شده است) برای ساختن TokenAB استفاده شده است، را مورد بررسی قرار می‌دهد.

۵-۲ تشخیص‌هویت دوطرفه

تشخیص‌هویت دوطرفه به این معنی است که هر دو نهاد برقرار کننده ارتباط، با استفاده از مکانیزم توسط یکدیگر هویت سنجی می شوند.

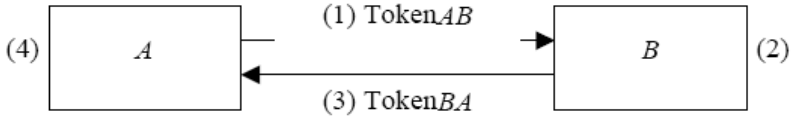
دو مکانیزم تشریح شده در بندهای ۵-۱-۱ و ۵-۱-۲، به ترتیب در بندهای ۵-۲-۱ و ۵-۲-۲ برای دستیابی به تشخیص‌هویت دوطرفه تطبیق داده شده‌اند. این کار، در هر دو حالت نیازمند یک‌مرحله اضافی است که به دو گام بیشتر، منجر می‌شود.

یادآوری – با دو بار اجرای مکانیزم تشریح شده در بند ۵-۱-۲ که یکی توسط نهاد A و دیگری توسط نهاد B آغاز می‌شود، یک مکانیزم سوم برای تشخیص‌هویت دوطرفه ساخته می‌شود.

۵-۲-۱ تشخیص‌هویت دو مرحله‌ای

در این مکانیزم تشخیص‌هویت، یکتا بودن / بهنگام بودن با تولید و بررسی تمبرهای زمانی یا شماره‌های توالی کنترل می‌شود (به پیوست ب از استاندارد ISO/IEC 9798-1 رجوع کنید).

مکانیزم تشخیص‌هویت در شکل ۳ نمایش داده شده است.



شکل ۳- تشخیص هویت دومرحله‌ای

قالب نشانه (TokenAB) که توسط A برای B ارسال می‌شود، مشابه با قالبی است که در بند ۵-۱-۱ مشخص شده است.

$$TokenAB = \overset{T_A}{\underset{N_A}{\|}} Text2 \| f_{K_{AB}}(\overset{T_A}{\underset{N_A}{\|}} B \| Text1)$$

قالب نشانه (TokenBA) که توسط B برای A ارسال می‌شود، بصورت زیر است:

$$TokenBA = \overset{T_B}{\underset{N_B}{\|}} Text4 \| f_{K_{AB}}(\overset{T_B}{\underset{N_B}{\|}} A \| Text3)$$

وجود شناسه متمایزکننده B در TokenAB و شناسه متمایزکننده A در TokenBA (بصورت مستقل از هم) اختیاری است.

یادآوری ۱ – شناسه متمایز کننده B در TokenAB گنجانده می‌شود تا از استفاده مجدد از TokenAB برای نهاد A توسط دشمنی که خود را به عنوان نهاد B معرفی می کند، جلوگیری شود. بنا به دلایل مشابه، شناسه متمایز کننده A در TokenBA وجود دارد. گنجاندن این شناسه‌های متمایز کننده اختیاری قرار داده شده است تا در محیط هایی که امکان چنین حمله هایی وجود ندارد، بتوان یک یا هر دو شناسه متمایز کننده را حذف کرد.

شناسه‌های متمایزکننده A و B را نیز در صورت استفاده از کلیدهای یک‌سویه (بخش زیر را ببینید)، می‌توان حذف کرد.

در این مکانیزم، انتخاب استفاده از تمبر زمانی یا شماره توالی به قابلیت‌های نهادمدعی و نهادتاییدکننده اعتبار و همچنین به محیط اجرا وابسته است.

گام های (۱) و (۲) از این بند، با گام‌های (۱) و (۲) از بند ۵-۱-۱ تشخیص‌هویت یک‌مرحله‌ای، یکسان هستند.

(۳) B، TokenBA را تولید کرده و آن را برای A ارسال می‌کند.

(۴) پیام گام (۳) با روشی مشابه با گام (۲) از بند ۵-۱-۱ مورد ارزیابی قرار می گیرد.

یادآوری ۲ – در این مکانیزم، دو پیام به هیچ وجه - بجز تلویحا از نظر بهنگام بودن - با یکدیگر ارتباط ندارند؛ مکانیزم شامل دو بار استفاده مستقل از مکانیزم بند ۵-۱-۱ است. ایجاد ارتباط بیشتر بین این دو پیام از طریق بکار گیری مناسب قسمت های متنی، امکان‌پذیر است (به پیوست الف رجوع کنید).

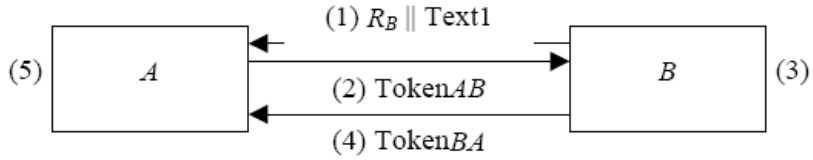
اگر از کلیدهای یک‌سویه استفاده شود آنگاه کلید K_{AB} در TokenBA با کلید یک‌سویه K_{BA} جایگزین شده و در گام (۴) از کلید مناسب استفاده می‌شود.

۵-۲-۲ تشخیص‌هویت سه مرحله‌ای[1]

در این مکانیزم تشخیص‌هویت، یکتا بودن / بهنگام بودن با تولید و بررسی اعداد تصادفی کنترل می‌شود (به پیوست ب از استاندارد ISO/IEC 9798-1 رجوع کنید).

مکانیزم تشخیص‌هویت در شکل ۴ نمایش داده شده است.

1- Three pass authentication



شکل ۴- تشخیص هویت سه مرحله‌ای

نشانه‌ها دارای قالب‌های زیر هستند:

$$TokenAB = R_A \| Text3 \| f_{K_{AB}}(R_A \| R_B \| B \| Text2)$$
$$TokenBA = Text5 \| f_{K_{AB}}(R_B \| R_A \| Text4)$$

گنجاندن شناسه متمایزکننده B در TokenAB اختیاری است.

یادآوری – در صورت وجود، شناسه متمایز کننده B در TokenAB گنجانده می‌شود تا از نوعی حمله که حمله بازتابی نامیده می‌شود، جلوگیری شود. در این حمله مهاجم با بازگرداندن چالش R_B به B، وانمود می‌کند که A است. گنجاندن شناسه متمایز کننده B اختیاری قرار داده شده است تا در محیط هایی که امکان چنین حمله هایی وجود ندارد، بتوان آن را حذف کرد.

همچنین شناسه متمایزکننده B را نیز در صورت استفاده از کلیدهای یک‌سویه (بخش زیر را ببینید)، می‌توان حذف کرد.

(۱) B یک عدد تصادفی R_B را تولید کرده و آن را، بصورت اختیاری، به همراه یک قسمت متنی Text1، برای A ارسال می‌کند.

(۲) A یک عدد تصادفی R_A و TokenAB را تولید کرده و برای B ارسال می‌کند.

(۳) با دریافت پیامی که شامل TokenAB است، B با محاسبه

$$f_{K_{AB}}(R_A \| R_B \| B \| Text2)$$

و مقایسه نتیجه با مقدارمقابله رمزنگاری نشانه، درستی یا نادرستی TokenAB را بررسی کرده و بدین‌ترتیب، صحیح بودن شناسه متمایزکننده B (در صورت وجود) و اینکه از عدد تصادفی R_B (که در گام (۱) به A فرستاده شده است) برای ساختن TokenAB استفاده شده است، را مورد بررسی قرار می‌دهد.

(۴) B ، TokenBA را تولید کرده و آن را برای A ارسال می‌کند.

(۵) با دریافت پیامی که شامل TokenBA است، A با محاسبه

$$f_{K_{AB}}(R_B \| R_A \| Text4)$$

و مقایسه نتیجه با مقدارمقابله رمزنگاری نشانه، درستی یا نادرستی TokenBA را بررسی کرده و بدین‌ترتیب، صحیح بودن شناسه متمایزکننده B (در صورت وجود) و اینکه از عدد تصادفی R_B (که در گام (۱) از B دریافت شده است) برای ساختن TokenBA استفاده شده است و اینکه از عدد تصادفی R_A (که در گام (۲) به B فرستاده شده است) برای ساختن TokenBA استفاده شده است، را مورد بررسی قرار می‌دهد.

اگر از کلیدهای یک‌سویه استفاده شود، آنگاه کلید K_{AB} در TokenBA با کلید یک‌سویه K_{BA} جایگزین شده و در گام (۵) از کلید مناسب استفاده می‌شود.

پیوست الف
(اطلاعاتی)
استفاده از قسمت های متنی

نشانه های مشخص شده در بند ۵ این قسمت از مجموعه استاندارد ملی ایران به شماره ۱۰۸۲۵، شامل قسمت های متنی هستند. کاربرد واقعی و ارتباط بین قسمت های متنی مختلف در هر مرحله به زمینه کاربرد بستگی دارد.

برای مثال، با گنجاندن اطلاعات در یک قسمت متنی مناسب، مثلا Text1 در Token*AB* در بند ۵-۱-۱، می‌توان از این اطلاعات در محاسبه مقدارمقابله رمزنگاری استفاده کرد. به این ترتیب، برای این اطلاعات می‌توان تشخیص‌هویت منبع داده‌ها را فراهم کرد.

برای مثال‌های بیشتر درباره استفاده از قسمت های متنی، به پیوست الف از استاندارد ISO/IEC 9798-1 رجوع کنید.