INSO

17253-2

1st. Edition

2015

جمهوری اسلامی ایران

Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standards Organization

استاندارد ملی ایران

۱۷۲۵۳-۲

چاپ اول

۱۳۹۳

فناوری اطلاعات- فنون امنیتی- اصالت‌سنجی هستار ناشناس قسمت ۲: سازوکارهایی بر اساس امضاهایی که از یک کلید عمومی گروهی استفاده می‌کنند

Information technology — Security techniques — Anonymous entity authentication :Part 2 Mechanisms Based on Signatures using A group public key

ICS: 35.040

به 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- اصالت‌سنجی هستار ناشناس- قسمت ۲: سازوکارهایی بر اساس امضاهایی که از یک کلید عمومی گروهی استفاده می‌کنند»

رئیس:	**سمت و/یا نمایندگی**
قسمتی، سیمین (فوق لیسانس مهندسی فناوری اطلاعات)	مشاور مرکز آپا تربیت مدرس
دبیر:	
یزدیان ورجانی، علی (دکتری، برق)	عضو هیات علمی دانشگاه تربیت مدرس و مسئول مرکز آپا تربیت مدرس
اعضا: (اسامی به ترتیب حروف الفبا)	
اسدی‌پویا، سمیرا (فوق لیسانس مهندسی فناوری اطلاعات)	مدیر عامل شرکت مهندسی پویا دانش و کیفیت آوا
شیخ‌الاسلامی، محمد کاظم (دکتری، برق)	عضو هیات علمی دانشگاه تربیت مدرس
شیرازی، مریم (لیسانس فناوری اطلاعات)	کارشناس پژوهشگاه استاندارد سازمان ملی استاندارد ایران
صادقی، مریم (لیسانس مهندسی کامپیوتر، نرم‌افزار)	کارشناس سازمان نظام صنفی رایانه‌ای کشور
سعیدی، عذرا (فوق لیسانس مهندسی مخابرات)	کارشناس سازمان فناوری اطلاعات ایران
فرهاد شیخ احمد، لیلا (فوق لیسانس مهندسی کامپیوتر، نرم‌افزار)	کارشناس استاندارد سازمان ملی استاندارد ایران
محمدیان، مصطفی (دکتری، برق)	عضو هیات علمی و معاون پژوهشی دانشکده برق و کامپیوتر
معروف، سینا (لیسانس مهندسی کامپیوتر، سخت‌افزار)	کارشناس سازمان فناوری اطلاعات ایران

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد «فناوری اطلاعات- فنون امنیتی- اصالت‌سنجی هستار ناشناس- قسمت ۲: سازوکارهایی بر اساس امضاهایی که از یک کلید عمومی گروهی استفاده می‌کنند» که پیش‌نویس آن در کمیسیون‌های مربوط توسط مرکز آپا دانشگاه تربیت مدرس تهیه و تدوین شده است و در سیصد و شصتمین اجلاس کمیته ملی استاندارد فناوری اطلاعات مورخ ۹۳/۱۲/۶ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه 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 زمینه 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 تجدید نظر استانداردهای ملی استفاده کرد.

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

ISO/IEC 20009-2:2013, Information technology — Security techniques — Anonymous entity authentication — Part 2: Mechanisms Based on Signatures using a group public key

فناوری اطلاعات- فنون امنیتی- اصالت‌سنجی هستار ناشناس- قسمت ۲:

سازوکارهایی بر اساس امضاهایی که از یک کلید عمومی گروهی استفاده می‌کنند

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین سازوکارهای اصالت‌سنجی هستار ناشناس بر اساس امضاهایی است که از یک کلید عمومی گروهی استفاده می‌کنند و در آن تصدیق‌کننده، به منظور اصالت‌سنجی هستاری که با آن در ارتباط است، طرح امضای گروهی را بدون دانستن هویت این هستار تصدیق می‌کند.

این استاندارد ملی موارد زیر را ارائه می‌کند:

- توصیف کلی سازوکار اصالت‌سنجی هستار ناشناس بر اساس امضاهایی که از کلید عمومی گروهی استفاده می‌کنند؛
- انواع مختلف سازوکارهایی از این نوع.

این استاندارد ملی موارد زیر را توصیف می‌کند:

- فرآیندهای صدور عضویت گروهی؛
- سازوکارهای اصالت‌سنجی ناشناس بدون طرف سوم مورد اعتماد برخط (TTP)[1]؛
- سازوکارهای اصالت‌سنجی ناشناس که TTP برخط را در برمی‌گیرند.

علاوه بر این، این استاندارد موارد زیر را نیز مشخص می‌کند:

- فرایند باز بودن[2] عضویت گروهی (اختیاری)؛
- فرآیند پیونددادن امضای گروهی (اختیاری).

۲ مراجع الزامی

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

در صورتی که به مدرکی با ذکر تاریخ انتشار آن ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی نمی‌باشد و در غیر این صورت همواره تاریخ تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

2-1 ISO/IEC 20008-1, Information technology — Security techniques — Anonymous digital signatures — Part 1: General

2-2 ISO/IEC 20008-2, Information technology — Security techniques — Anonymous digital signature — Part 2 :Mechanisms using a group public key

1 - Trusted Third Party

2 - opening

2-3 ISO/IEC 20009-1, Information technology — Security techniques — Anonymous entity authentication — Part 1: General

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف ارائه‌شده در استانداردهای ISO/IEC 20008-1 وISO/IEC 20009-1 و اصطلاحات زیر به کار می‌رود:

۱-۳

خصوصیت- انقیاد[1]

خصوصیتی که تضمین انقیاد بین پیام‌های هستار ارتباطی را فراهم می‌کند.

۲-۳

مرجع صدور گواهی

هستار مورد اعتماد برای ایجاد و تخصیص گواهی‌های کلید عمومی است.

[منبع: استاندارد ملی ایران شماره ۱-۱۰۸۲۲: سال ۱۳۹۲]

۳-۳

جفت کلید موقت

جفت کلید نامتقارن شامل کلید عمومی موقت و کلید خصوصی موقت است که به عنوان کلید موقت استفاده می‌شود و برای هر اجرای طرح رمزنگاری، منحصر به فرد است.

۴-۳

گواهی کلید عمومی گروهی

اطلاعات کلید عمومی گروهیِ یک گروه که توسط مرجع صدور گواهی کلید عمومی گروهی امضا شده است.

۵-۳

مرجع صدور گواهی کلید عمومی گروهی

هستار مورد اعتماد برای ایجاد و تخصیص گواهی‌های کلید عمومی گروهی است.

۶-۳

اطلاعات کلید عمومی گروهی

اطلاعات حاوی دست کم شناسانه[2] گروه و کلید عمومی گروهی است، اما می‌تواند شامل سایر اطلاعات ایستا با توجه به مرجع صدور گواهی کلید عمومی گروهی، گروه، محدودیت‌های استفاده کلید، مدت اعتبار یا الگوریتم‌های به کار رفته، باشد.

۷-۳

تابع اشتقاق کلید

تابعی که یک یا چند مورد مخفی اشتراک گذاشته‌شده را به عنوان خروجی می‌دهد تا کلیدها را به عنوان موارد مخفی به اشتراک گذاشته شده و سایر پارامترهای شناخته‌شده متقابل را به عنوان ورودی استفاده کند.

1 - Binding-property
2 - Identifier

[منبع: استاندارد ISO/IEC 11770-3:2008]

۸-۳

قابلیت پیونددادن محلی[1]

قابلیت پیونددادن با ویژگی که دو یا چند امضا از یک کاربر ناشناس تنها توسط پیونددهنده امضای گروهی خاص با کلید پیونددهنده، پیوند داده شود، اما هستارهای دیگر نتوانند امضا را پیوند دهند.

۹-۳

کد اصالت‌سنجی پیام (MAC)[2]

رشته‌ای از بیت‌ها که خروجی الگوریتم MAC است.

[منبع: استاندارد ملی ایران شماره ۱-۹۷۹۷: سال ۱۳۹۰]

۱۰-۳

الگوریتم کد اصالت‌سنجی پیام (MAC)

الگوریتمی برای محاسبه تابعی که رشته‌های بیت‌ها و کلید مخفی را به رشته‌های بیت‌هایی با طول ثابت نگاشت می‌کند که دو خصوصیت زیر را دارد:

- برای هر کلید و هر رشته ورودی، تابع به طور کارآمد قابل محاسبه است.
- برای هر کلید ثابت و در حالی که هیچ دانش قبلی از کلید، داده نشده است، محاسبه مقدار تابع در هر رشته ورودی جدید از نظر محاسباتی غیرعملی است، حتی اگر دانش مجموعه رشته‌های ورودی و مقادیر تابع متناظر نیز داده شود که مقدار i امین رشته ورودی ممکن است پس از مشاهده مقدار اولین مقادیر تابع i-1 انتخاب شده باشد، باز هم از نظر محاسباتی غیرعملی خواهد بود.

[منبع: استاندارد ملی ایران شماره ۱-۹۷۹۷: سال ۱۳۹۰]

۱۱-۳

گواهی کلید عمومی

اطلاعات کلید عمومی هستار که توسط مرجع صدور گواهی امضاشده است.

[منبع: استاندارد ملی ایران شماره ۱-۱۰۸۲۲: سال ۱۳۹۲]

۱۲-۳

اطلاعات کلید عمومی

اطلاعاتی حاوی دست کم شناسانه تمایز هستار و کلید عمومی است، اما می‌تواند شامل سایر اطلاعات ایستا در مورد مرجع صدور گواهی، هستار، محدودیت‌ها در استفاده کلید، مدت اعتبار، یا الگوریتم‌های به کار رفته باشد.

[منبع: استاندارد ملی ایران شماره ۱-۱۰۸۲۲: سال ۱۳۹۲]

1 - local linking capability
2 - Message authentication code

۴ نمادها و اصطلاحات کوته‌نوشت

در این استاندارد، نمادها و کوته‌نوشت‌های زیر به کار می‌رود.

A، B	شناسانه تمایز هستار A یا B
$Cert_A$، $Cert_B$	گواهی کلید عمومی هستار A یا B
$Cert_G$	گواهی کلید عمومی گروهی، گروه G
G، G'	شناسانه تمایز گروهی G یا G'
$\boldsymbol{G}$	گروه دوری[1] q ترتیبی که مسئله تصمیمی دیفی- هلمن (DDH)[2] آن دشوار است
g	تولیدکننده $\boldsymbol{G}$
$gsS_{XG}(m)$	امضای ناشناس که از کلید عمومی گروهی ایجادشده توسط هستار X استفاده می‌کند که یکی از سازوکارهای امضای گروهی مشخص‌شده در استاندارد ISO/IEC 20008-2 در پیامی که باید m را با استفاده از کلید امضای عضو گروه S_{XG} امضا کند، به کار می‌گیرد.
kdf	تابع اشتقاق کلید
I_G	هویت G گروهی که G یا $Cert_G$ است
I_X	هویت هستار X که X یا $Cert_X$ است
m	پیامی که باید امضا شود
MAC	کد اصالت‌سنجی پیام
MAC	مقدار خروجی الگوریتم MAC
$mac_K(M)$	الگوریتمMAC با استفاده از کلید مخفی K و رشته داده دلخواه M
N_X	عدد دنباله‌ای صادرشده توسط هستار X
P_A، P_B	کلید عمومی هستار A یا B
P_G	کلید عمومی گروهی گروه G
q	عدد اول
Res_A، Res_B	نتیجه تصدیق کلید عمومی یا گواهی کلید عمومی هستار A یا B
Res_G	نتیجه تصدیق کلید عمومی گروهی یا گواهی کلید عمومی گروهی برای گروه G
R_X	عدد تصادفی صادرشده توسط هستار X
S_{XG}	کلید امضا عضو گروه مرتبط با هستار X که در آن هستار X عضو گروه G است
$sS_X(m)$	امضای دیجیتال ایجادشده توسط هستار X در پیام m که از کلید امضای خصوصی هستار X استفاده می‌کند
TP	شناسانه تمایز TTP
TTP	طرف سوم مورد اعتماد
T_X	مهر زمانی صادرشده توسط هستار X

1 - Cyclic group
2 - Decisional Diffie-Hellmann problem

Z_q مجموعه‌ای از اعداد صحیح بین $[0, q-1]$

$||$ $Y \| Z$ به این معنی است که نتیجه الحاق اقلام داده Y و Z به ترتیب مشخص شده استفاده می‌شود. در مواردی که نتیجه الحاق دو یا چند قلم داده به عنوان بخشی از یکی از سازوکارهای مشخص‌شده در این استاندارد، ورودی به یک تابع است، این نتیجه باید به گونه‌ای ترکیب شود که بتواند به صورت منحصر به فرد به رشته داده‌های تشکیل‌دهنده آن تفکیک شود، تا هیچ امکان ابهامی در تفسیر وجود نداشته باشد. این خصوصیت آخر می‌تواند در انواع روش‌های مختلف، بسته به نوع کاربرد به دست آید. به طور مثال، می‌تواند با موارد ذیل تضمین شود (الف) تثبیت طول هر یک از زیر رشته‌ها در دامنه استفاده از سازوکار یا (ب) کدگذاری دنباله‌ای رشته‌های الحاقی با استفاده از روشی که کدگشایی منحصر به فرد را تضمین می‌کند، به طور مثال استفاده از قواعد کدگذاری متمایز که در ISO/IEC 8825-1 تعریف‌شده است. [1]

اقلام داده‌ای که اختیاری هستند در کروشه نشان داده شده است.

۵ مدل عمومی و الزامات

این بند، مدل عمومی و الزامات سازوکارهای اصالت‌سنجی ناشناس مشخص‌شده در این استاندارد ملی را مشخص می‌کند.

سازوکار اصالت‌سنجی هستار ناشناس بر اساس امضاهایی که از کلید عمومی گروهی استفاده می‌کنند، مجموعه‌ای از اعضای گروه را در برمی‌گیرد. هر گروه باید یک صادرکننده عضویت گروه مرتبط داشته باشد. در صورتی که لازم باشد اجازه بازشدن امضای گروهی که در طول پروتکل اصالت‌سنجی برای آشکارکردن مدعی ایجادشده داده شود، گروه ممکن است بازکننده گروه[1] نیز داشته باشد. همچنین اگر لازم باشد دو امضا گروهی که توسط مدعی مشابه برای اصالت‌سنجی تولید شده، پیوند داده شوند، گروه ممکن است یک پیونددهنده داشته باشد. میزان ناشناس ماندن سازوکار بستگی به تعداد اعضای گروه دارد. سازوکار اصالت‌سنجی هستار ناشناس با ویژگی فرآیندهای زیر تعریف می‌شود.

- فرایند تولید کلید.
- فرآیند اصالت‌سنجی هستار ناشناس.
- فرآیند بازکردن (در صورتی که سازوکار از بازکردن پشتیبانی کند).
- فرایند پیونددادن (اگر سازوکار از پیونددادن پشتیبانی کند).

همان طور که در زیر تعریف شده است، انواع مختلفی از هستارها می‌توانند در سازوکارهای مشخص‌شده در این استاندارد ملی در برگرفته شود. در حالی که برخی از آنها در تمام سازوکارها در برگرفته می‌شوند، سایر هستارهای دیگر تنها در برخی سازوکارها شرکت می‌کنند. در این استاندارد ملی، اگر سازوکار از بازکردن یا

1 - Group Opener

پیونددادن پشتیبانی کند، عملیات فرآیندهای مرتبط از طرح امضای گروهی در حال استفاده، همان طور که در ISO/IEC 20008-2 مشخص‌شده، پیروی می‌کند.

- **مدعی**[1]: هستاری که باید در مسیری که هویت مدعی آشکار نشود، اصالت‌سنجی شود. در این استاندارد، مدعی نقش امضاکننده در طرح‌های امضای گروهی را ایفا می‌کند که در استاندارد ISO/IEC 20008-2 مشخص شده است.

یادآوری- در برخی سازوکارها، نقش مدعی بین چندین هستار تقسیم می‌شود. به طور مثال، سازوکارهای گواهی ناشناس مستقیم (DAA)[2]، مدعی اصلی با قابلیت محاسباتی و ذخیره‌سازی محدود، به طور مثال پودمان بستر مورداعتماد (TPM)[3]، و مدعی دستیار (کمکی)[4] با قدرت محاسباتی بیشتر اما تحمل امنیتی کمتر، به طور مثال بستر رایانه معمولی (میزبانی در که TPM تعبیه شده است) را در برمی‌گیرد.

- **تصدیق‌کننده**[5]: هستاری که صحت مدعی را تصدیق می‌کند و هویت مدعی را یاد نمی‌گیرد.

- **صادرکننده**: هستاری که گواهی عضویت گروهی را برای مدعی صادر می‌کند. این هستار در تمام سازوکارهای مشخص‌شده در استاندارد ISO/IEC 20008-2 وجود دارد.

- **بازکننده**: هستاری که قادر به تعیین مدعی است که امضای گروهی که در طول پروتکل اصالت‌سنجی ایجاد شده است را تولید می‌کند. این هستار در برخی سازوکارهای مشخص‌شده در ISO/IEC 20008-2 وجود دارد. در برخی سازوکارها، صادرکننده عضویت گروهی و بازکننده عضویت گروهی، هستار مشابهی است.

- **پیونددهنده**: هستاری که قادر است تعیین کند دو امضای گروهی تولیدشده به منظور اصالت‌سنجی توسط مدعی مشابه ایجاد شده است. این هستار در برخی سازوکارهای مشخص‌شده در استاندارد ISO/IEC 20008-2 وجود دارد. در برخی سازوکارها، پیونددهنده، تصدیق‌کننده نیز می‌باشد. تعداد پیونددهنده‌ها در سازوکار اصالت‌سنجی هستار ناشناس ثابت نیست.

لازم است هر هستار شامل‌شده در سازوکار اصالت‌سنجی هستار ناشناس از مجموعه مشترک پارامترهای عمومی گروهی که برای محاسبه انواع توابع در سازوکار استفاده می‌شود، آگاه باشد.

۲۴ سازوکار اصالت‌سنجی که در این استاندارد ملی مشخص شده است برای استفاده‌های زیر در نظر گرفته شده است. اگر TTP برخط، مورد نیاز یا در دسترس نیست، سازوکار بند ۷ باید استفاده شود. از ۱۶ سازوکار بند ۷، سازوکارهای ۱-۸، خصوصیت انقیاد ندارند، در حالی که سازوکارهای ۹-۱۶ این خصوصیت را دارند. اگر سازوکار استفاده‌کننده از TTP برخط مورد نیاز و در دسترس است، سازوکار بند ۸ باید استفاده شود. هر دو بند ۷ و ۸ سازوکارهایی را مشخص می‌کند که اصالت‌سنجی ناشناس یک سویه، اصالت‌سنجی ناشناس متقابل و اصالت‌سنجی متقابل ناشناس یک سویه را ارائه می‌دهد و گزینه‌هایی با تعداد عبورهای مختلف را پیشنهاد می‌دهد.

---

1 - Claimant
2 - Direct Anonymous Attestation
3 - Trusted platform module
4 - Assistant
5 - Verifier

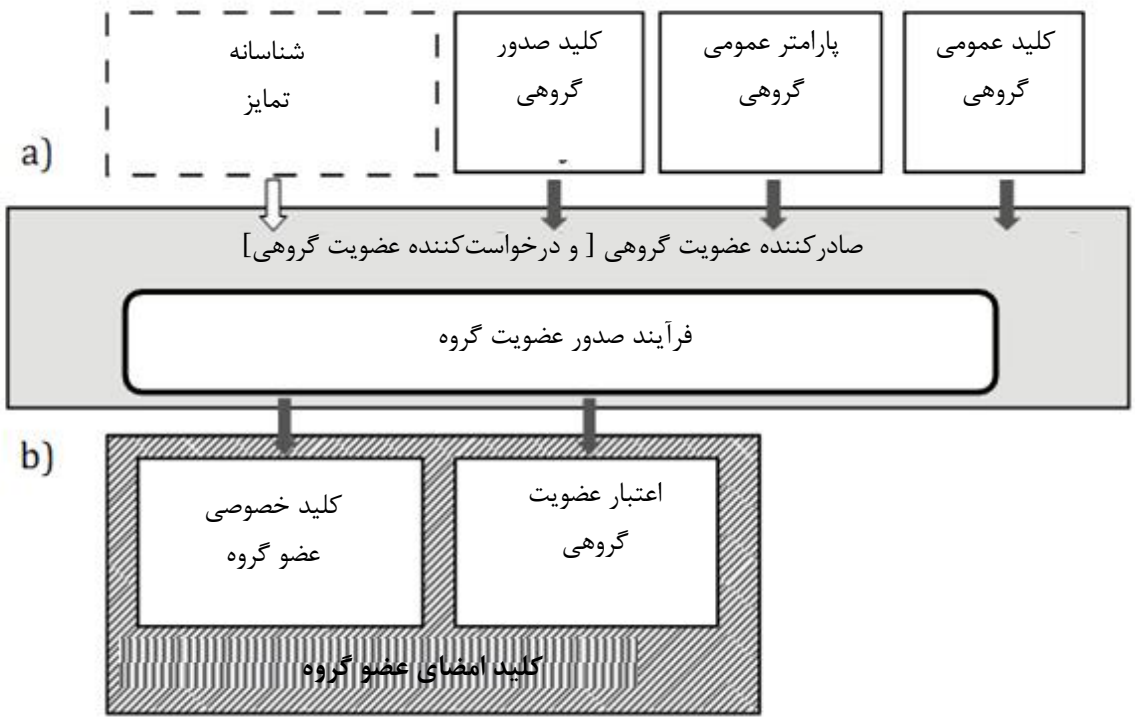
فرآیند ابطال برای ابطال کاربر و وارسی این آیا کاربر ابطال شده است یا خیر، استفاده می‌شود. جزئیات فرآیند به طرح امضای دیجیتال ناشناس استفاده‌شده در ایجاد نشان[1] برای اصالت‌سنجی ناشناس بستگی دارد. مدل کلی برای فرآیند ابطال در ISO/IEC 20008-1 مشخص شده است و فرآیندهای عملیاتی طرح امضای ناشناس منفرد با استفاده از کلید عمومی گروهی در استاندارد ISO/IEC 20008-2 مشخص شده است.

۶ فرآیند تولید کلید

فرآیند تولید کلید شامل الگوریتم‌های تولید کلید است که کلید صدور عضویت گروهی، کلید باز کردن عضویت گروهی و کلید(های) پیونددادن امضای گروه را در صورت نیاز در سازوکار، ایجاد می‌کنند. جزئیات الگوریتم‌های تولید کلید خارج از دامنه کاربرد این استاندارد است.

فرآیند تولید کلید همچنین شامل فرایند صدور عضویت گروهی است. فرآیند صدور عضویت گروهی بین عضو گروه و صادرکننده کار می‌کند و شامل ایجاد کلید امضای عضو گروه است.

برای پیشگیری از مشاهده اعتبار عضویت گروهی توسط شنودگر[2] و برای اطمینان از این که اعتبار عضویت گروهی فقط به عضو گروه قانونی ارائه شده است، به یک کانال امن و با اصالت بین عضو گروه (به عنوان مدعی) و صادرکننده نیاز است. این استاندارد مشخص نمی‌کند صادرکننده گروهی چگونه عضو گروه را اصالت‌سنجی می‌کند.



شکل ۱ – فرایند صدور عضویت گروهی

1 - Token
2 - Eavesdropper

تولید کلید همان طور که در شکل ۱ نشان داده شده و در زیر توضیح داده شده است می‌تواند به مراحل a) و b) تقسیم شود.

a) صادرکننده عضویت گروهی، کلید صدور گروهی، کلید عمومی گروهی، پارامتر عمومی گروهی و به صورت اختیاری شناسانه تمایز به عنوان ورودی را می‌گیرد. در این مرحله، صادرکننده عضویت گروهی ممکن است با عضو گروه همکاری کند.

b) فرایند صدور عضویت گروه، کلید امضای عضو گروه را به عنوان خروجی می‌دهد.

۷ سازوکارهای بدون TTP برخط

۷-۱ مقدمه

بند ۷، سازوکارهای اصالت‌سنجی هستار ناشناس بدون TTP برخط را مشخص می‌کند. سازوکارهای مشخص‌شده در بند ۷ از گواهی کلید عمومی گروهی یا برخی ابزارهای دیگر برای فعال کردن اعتبار کلید عمومی گروهی که باید تصدیق شود، استفاده می‌کند. گسترش‌های این سازوکارها برای پوشش فرآیندهای بازکردن و پیونددادن به ترتیب در بندهای ۹ و ۱۰ مشخص شده است.

سازوکارهای اصالت‌سنجی هستار مشخص‌شده از پارامترهای نوع زمان[1] مانند مهرهای زمانی[2]، اعداد دنباله‌ای یا اعداد تصادفی استفاده می‌کنند (به پیوست ب استاندارد ملی ایران شماره ۱-۱۰۸۲۵: سال ۱۳۹۱ و یادآوری ۱ زیر آن مراجعه شود).

در این استاندارد ملی، نشان‌ها گاهی اوقات به شکل زیر است:

$$Token = X_1 \,||\, X_2 \,||\, \dots \,||\, X_i \,||\, gsS_{XG}(Y_1 \,||\, Y_2 \,||\, \dots \,||\, Y_j)$$

در اصالت‌سنجی متقابل ناشناس یک سویه، امضای دیجیتالی (رقمی) $sS_X(Y_1 \,||\, Y_2 \,||\, \dots \,||\, Y_j)$ می‌تواند جایگزین امضای گروهی $gsS_{XG}\ (Y_1 \,||\, Y_2 \,||\, \dots \,||\, Y_J)$ شود.

در هر دو اصالت‌سنجی ناشناس متقابل با خصوصیت انقیاد و اصالت‌سنجی متقابل ناشناس یک سویه با خصوصیت انقیاد، MAC نیز می‌تواند الحاق شود یا MAC می‌تواند برای امضای گروهی $gsS_{XG}\ (Y_1 \,||\, Y_2 \,||\, \dots \,||\, Y_J)$ جایگزین شود.

در این استاندارد ملی، اصطلاح «پیامی که باید امضا شود»[3] به رشته $''Y_1 \,||\, Y_2 \,||\, \dots \,||\, Y_j''$ اشاره دارد که به عنوان ورودی به طرح امضای گروهی استفاده می‌شود و «پیام» به رشته $''X_1 \,||\, X_2 \,/\!/\, \dots \,||\, X_i''$ اشاره دارد. قسمت‌های ضروری $X_1 \,||\, X_2 \,||\, \dots \,||\, X_i$ و $Y_1 \,||\, Y_2 \,||\, \dots \,||\, Y_j$ باید یکسان باشد. قسمت‌های دیگر ممکن است بسته به طرح‌های امضای گروهی و برنامه‌های کاربردی خاص متفاوت باشد.

اگر اطلاعات موجود در پیامی از نشان که باید امضا شود بتواند از امضای گروه بازیابی شود، نیاز به شامل شدن آن در پیام نشان نیست.

---

1 - Time Varient
2 - Time Stamps
3 - The message-to-be-signed

اگر اطلاعات موجود در فیلد متنی پیامی از نشان که باید امضا شود نتواند از امضای گروهی بازیابی شود، نشان باید آن در فیلد متنی امضانشده نشان شامل شود.
اگر اطلاعات موجود در پیامی از نشان که باید امضا شود که توسط مدعی به تصدیق‌کننده فرستاده شده در حال حاضر برای تصدیق‌کننده شناخته شده باشد (به طور مثال عدد تصادفی)، نیاز به شامل شدن آن در پیام نشان نیست.
همه فیلدهای متنی مشخص‌شده در سازوکارهای مشخص‌شده در این استاندارد ملی برای استفاده در برنامه‌های کاربردی، خارج از دامنه کاربرد این استاندارد ملی (ممکن است خالی باشد) در دسترس است. رابطه و محتویات آنها به کاربرد خاص بستگی دارد. برای اطلاعات در مورد استفاده از فیلدهای متنی به پیوست الف استاندارد ملی ایران شماره ۳-۱۰۸۲۵: سال ۱۳۹۱ مراجعه شود.

یادآوری ۱- هستار اول می‌تواند با شامل کردن عدد تصادفی خود در بلوک داده‌ای که امضا می‌کند، مسائل امنیتی مرتبط با امضا توسط یک هستار بلوک داده که توسط هستار دوم برای برخی انگیزه‌های نهان دستکاری شده است را کاهش دهد. در این مورد، غیر قابل پیش‌بینی بودن عدد تصادفی از امضای داده کاملا از پیش تعریف‌شده، پیشگیری می‌کند.

یادآوری ۲- از آنجا که توزیع گواهی‌های کلید عمومی گروهی خارج از دامنه کاربرد این استاندارد است، ارسال گواهی‌های کلید عمومی گروهی در تمام سازوکارها اختیاری است، به جز سازوکارهایی که در TTP برخط مشخص‌شده در بند ۸ شامل شده است.

بند ۷-۲ سازوکارهای اصالت‌سنجی ناشناس یک طرفه‌ای را ارائه می‌دهد که یک هستار را با تضمین قانونی بودن هستار دیگر فراهم می‌کند، اما نه بالعکس. بند ۷-۳ سازوکارهای اصالت‌سنجی ناشناس متقابلی را ارائه می‌دهد که هر دو هستار را با تضمین از قانونی بودن هستار دیگر فراهم می‌کند. بند ۷-۴ سازوکارهای اصالت‌سنجی متقابل ناشناس یک سویه‌ای را ارائه می‌دهد که اصالت‌سنجی هستار ناشناس را در یک جهت و اصالت‌سنجی هستار را در جهت دیگر فراهم می‌کند.
پروتکل‌های اصالت‌سنجی سه مرحله‌ای و اصالت‌سنجی موازی دو مرحله‌ای در بندهای ۷-۳ و ۷-۴ ممکن است به مفهوم حمله انقیاد نادرست[1] باشد (به شماره [۱۱] کتابنامه مراجعه شود). هنگامی که چالش و پیام‌های نشان با هم مرتبط نیستند، ارسال پیام چالش برای یک هستار و ارسال پیام نشان برای هستار دیگر در همان گروه امکان‌پذیر است. اطلاعات بیشتر در مورد حمله انقیاد نادرست و خصوصیت انقیاد در پیوست ب ارائه شده است.
برای کاهش حمله انقیاد نادرست، بند ۷-۵ و ۷-۶، هشت سازوکار با خصوصیت انقیاد برای هر دو پروتکل اصالت‌سنجی سه مرحله‌ای و دو مرحله‌ای موازی ارائه می‌دهد.

1 - Misbinding attack

۷-۲ اصالت‌سنجی ناشناس یک سویه

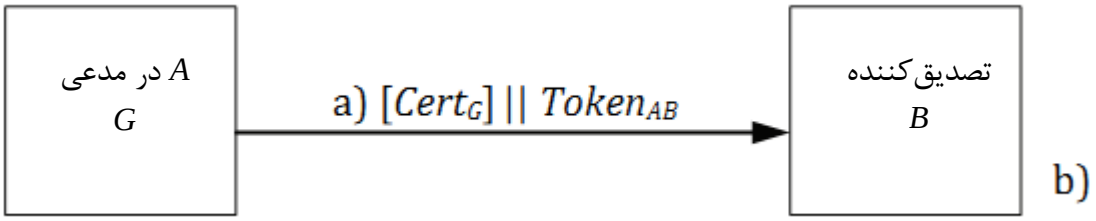
۷-۲-۱ کلیات

اصالت‌سنجی ناشناس یک سویه بدان معنی است که تنها یکی از دو هستار، مدعی (هستار A در گروه G)، با استفاده از سازوکار، اصالت‌سنجی می‌شود و هویت هستار اصالت‌سنجی‌شده برای هستار دیگر، تصدیق‌کننده (هستار B) ناشناس است.

۷-۲-۲ سازوکار ۱ - اصالت‌سنجی ناشناس یک سویه یک مرحله‌ای

در این سازوکار، هستار A در گروه G، پروتکل اصالت‌سنجی با هستار B را شروع می‌کند و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی مهر زمانی یا عدد دنباله‌ای کنترل می‌شود (به پیوست ب استاندارد ملی ایران شماره ۱-۱۰۸۲۵: سال ۱۳۹۱ مراجعه شود).

سازوکار اصالت‌سنجی در شکل ۲ نشان داده شده است.



شکل ۲ - اصالت‌سنجی ناشناس یک سویه یک مرحله‌ای

فرم نشان ($Token_{AB}$) که توسط مدعی A به تصدیق‌کننده B ارسال می‌شود عبارت است از:

$$Token_{AB} = T_A \text{ or } N_A \mid\mid B \mid\mid [Text_2] \mid\mid gsS_{AG}(T_A \text{ or } N_A \mid\mid B \mid\mid [Text_1])$$

مدعی A از مهر زمانی T_A یا عدد دنباله‌ای N_A به عنوان پارامتر نوع زمان استفاده می‌کند. انتخاب به قابلیت‌های فنی مدعی و تصدیق‌کننده و همچنین محیط بستگی دارد. امضای gsS_{AG}، امضای گروهی ایجادشده با استفاده از یکی از سازوکارهای امضای گروهی مشخص‌شده در ISO/IEC 20008-2 است. $Cert_G$ گواهی کلید عمومی گروهی برای کلید عمومی گروهی گروه G است.

یادآوری ۱- گنجاندن شناسانه B در پیامی از $Token_{AB}$ که باید امضا شود برای پیشگیری از پذیرش نشان توسط هر موردی به غیر از تصدیق‌کننده مورد نظر، لازم است.

یادآوری ۲- به طور کلی، $Text_2$ با این فرآیند تصدیق نمی‌شود.

یادآوری ۳- یکی از کاربردهای این سازوکار می‌تواند توزیع کلید باشد (به پیوست الف استاندارد ملی ایران شماره ۱-۱۰۸۲۵: سال ۱۳۹۱ مراجعه شود).

سازوکار آن به صورت زیر انجام می‌شود:

a) A، $Token_{AB}$ و به صورت اختیاری $Cert_G$ را به B ارسال می‌کند.

b) در دریافت پیام حاوی $Token_{AB}$، B مراحل زیر را انجام می‌دهد:

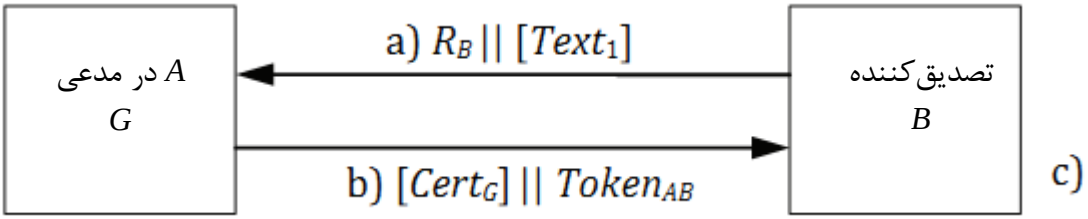
۱) با تصدیق گواهی کلید عمومی گروهی G یا با ابزارهای دیگر اطمینان حاصل می‌کند در موقعیت کلید عمومی گروهی معتبر گروه G است.

۲) $Token_{AB}$ را با تصدیق امضای گروهی A موجود در نشان، با وارسی مهر زمانی یا عدد دنباله‌ای و با وارسی این که مقدار فیلد شناسانه (B) در پیامی از $Token_{AB}$ که باید امضا شود برابر شناسانه هستار B است، تصدیق می‌کند.

۷-۲-۳ سازوکار ۲ - اصالت‌سنجی ناشناس یک سویه دو مرحله‌ای

در این سازوکار، هستار A در G توسط هستار B که فرآیند را شروع می‌کند، اصالت‌سنجی می‌شود و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی عدد تصادفی R_B کنترل می‌شود (به پیوست ب استاندارد ملی ایران شماره ۱-۱۰۸۲۵ سال: ۱۳۹۱ مراجعه شود)

سازوکار اصالت‌سنجی در شکل ۳ نشان داده شده است.



شکل ۳ - اصالت‌سنجی ناشناس یک سویه دو مرحله‌ای

فرم نشان ($Token_{AB}$) که توسط مدعی A به تصدیق‌کننده B ارسال می‌شود، عبارت است از:

$Token_{AB} = R_A \,||\, R_B \,||\, [B] \,||\, [Text_3] \,||\, gsS_{AG}\,(R_A \,||\, R_B \,||\, [B] \,||\, [Text_2])$

گنجاندن شناسانه B در $Token_{AB}$ اختیاری است. این مورد به محیطی که این سازوکار اصالت‌سنجی در آن استفاده می‌شود بستگی دارد.

یادآوری ۱- گنجاندن شناسانه اختیاری B در پیامی از $Token_{AB}$ که باید امضا شود می‌تواند از پذیرش نشان توسط هر موردی به غیر از تصدیق‌کننده مورد نظر پیشگیری کند (به طور مثال ممکن است در حمله فرد-در-میانه[1] رخ دهد).

یادآوری ۲- گنجاندن عدد تصادفی R_A در قسمت امضاشده $Token_{AB}$، از دستیابی B به امضای گروهی A در داده‌های انتخاب‌شده توسط B قبل از شروع سازوکار اصالت‌سنجی پیشگیری می‌کند. به طور مثال، این سنجه ممکن است زمانی که کلید عمومی گروهی مشابه توسط A برای مقاصدی غیر از اصالت‌سنجی هستار یا با عضو گروه دیگر استفاده می‌شود، مورد نیاز باشد.

سازوکار به صورت زیر انجام می‌شود:

a) B، عدد تصادفی R_B و به صورت اختیاری فیلد متنی $Text_1$ را به A ارسال می‌کند.

b) A، $Token_{AB}$ و به صورت اختیاری $Cert_G$ را به B ارسال می‌کند.

c) در دریافت پیام حاوی $Token_{AB}$، B مراحل زیر را انجام می‌دهد:

1- man-in-the-middle attack

۱) با تصدیق گواهی کلید عمومی گروهی G یا با ابزارهای دیگر اطمینان حاصل می‌کند در موقعیت کلید عمومی گروهی معتبر G است.

۲) $Token_{AB}$ را با وارسی امضای گروهی A موجود در نشان، با وارسی این که عدد تصادفی R_B ارسال‌شده به A در مرحله a) با عدد تصادفی موجود در پیامی از $Token_{AB}$ که باید امضا شود در توافق است و با وارسی این که مقدار فیلد شناسانه (B) در پیامی از $Token_{AB}$ که باید امضا شود، در صورت وجود، برابر با شناسانه B است، تصدیق می‌کند.

۷-۳ اصالت‌سنجی ناشناس متقابل

۷-۳-۱ کلیات

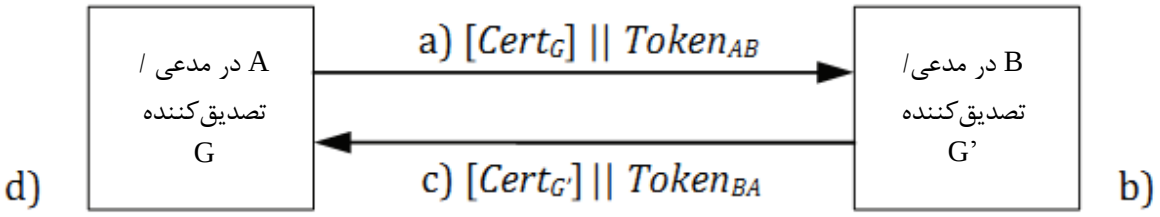
اصالت‌سنجی ناشناس متقابل بدان معنی است که دو هستار ارتباطی برای همدیگر اصالت‌سنجی شده‌اند و هویت‌های دو هستار برای یکدیگر ناشناس است.

دو سازوکار شرح‌داده‌شده در بندهای ۷-۲-۲ و ۷-۲-۳ به ترتیب، در ۷-۳-۲ و ۷-۳-۳ برای رسیدن به اصالت‌سنجی متقابل به صورت مبسوط توضیح داده شده است. این با انتقال یک پیام افزوده به دست می‌آید. سازوکار مشخص‌شده در بند ۷-۳-۴ از چهار مرحله استفاده می‌کند که با این حال، لازم نیست همه آن‌ها به صورت دنباله‌ای ارسال شود. در نتیجه کاهش زمان صرف‌شده برای انجام فرآیند اصالت‌سنجی امکان‌پذیر است.

۷-۳-۲ سازوکار ۳ - اصالت‌سنجی ناشناس متقابل دو مرحله‌ای

در این سازوکار، هستار A در گروه G، پروتکل اصالت‌سنجی با هستار B در گروه G’ را شروع می‌کند و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی مهرهای زمانی یا اعداد دنباله‌ای کنترل می‌شود (به پیوست ب استاندارد ملی ایران شماره ۱-۱۰۸۲۵ سال: ۱۳۹۱ مراجعه شود). هستار A، هویت گروه G' را می‌شناسد.

سازوکار اصالت‌سنجی در شکل ۴ نشان داده شده است.



شکل ۴ - اصالت‌سنجی ناشناس متقابل دو مرحله‌ای

فرم نشان ($Token_{AB}$) که توسط A به B ارسال می‌شود عبارت است از:

$$Token_{AB} = T_A \text{ or } N_A \,||\, G' \,||\, [Text_2] \,||\, gsS_{AG}(T_A \text{ or } N_A \,||\, G' \,||\, [Text_1])$$

فرم نشان ($Token_{AB}$) که توسط B به A ارسال می‌شود عبارت است از:

$$Token_{BA} = T_B \text{ or } N_B \,||\, G \,||\, [Text_4] \,||\, gsS_{BG'}(T_A \text{ or } N_A \,||\, G \,||\, [Text_3])$$

انتخاب استفاده از مهرهای زمانی یا اعداد دنباله‌ای در این سازوکار به قابلیت‌های فنی مدعی و تصدیق‌کننده و همچنین محیط بستگی دارد.

یادآوری ۱- گنجاندن شناسانه G و G' به ترتیب در پیامی از $Token_{BA}$ و $Token_{AB}$ که باید امضا شود، برای پیشگیری از پذیرش نشان‌ها توسط موردی غیر از عضو گروه مورد نظر لازم است.

سازوکار به صورت زیر انجام می‌شود:

a) A، $Token_{AB}$ و به صورت اختیاری $Cert_G$ را به B ارسال می‌کند.

b) در دریافت پیام حاوی $Token_{AB}$، B مراحل زیر را انجام می‌دهد:

۱) با تصدیق گواهی کلید عمومی گروهی G یا با ابزارهای دیگر اطمینان حاصل می‌کند در موقعیت کلید عمومی گروهی معتبر گروه G است.

۲) $Token_{AB}$ را با تصدیق امضای گروهی A موجود در نشان، با وارسی مهر زمانی یا عدد دنباله‌ای، و با وارسی این که مقدار فیلد شناسانه (G') در پیامی از $Token_{AB}$ که باید امضا شود برابر هویت G' است، تصدیق می‌کند.

c) B، $Token_{BA}$ و به صورت اختیاری، $Cert_{G'}$ را به A ارسال می‌کند.

d) در دریافت پیام حاوی $Token_{BA}$، A مراحل زیر را انجام می‌دهد:

۱) با تصدیق گواهی کلید عمومی گروهی G' یا با ابزارهای دیگر اطمینان حاصل می‌کند در موقعیت کلید عمومی گروهی معتبر گروه G' است.

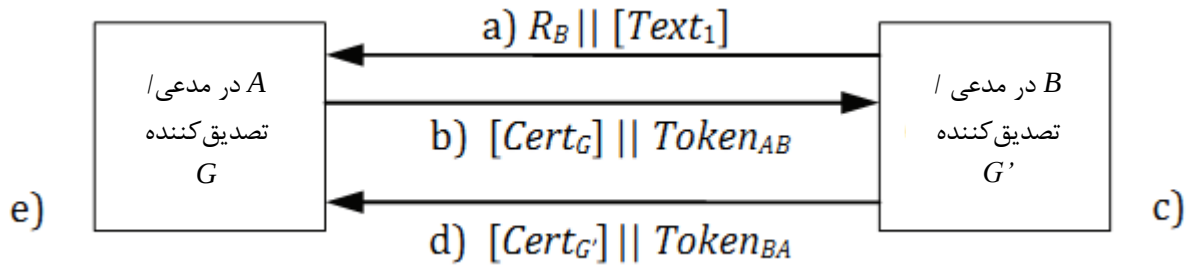
۲) $Token_{BA}$ را با تصدیق امضای گروهی B موجود در نشان، با وارسی مهر زمانی یا عدد دنباله‌ای و با وارسی که این که مقدار فیلد شناسانه (G) در پیامی از $Token_{BA}$ که باید امضا شود برابر هویت G است، درستی سنجی می‌کند.

یادآوری ۲- دو پیام این سازوکار به هیچ وجه با هم مرتبط نمی‌شوند مگر با به‌هنگام بودن ضمنی. سازوکار شامل دو استفاده مستقل از نسخه اصلاح‌شده سازوکار مشخص‌شده در بند ۷-۲-۲ است. انقیاد بیشتر این پیام‌ها می‌تواند با استفاده مناسب از فیلدهای متنی به دست آید.

۷-۳-۳ سازوکار ۴ - اصالت‌سنجی ناشناس متقابل سه مرحله‌ای

در این سازوکار، هستار B در G' پروتکل اصالت‌سنجی با هستار A در G را شروع می‌کند و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی اعداد تصادفی کنترل می‌شود (به پیوست ب استاندارد ملی ایران شماره ۱-۱۰۸۲۵ سال: ۱۳۹۱ مراجعه شود).

سازوکار اصالت‌سنجی در شکل ۵ نشان داده شده است.



شکل ۵ - اصالت‌سنجی ناشناس متقابل سه مرحله‌ای

نشان‌ها به شکل زیر است:

$Token_{AB} = R_A \,||\, R_B \,||\, [G'] \,||\, [Text_3] \,||\, gsS_{AG}\,(R_A \,||\, R_B \,||\, [G'] \,||\, [Text_2])$
$Token_{BA} = R_B \,||\, R_A \,||\, [G] \,||\, [Text_5] \,||\, gsS_{BG'}\,(R_B \,||\, R_A \,||\, [G] \,||\, [Text_4])$

یادآوری ۱- گنجاندن عدد تصادفی RA در پیامی از $Token_{AB}$ که باید امضا شود از دستیابی B به امضای گروهی A در داده‌های انتخاب‌شده توسط B قبل از شروع سازوکار اصالت‌سنجی پیشگیری می‌کند. این سنجه ممکن است برای مثال، زمانی لازم باشد که کلید عمومی گروهی مشابه توسط A برای مقاصدی غیر از اصالت‌سنجی هستار استفاده شده باشد یا توسط اعضای دیگر گروه G استفاده شده باشد. با این حال، گنجاندن R_B در $Token_{BA}$، به دلایل امنیتی که تعیین می‌کند که A باید وارسی کند که همان مقدار ارسال‌شده در اولین پیام را دارد، ممکن است حفاظتی مشابه با B ارائه ندهد، با این که R_B قبل از انتخاب R_A برای A شناخته می‌شود. اگر این نوع حفاظت مورد نیاز باشد، B می‌تواند عدد تصادفی افزوده R'_B را در فیلدهای متنی $Text_4$ و $Text_5$ $Token_{BA}$ وارد کند.

یادآوری ۲- گنجاندن شناسانه G' در $Token_{AB}$ و شناسانه G در $Token_{BA}$ اختیاری است. نیاز به گنجاندن این شناسانه‌ها به محیطی که در آن این سازوکار اصالت‌سنجی استفاده می‌شود بستگی دارد.

سازوکار به صورت زیر انجام می‌شود:

a) B، عدد تصادفی R_B و به صورت اختیاری فیلد متنی $Text_1$ را به A ارسال می‌کند.

b) A، $Token_{AB}$ و به صورت اختیاری $Cert_G$را به B ارسال می‌کند.

c) در دریافت پیام حاوی $Token_{AB}$، B مراحل زیر را انجام می‌دهد:

۱) با تصدیق گواهی کلید عمومی گروهی G یا با ابزارهای دیگر اطمینان حاصل می‌کند در موقعیت کلید عمومی گروهی معتبر G است.

۲) $Token_{AB}$ را با وارسی امضای گروهی A موجود در نشان، با وارسی این که عدد تصادفی R_B، به A ارسال‌شده در مرحله *a*) در توافق با عدد تصادفی موجود در پیامی از $Token_{AB}$ که باید امضا شود است و با وارسی این که مقدار فیلد شناسانه (G') در پیامی از $Token_{AB}$ که باید امضا شود، در صورت وجود، برابر با هویت G' است، تصدیق می‌کند.

d) B، $Token_{BA}$ و به صورت اختیاری، $CertG'$ را به A ارسال می‌کند.

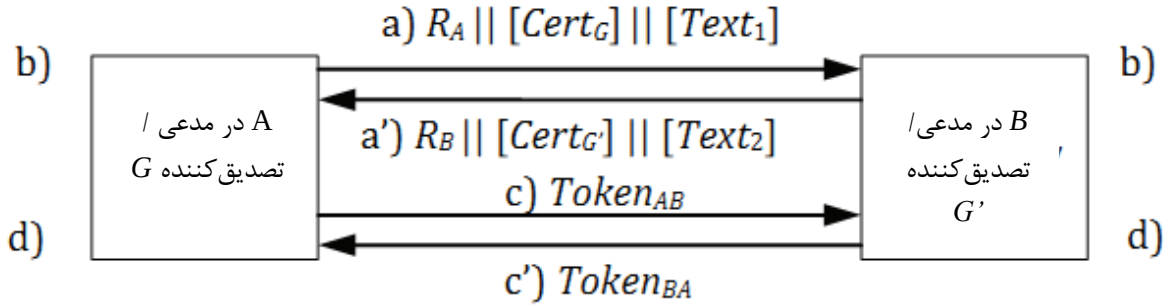
e) در دریافت پیام حاوی $Token_{BA}$، A به طور مشابه مراحل ۱) و ۲) فهرست‌شده در *c*) را انجام می‌دهد. علاوه بر این، A وارسی می‌کند که عدد تصادفی R_B موجود در پیامی از $Token_{BA}$ که باید امضا شود برابر با

عدد تصادفی R_B دریافت‌شده در مرحله a) است و آن عدد تصادفی R_A موجود در پیامی از $Token_{BA}$ که باید امضا شود برابر با عدد تصادفی R_A ارسال‌شده در مرحله b) است.

۷-۳-۴ سازوکار ۵ - اصالت‌سنجی ناشناس متقابل موازی دو مرحله‌ای

در این سازوکار، اصالت‌سنجی ناشناس به صورت موازی با هستار A در G و هستار B در G' انجام می‌شود و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی اعداد تصادفی کنترل می‌شود (به پیوست ب استاندارد ملی ایران شماره ۱-۱۰۸۲۵ سال: ۱۳۹۱ مراجعه شود).

سازوکار اصالت‌سنجی در شکل ۶ نشان داده شده است.



شکل ۶ - اصالت‌سنجی ناشناس متقابل موازی دو مرحله‌ای

نشان‌ها مشابه بند ۷-۳-۳ هستند:

$Token_{AB} = R_A \,||\, R_B \,||\, [G] \,||\, [Text_4] \,||\, gsS_{AG}\,(R_A \,||\, R_B \,||\, [G] \,||\, [Text_3])$
$Token_{BA} = R_B \,||\, R_A \,||\, [G] \,||\, [Text_6] \,||\, gsS_{BG}\,(R_B \,||\, R_A \,||\, [G] \,||\, [Text_5])$

گنجاندن شناسانه G' در $Token_{AB}$ و شناسانه G در $Token_{BA}$ اختیاری است. نیاز به گنجاندن این شناسانه‌ها به محیطی که این سازوکار اصالت‌سنجی در آن استفاده می‌شود، بستگی دارد.

یادآوری ۱- عدد تصادفی R_A در $Token_{AB}$ وجود دارد تا از دستیابی B به امضای گروهی A در داده‌های انتخاب‌شده توسط B قبل از شروع سازوکار اصالت‌سنجی پیشگیری کند. این پیشگیری ممکن است، به طور مثال، زمانی که کلید امضای گروهی مشابه توسط A برای مقاصدی علاوه بر اصالت‌سنجی هستار استفاده می‌شود یا با عضو دیگری از این گروه استفاده می‌شود، لازم باشد. به دلایل مشابه عدد تصادفی R_B در $Token_{BA}$ وجود دارد.

بسته به زمان نسبی دریافت پیام‌های ارسال‌شده در مراحل a) و a')، یکی از طرف‌ها ممکن است عدد تصادفی طرف دیگر را در هنگام انتخاب عدد تصادفی خود بداند. اگر این موضوع نامطلوب باشد، هر دو طرف می‌توانند به ترتیب عدد تصادفی افزوده R'_A و R'_B را در فیلدهای متنی $Text_3$ و $Text_4$، $Token_{AB}$ و $Text_5$ و $Token_{BA}$، $Text_6$ وارد کنند.

سازوکار به صورت زیر انجام می‌شود:

a) A، R_A و به صورت اختیاری $Cert_G$ و فیلد متنی $Text_1$ را به B ارسال می‌کند.

a') B، R_B و به صورت اختیاری $Cert_{G'}$ و فیلد متنی $Text_2$ را به A ارسال می‌کند.

b) A و B که با تصدیق گواهی کلید عمومی گروهی یا با ابزارهای دیگر اطمینان حاصل می‌کنند در موقعیت کلید عمومی گروهی معتبری هستند که هستار دیگر متعلق به آن است.

c) A، $Token_{AB}$ را به B ارسال می‌کند.

c') B، $Token_{BA}$ به A ارسال می‌کند.

d) A و B مراحل زیر را انجام می‌دهند: هر کدام از آنها نشان دریافت‌شده را با وارسی امضای گروهی موجود در نشان و با وارسی این که عدد تصادفی که قبلا به هستار دیگر ارسال شده، در توافق با عدد تصادفی موجود در پیامی از نشان دریافت‌شده‌ای که باید امضا شود است، تصدیق می‌کنند.

یادآوری ۲- اجرای سازوکار ۷-۲-۳ دو بار در هر دو جهت، جایگزین سازوکار ۷-۳-۴ است. گنجاندن گواهی‌های کلید عمومی گروهی در اولین پیام سازوکار ۷-۳-۴ اجازه تصدیق گواهی‌های کلید عمومی گروهی زودتر را می‌دهد، که ممکن است به فرآیند اصالت‌سنجی سرعت بخشد.

یادآوری ۳- دو پیام این سازوکار به هیچ وجه با هم مرتبط نمی‌شود مگر با به‌هنگام بودن ضمنی.

۷-۴ اصالت‌سنجی متقابل ناشناس یک سویه

۷-۴-۱ کلیات

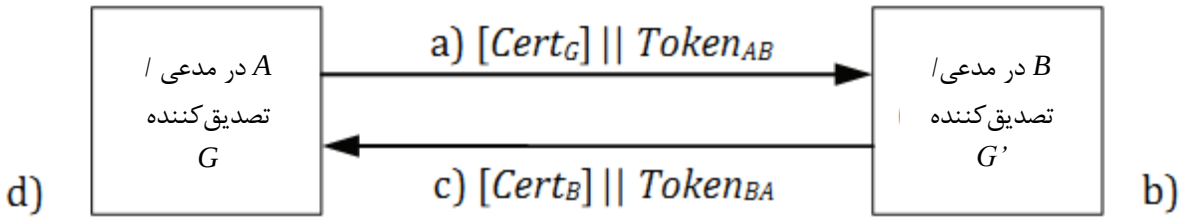
اصالت‌سنجی متقابل ناشناس یک سویه بدان معنی است که دو هستار ارتباطی برای یکدیگر اصالت‌سنجی شده‌اند و هویت یک هستار برای هستار دیگر ناشناس است.

در سازوکارها، هستار A در گروه G به صورت ناشناس توسط هستار B با استفاده از یکی از طرح‌های امضای گروهی مشخص‌شده در استاندارد ISO/IEC 20008-2 اصالت‌سنجی می‌شود. هستار B توسط هستار A با استفاده از یکی از طرح‌های امضای دیجیتال (رقمی) مشخص‌شده در استاندارد ISO/IEC 14888 یا ISO/IEC 9796 اصالت‌سنجی می‌شود.

۷-۴-۲ سازوکار ۶ – اصالت‌سنجی متقابل ناشناس یک سویه دو مرحله‌ای

در این سازوکار، هستار A در G پروتکل اصالت‌سنجی با هستار B را شروع می‌کند و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی مهرهای زمانی یا اعداد دنباله‌ای کنترل می‌شود (به پیوست ب استاندارد ملی ایران شماره ۱-۱۰۸۲۵ سال: ۱۳۹۱ مراجعه شود).

سازوکار اصالت‌سنجی در شکل ۷ نشان داده شده است.



شکل ۷- اصالت‌سنجی متقابل ناشناس یک سویه دو مرحله‌ای

فرم نشان ($Token_{AB}$) که توسط A در G به B ارسال می‌شود:

$Token_{AB} = T_A \text{ or } N_A \,||\, B \,||\, [Text_2] \,||\, gsS_{AG}(T_A \text{ or } N_A \,||\, B \,||\, [Text_1])$

فرم نشان ($Token_{BA}$) که توسط B به A ارسال می‌شود:

$Token_{BA} = T_B \text{ or } N_B \,||\, G \,||\, [Text_4] \,||\, sSB(T_A \text{ or } N_A \,||\, G \,||\, [Text_3])$

انتخاب استفاده از مهرهای زمانی یا اعداد دنباله‌ای در این سازوکار به قابلیت‌های فنی اثبات‌کننده و تصدیق و همچنین محیط بستگی دارد.

یادآوری ۱- گنجاندن شناسانه G و B به ترتیب در پیامی از $Token_{BA}$ و $Token_{AB}$ که باید امضا شود برای پیشگیری از پذیرش نشان توسط هر موردی غیر از دریافت‌کننده‌های مورد نظر لازم است.

سازوکار به صورت زیر انجام می‌شود:

a) A، $Token_{AB}$ و به صورت اختیاری $Cert_G$ را به B ارسال می‌کند.

b) در دریافت پیام حاوی $Token_{AB}$، B مراحل زیر را انجام می‌دهد:

۱) با تصدیق گواهی کلید عمومی گروهی G یا با ابزارهای دیگر اطمینان حاصل می‌کند در موقعیت کلید عمومی گروهی معتبر گروه G است.

۲) $Token_{AB}$ را با تصدیق امضای گروهی A موجود در نشان، با وارسی مهر زمانی یا عدد دنباله‌ای و با وارسی این که مقدار فیلد شناسانه (B) در پیامی از $Token_{AB}$ که باید امضا شود برابر شناسانه آن است، تصدیق می‌کند.

c) B، $Token_{BA}$ و به صورت اختیاری $Cert_B$ را به A ارسال می‌کند.

d) در دریافت پیام حاوی $Token_{BA}$، A مراحل زیر را انجام می‌دهد:

۱) با تصدیق گواهی کلید عمومی B یا با ابزارهای دیگر اطمینان حاصل می‌کند در موقعیت کلید عمومی معتبر B است.

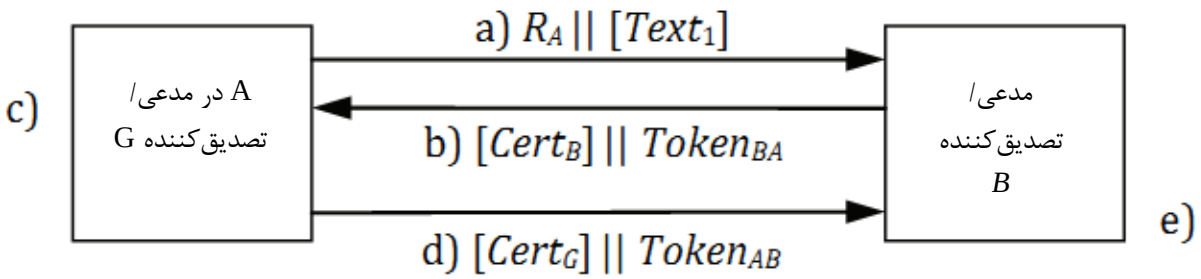
۲) $Token_{BA}$ را با تصدیق امضای B موجود در نشان، با وارسی مهر زمانی یا عدد دنباله‌ای و با وارسی این که مقدار فیلد شناسانه (G) در پیامی از $Token_{BA}$ که باید امضا شود برابر هویت G است، تصدیق می‌کند.

یادآوری ۲- دو پیام این سازوکار به هیچ وجه با هم مرتبط نمی‌شود، مگر با به‌هنگام بودن ضمنی. سازوکار شامل دو استفاده مستقل از نسخه اصلاح‌شده سازوکار مشخص‌شده در بند ۷-۲-۲ است. انقیاد بیشتر این پیام‌ها می‌تواند با استفاده مناسب از فیلدهای متنی به دست آید.

۷-۴-۳ سازوکار ۷ – اصالت‌سنجی متقابل ناشناس یک سویه سه مرحله‌ای

در این سازوکار، هستار A در G پروتکل اصالت‌سنجی با هستار B را شروع می‌کند و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی اعداد تصادفی کنترل می‌شود (به پیوست ب استاندارد ملی ایران شماره ۳-۱۰۸۲۵: سال ۱۳۹۱ مراجعه شود)

سازوکار اصالت‌سنجی در شکل ۸ نشان داده شده است



شکل ۸ - اصالت‌سنجی متقابل ناشناس یک سویه سه مرحله‌ای

نشان‌ها به شکل زیر است:

$Token_{BA} = R_B \,||\, R_A \,||\, [G] \,||\, [Text_3] \,||\, sS_B\,(R_B \,||\, R_A \,||\, [G] \,||\, [Text_2])$
$Token_{AB} = R_A \,||\, R_B \,||\, [B] \,||\, [Text_5] \,||\, gsS_{AG}\,(R_A \,||\, R_B \,||\, [B] \,||\, [Text_4])$

گنجاندن شناسانه G در $Token_{BA}$ و شناسانه B در $Token_{AB}$ اختیاری است. نیاز به گنجاندن این شناسانه‌ها به محیطی که این سازوکار اصالت‌سنجی در آن استفاده می‌شود بستگی دارد.

یادآوری- گنجاندن عدد تصادفی R_B در قسمت امضاشده $Token_{BA}$ از دستیابی به امضای B در داده‌های انتخاب‌شده توسط A قبل از شروع از سازوکار اصالت‌سنجی پیشگیری می‌کند. این سنجه ممکن است به طور مثال، زمانی که کلید عمومی مشابه توسط B برای مقاصدی غیر از اصالت‌سنجی هستار استفاده می‌شود مورد نیاز باشد. با این حال، گنجاندن R_A در $Token_{AB}$، به دلایل امنیتی لازم است که این امر تعیین می‌کند B باید وارسی کند که مشابه مقدار ارسال‌شده در اولین پیام باشد و به دلیل این که R_A قبل از انتخاب R_B برای B شناخته شده است ممکن است حفاظتی مشابه A را پیشنهاد نکند. اگر این نوع حفاظت مورد نیاز باشد، A می‌تواند R'_A عدد تصادفی افزوده را در فیلدهای متنی $Text_2$ و $Text_3$، $Token_{AB}$ وارد کند.

سازوکار آن به صورت زیر انجام می‌شود:

a) A، عدد تصادفی RA و به صورت اختیاری فیلد متنی $Text_1$ را به B ارسال می‌کند.

b) B، $Token_{BA}$ و به صورت اختیاری گواهی کلید عمومی خود را به A ارسال می‌کند.

c) در دریافت پیام حاوی $Token_{BA}$، مراحل زیر انجام می‌شود:

۱) با تصدیق گواهی کلید عمومی B یا با ابزارهای دیگر اطمینان حاصل می‌کند در موقعیت کلید عمومی معتبر B است.

۲) $Token_{BA}$ را با وارسی امضای B موجود در نشان، با وارسی این که عدد تصادفی R_A، ارسال‌شده به B در مرحله *a*) در توافق با عدد تصادفی موجود در پیامی از $Token_{BA}$ که باید امضا شود است و با وارسی این که مقدار فیلد شناسانه (G) در پیامی از $Token_{BA}$ که باید امضا شود در صورت وجود، برابر با شناسانه G است، تصدیق می‌کند.

d) A، $Token_{AB}$ و به صورت اختیاری، گواهی کلید عمومی گروهی خود را به B ارسال می‌کند.

e) در دریافت پیام حاوی $Token_{AB}$، B به طور مشابه مراحل زیر را انجام می‌دهد:

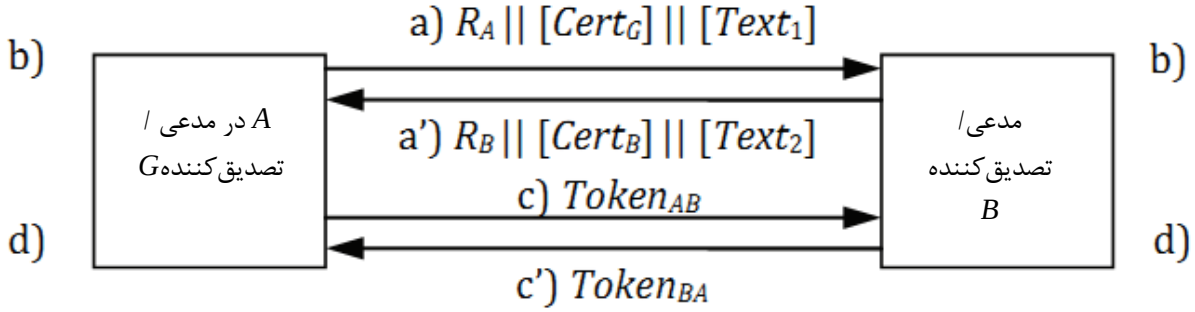
۱) با تصدیق گواهی کلید عمومی گروهی G یا با ابزارهای دیگر اطمینان حاصل می‌کند در موقعیت کلید عمومی گروهی معتبر G است.

۲) $Token_{BA}$ را با وارسی امضای A موجود در نشان، با وارسی این که عـدد تصـادفی R_A موجـود در پیامی از $Token_{BA}$ که باید امضا شود برابر عدد تصادفی R_A دریافت‌شده در مرحلـه a) اسـت و عـدد تصادفی R_B موجود در پیامی از $Token_{AB}$ که باید امضا شود برابر عدد تصـادفی R_B ارسـال‌شـده در مرحله b) است و با وارسی این که مقدار فیلد شناسانه (B) در پیامی از $Token_{AB}$ که باید امضا شود در صورت وجود، برابر با شناسانه تمایز B است، تصدیق می‌کند.

۷-۴-۴ سازوکار ۸ - اصالت‌سنجی متقابل ناشناس یک سویه موازی دو مرحله‌ای

در این سازوکار، اصالت‌سنجی ناشناس به صورت موازی با هستار A در G و هستار B انجام می‌شود و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی اعداد تصادفی کنترل می‌شود (به پیوست ب استاندارد ملـی ایـران شماره ۱-۱۰۸۲۵ سال: ۱۳۹۱ مراجعه شود).

سازوکار اصالت‌سنجی در شکل ۹ نشان داده شده است.



شکل ۹ - اصالت‌سنجی متقابل ناشناس یک سویه موازی دو مرحله‌ای

نشان‌ها به شکل زیر است:

$Token_{AB} = R_A \,||\, R_B \,||\, [B] \,||\, [Text_4] \,||\, gsS_{AG}\,(R_A \,||\, R_B \,||\, [B] \,||\, [Text_3])$
$Token_{BA} = R_B \,||\, R_A \,||\, [G] \,||\, [Text_6] \,||\, sSB(R_B \,||\, R_A \,||\, [G] \,||\, [Text_5])$

گنجاندن شناسانه B در $Token_{AB}$ و شناسانه G در $Token_{BA}$ اختیاری است. نیاز به گنجاندن این شناسانه‌هـا به محیطی که این سازوکار اصالت‌سنجی در آن استفاده می‌شود بستگی دارد.

یادآوری- عدد تصادفی R_A در $Token_{AB}$ وجود دارد تا از دستیابی B به امضای گروهی A در داده‌هـای انتخـاب‌شـده توسـط B قبل از شروع سازوکار اصالت‌سنجی، پیشگیری کند. این ویژگی ممکن است ، برای مثال، هنگامی که کلید گروهی مشابه توسط A برای مقاصدی بیشتر از اصالت‌سنجی هستار استفاده می‌شود یا توسط عضو دیگر گروه استفاده می‌شود، لازم باشد. به دلایـل مشابه عدد تصادفی R_B در $Token_{BA}$ وجود دارد. بسته به زمان نسبی دریافت پیام‌های ارسال‌شـده در مراحـل a) و a')، یکـی از طرف‌ها ممکن است عدد تصادفی طرف دیگر را در هنگام انتخاب عدد تصادفی آن بداند. اگر این موضوع نامطلوب باشد، هـر دو طرف می‌توانند عدد تصادفی افزوده $R'A$ و R'_B را در فیلـدهای متنـی $Text_3$ و $Text_4$، $Token_{AB}$، و $Text_5$ و $Text_6$، $Token_{BA}$ وارد کنند.

سازوکار به صورت زیر انجام می‌شود:

a) A، R_A و به صورت اختیاری گواهی کلید عمومی گروهی آن و فیلد متنی $Text_1$ را به B ارسال می‌کند.

a') B، R_B و به صورت اختیاری گواهی کلید عمومی آن و فیلد متنی $Text_2$ را به A ارسال می‌کند.

b) A با تصدیق گواهی کلید عمومی B یا با ابزارهای دیگر اطمینان حاصل می‌کند در موقعیت کلید عمومی معتبر B است. به طور مشابه B اطمینان حاصل می‌کند که در موقعیت کلید عمومی معتبر گروهی است که A متعلق به آن است. این کار با تصدیق گواهی کلید عمومی گروهی A یا با ابزارهای دیگر انجام می‌شود.

c) A، $Token_{AB}$ را به B ارسال می‌کند.

c') B، $Token_{BA}$ را به A ارسال می‌کند.

d) A و B نشان دریافت‌شده را با وارسی امضا یا امضای گروهی موجود در نشان و با وارسی این که عدد تصادفی که قبلا به هستار دیگر فرستاده شده، در توافق با عدد تصادفی موجود در پیامی از نشانِ دریافت‌شده که باید امضا شود، است، تصدیق می‌کند.

۷-۵ اصالت‌سنجی ناشناس متقابل با خصوصیت انقیاد

۷-۵-۱ کلیات

اصالت‌سنجی ناشناس متقابل با خصوصیت انقیاد بدان معنی است که دو هستار ارتباطی برای یکدیگر اصالت‌سنجی شده‌اند و هویت این دو هستار ناشناس در حالی که خصوصیت انقیاد تضمین شده است برای یکدیگر ناشناس است.

بند ۷-۵ جزییات مربوط به سازوکارهای متقابل اصالت‌سنجی ناشناس با خصوصیت انقیاد را ارائه می‌کند. در سازوکارها، هستار A در گروه G و هستار B در گروه G' باید یکی از طرح‌های امضای گروهی مشخص‌شده در استاندارد ISO/IEC 20008-2 را استفاده کند.

یادآوری- به صورت اختیاری، در سازوکار ۷-۵، هستارهای A و B می‌توانند کلید جلسه را از مورد مخفی به اشتراک گذاشته‌شده برای ارتباط امن آتی بین خود برگیرند. این موضوع خارج از دامنه کاربرد این استاندارد ملی است.

۷-۵-۲ سازوکار ۹ - اصالت‌سنجی ناشناس متقابل سه مرحله‌ای امضای آخر[1]

در این پروتکل اصالت‌سنجی ناشناس متقابل سه مرحله‌ای با خصوصیت انقیاد، اولین پیام، امضای گروه را شامل نمی‌شود. هستار B در G'، پروتکل اصالت‌سنجی با هستار A در G را شروع می‌کند و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی اعداد تصادفی کنترل می‌شود (به پیوست ب استاندارد ملی ایران شماره ۱-۱۰۸۲۵ سال: ۱۳۹۱ مراجعه شود). این پروتکل در شکل ۵ نشان داده شده است.

سازوکار دارای الزامات زیر است.

- قبل از استفاده از سازوکار، هستارهای A و B باید در استفاده از گروه دوری $\boldsymbol{G}$، q ترتیبی و تولیدکننده g از G، با توجه به این که کدام مسئله DDH دشوار است به توافق برسند.

اطلاعات افزوده مورد نیاز به شرح زیر است:

کلید عمومی موقت R_B، برای کلید خصوصی موقت b در Z_q، g^bاست.

کلید عمومی موقت R_A، برای کلید خصوصی موقت a در Z_q، g^aاست.

نشان‌های تبادل‌شده در سازوکار به شکل زیر است:

$$Token_{AB} = R_A \,||\, [Text_3] \,||\, gsS_{AG}\,(R_A \,||\, R_B \,||\, [Text_2]) \,||\, MAC_{AB}$$

1 - Three-pass sign-later mutual anonymous authentication

$Token_{BA} = R_B \,||\, [Text_5] \,||\, gsS_{BG'}\,(R_B \,||\, R_A \,||\, [Text_4]) \,||\, MAC_{BA}$

که در آن MAC_{AB} و MAC_{BA} به شرح زیر است:

$MAC_{AB} = mac_{MK}\,([Cert_G] \,||\, R_A \,||\, [Text3] \,||\, gsS_{AG}\,(R_A \,||\, R_B \,||\, [Text_2]))$.
$MAC_{BA} = mac_{MK}\,([Cert_{G'}] \,||\, R_B \,||\, [Text5] \,||\, gsS_{BG'}\,(R_B \,||\, R_A \,||\, [Text_4]))$.

سازوکار به صورت زیر انجام می‌شود:

a) B مراحل زیر را انجام می‌دهد:

۱) کلید خصوصی موقت b را از Z_q انتخاب می‌کند و کلید عمومی موقت $R_B = g^b$ را محاسبه می‌کند.

۲) g^b و به صورت اختیاری فیلد متنی $Text_1$ را به A ارسال می‌کند.

b) A مراحل زیر را انجام می‌دهد:

۱) کلید خصوصی موقت a را از Z_q انتخاب می‌کند و کلید عمومی موقت $R_A = g^a$ را محاسبه می‌کند.

۲) $g^{ab} = (R_B)^a$ را محاسبه می‌کند.

۳) کلید MAC $MK = kdf(g^{ab})$ را محاسبه می‌کند.

۴) $gsS_{AG}(R_A \,||\, R_B \,||\, Text_2)$ را با استفاده از کلید امضا محاسبه می‌کند.

۵) $MAC_{AB} = mac_{MK}\,([Cert_G\,] \,||\, R_A \,||\, [Text_3] \,||\, gsS_{AG}\,(R_A \,||\, R_B \,||\, [Text_2]))$ را با استفاده از کلید MAC MK محاسبه می‌کند.

۶) $Token_{AB}$ و به صورت اختیاری گواهی کلید عمومی گروهی $Cert_G$ آن را به B ارسال می‌کند.

c) در دریافت پیام حاوی $Token_{AB}$، B مراحل زیر را انجام می‌دهد:

۱) $g^{ab} = (R_A)^b$ را محاسبه می‌کند.

۲) MAC، کلید $MK = kdf(g^{ab})$ را محاسبه می‌کند.

۳) با تصدیق گواهی کلید عمومی گروهی G یا با ابزارهای دیگر اطمینان حاصل می‌کند در موقعیت کلید عمومی گروهی معتبر G است.

۴) $Token_{AB}$ را به شرح زیر تصدیق می‌کند:

أ) امضای گروهی A موجود در نشان را تصدیق می‌کند.

ب) وارسی می‌کند کلیدهای عمومی موقت R_A و R_B در امضای گروهی گنجانده شده است.

ج) وارسی می‌کند کلید عمومی موقت R_B موجود در $Token_{AB}$ برابر کلید عمومی موقت R_B ارسال‌شده در مرحله a) است.

د) مقدار MAC_{AB} را با استفاده از MK وارسی می‌کند.

۵) $gsS_{BG}\,(R_B \,||\, R_A \,||\, [Text_4])$ را با استفاده از کلید امضای آن محاسبه می‌کند.

۶) $MAC_{BA} = mac_{MK}\,([Cert_{G'}] \,||\, R_B \,||\, [Text_5] \,||\, gsS_{BG}\,(R_B \,||\, R_A \,||\, [Text_4]))$ را با استفاده از کلید MAC MK محاسبه می‌کند.

d) B، $Token_{BA}$ و به صورت اختیاری گواهی کلید عمومی گروهی $Cert_{G'}$ خود را به A ارسال می‌کند.

e) در دریافت پیام حاوی $Token_{BA}$، A مراحل زیر را انجام می‌دهد:

۱) با تصدیق گواهی کلید عمومی گروهی G' یا با ابزارهای دیگر اطمینان حاصل می‌کند در موقعیت کلید عمومی گروهی معتبر G است.

۲) تصدیق $Token_{BA}$ به شرح زیر است:

أ) امضای گروهی B موجود در نشان را تصدیق می‌کند.

ب) وارسی می‌کند کلید عمومی موقت R_B و R_A در امضای گروهی گنجانده شده است.

ج) وارسی می‌کند که کلید عمومی موقت R_B موجود در $Token_{BA}$ برابر با کلید عمومی موقت R_B دریافت‌شده در مرحله b) است.

د) وارسی می‌کند که کلید عمومی موقت R_A امضاشده در امضای گروهی $Token_{BA}$ برابر با کلید عمومی موقت R_A ارسال‌شده در مرحله b) است.

ه) مقدار MAC_{BA} را با استفاده از MK وارسی می‌کند.

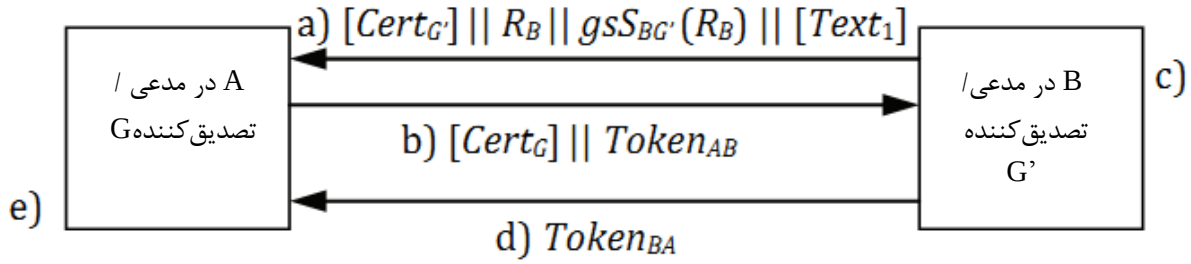
۷-۵-۳ سازوکار ۱۰ - اصالت‌سنجی ناشناس متقابل امضای اول سه مرحله‌ای

در این پروتکل اصالت‌سنجی ناشناس متقابل سه مرحله‌ای با خصوصیت انقیاد، اولین پیام، امضای گروه را شامل می‌شود. هستار B در G' پروتکل اصالت‌سنجی را با هستار A در G شروع می‌کند و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی اعداد تصادفی کنترل می‌شود (به پیوست ب استاندارد ملی ایران شماره ۱-۱۰۸۲۵ سال: ۱۳۹۱ مراجعه شود)

سازوکار دارای الزامات زیر است.

- قبل از استفاده از سازوکار، هستارهای A و B باید در استفاده گروه دوری G، q ترتیبی و تولیدکننده g از G، با توجه به این که کدام مسئله DDH دشوار است به توافق برسند.

پیام‌های پروتکل و اطلاعات افزوده مورد نیاز به شرح زیر است:



شکل ۱۰ - اصالت‌سنجی ناشناس متقابل امضای اول سه مرحله‌ای

کلید عمومی موقت R_B برای کلید خصوصی موقت b در Zq، g^b است.

کلید عمومی موقت R_A برای کلید خصوصی موقت a در Zq، g^a است.

نشان‌های تبادل‌شده در سازوکار به شکل زیر است:

$$Token_{AB} = R_A \,||\, gsS_{AG}(R_A) \,||\, MAC_{AB} \,||\, [Text_2]$$
$$Token_{BA} = MAC_{BA} \,||\, [Text_3]$$

که در آن MAC_{AB} و MAC_{BA} به شرح زیر است:

$$MAC_{AB} = mac_{MK}(R_A \,||\, gsS_{AG}(R_A) \,||\, R_B \,||\, gsS_{BG}(R_B) \,||\, [Text_4]).$$

$MAC_{BA} = mac_{MK}\ (R_B \,||\, gsS_{BG'}\ (R_B) \,||\, R_A \,||\, gsS_{AG}\ (R_A) \,||\, [Text_5])$.

سازوکار به صورت زیر انجام می‌شود:

a) B مراحل زیر را انجام می‌دهد:

۱) کلید خصوصی موقت b را از Zq انتخاب می‌کند و کلید عمومی موقت $R_B = g^b$ را محاسبه می‌کند.

۲) $gsS_{BG'}\ (R_B)$ را با استفاده از کلید امضای آن را محاسبه می‌کند.

۳) g^b، $gsS_{BG'}\ (R_B)$ و به صورت اختیاری $Cert_{G'}$ و فیلد متنی $Text_1$ را به A ارسال می‌کند.

b) A مراحل زیر انجام را می‌دهد:

۱) با تصدیق گواهی کلید عمومی گروهی G' یا با ابزارهای دیگر اطمینان حاصل می‌کند در موقعیت کلید عمومی گروهی معتبر G' است.

۲) امضای گروهی B را تصدیق می‌کند.

۳) کلید خصوصی موقت a را از Zq انتخاب می‌کند و کلید عمومی موقت $R_A = g^a$ را محاسبه می‌کند.

۴) $gsS_{AG}\ (R_A)$ را با استفاده از کلید امضای خود محاسبه می‌کند.

۵) $g^{ab} = (R_B)^a$ را محاسبه می‌کند.

۶) MAC، کلید $MK = kdf(g^{ab})$ را محاسبه می‌کند.

۷) $MAC_{AB} = mac_{MK}\ (R_A \,||\, gsS_{AG}\ (R_A) \,||\, R_B \,||\, gsS_{BG'}\ (R_B) \,||\, [Text_4])$ را با استفاده از کلید MK MAC محاسبه می‌کند.

۸) $Token_{AB}$ و به صورت اختیاری گواهی کلید عمومی گروهی $Cert_G$ آن را به B ارسال می‌کند.

c) در دریافت پیام حاوی $Token_{AB}$، B مراحل زیر را انجام می‌دهد:

۱) با تصدیق گواهی کلید عمومی گروهی G یا با ابزارهای دیگر اطمینان حاصل می‌کند در موقعیت کلید عمومی گروهی معتبر G است.

۲) امضای گروهی A را تصدیق می‌کند.

۳) $g^{ab} = (R_A)^b$ را محاسبه می‌کند.

۴) کلید MAC $MK = kdf(g^{ab})$ را محاسبه می‌کند.

۵) $MAC_{BA} = mac_{MK}\ (R_B \,||\, gsS_{BG}\ (R_B) \,||\, R_A \,||\, gsS_{AG}\ (R_A) \,||\, [Text5])$ را با استفاده از کلید MK MAC محاسبه می‌کند.

۶) مقدار MAC_{AB} را با استفاده از MK وارسی می‌کند.

d) B، $Token_{BA}$ را به A ارسال می‌کند.

e) در دریافت پیام حاوی $Token_{BA}$، A مقدار MAC_{BA} را با استفاده از MK وارسی می‌کند.

یادآوری- در سازوکار بالا، برای ارائه خصوصیت انقیاد قوی‌تر، MAC می‌تواند به امضاهای گروهی تغییر کند که از قابلیت پیونددادن کنترل کاربر، مانند DAA پشتیبانی می‌کند. خصوصیت انقیاد قوی‌تر که خصوصیت انقیاد کامل نامیده می‌شود،

تضمین می‌کند که تمام پیام‌های دریافت‌شده از مدعی مشابه می‌آید (برای اطلاعات بیشتر بـه شـماره [۱۰] کتابنامـه مراجعـه شود). این یادآوری همچنین می‌تواند به شیوه‌ای مشابه در سازوکارهای ۱۲، ۱۴ و ۱۶ استفاده شود.

۷-۵-۴ سازوکار ۱۱ - اصالت‌سنجی ناشناس متقابل امضای آخر موازی دو مرحله‌ای

در این پروتکل اصالت‌سنجی ناشناس متقابل موازی دو مرحله‌ای با خصوصیت انقیاد، اولین پیام، امضای گروه را شامل می‌شود. اصالت‌سنجی ناشناس موازی با هستار A در G و هستار B در G' انجام می‌شود و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی اعداد تصادفی کنترل می‌شود (بـه پیوسـت ب اسـتاندارد ملـی ایـران شماره ۱-۱۰۸۲۵ سال: ۱۳۹۱مراجعه شود). پروتکل در شکل ۶ نشان داده شده است.

سازوکار دارای الزامات زیر است.

- قبل از استفاده از سازوکار، هستارهای A و B باید در استفاده از گروه دوری $\boldsymbol{G}$، q ترتیبی و تولیدکننده g از G، با توجه به این که کدام مسئله DDH دشوار است به توافق برسند.

اطلاعات افزوده مورد نیاز به شرح زیر است:

کلید عمومی موقت R_B برای کلید خصوصی موقت b در Zq، g^b است.

کلید عمومی موقت R_A برای کلید خصوصی موقت a در Zq، g^a است.

نشان‌های تبادل‌شده در سازوکار به شکل زیر است:

$Token_{AB} = R_A \,||\, [Text_4] \,||\, gsS_{AG}\,(R_A \,||\, R_B \,||\, [Text_3]) \,||\, MAC_{AB}$
$Token_{BA} = R_B \,||\, [Text_6] \,||\, gsS_{BG'}\,(R_B \,||\, R_A \,||\, [Text5]) \,||\, MAC_{BA}$

که MAC_{AB} و MAC_{BA} به شرح زیر است:

$MAC_{AB} = mac_{MK}\,([Cert_G] \,||\, R_A \,||\, [Text_4] \,||\, gsS_{AG}\,(R_A \,||\, R_B \,||\, [Text_3]))$.
$MAC_{BA} = mac_{MK}\,([Cert_{G'}] \,||\, R_B \,||\, [Text_6] \,||\, gsS_{BG'}\,(R_B \,||\, R_A \,||\, [Text_5]))$.

سازوکار به صورت زیر انجام می‌شود:

a) A مراحل زیر را انجام می‌دهد:

۱) کلید خصوصی موقت a را از Zq انتخـاب مـی‌کنـد و کلیـد عمـومی موقـت $R_A = g^a$ را محاسـبه می‌کند.

۲) R_A و به صورت اختیاری $Cert_G$ و فیلد متنی $Text_1$ را به B ارسال می‌کند.

a') B مراحل زیر را انجام می‌دهد:

۱) کلید خصوصی موقت b را از Zq انتخـاب مـی‌کنـد و کلیـد عمـومی موقـت $R_B = g^b$ را محاسـبه می‌کند.

۲) R_B و به صورت اختیاری $Cert_G$ ' و فیلد متنی $Text_2$ را به A ارسال می‌کند.

b) A و B اطمینان حاصل می‌کنند که در موقعیت کلید عمومی گروه معتبر هستند که هستار دیگر متعلق به آن است این کار با تصدیق گواهی کلید عمومی گروه مرتبط یا با ابزارهای دیگر انجام می‌شود.

c) A مراحل زیر را انجام می‌دهد:

۱) $g^{ab} = (R_B)^a$ را محاسبه می‌کند.

۲) MAC، کلید $MK = kdf(g^{ab})$ را محاسبه می‌کند.

۳) $gsS_{AG}(R_A \,||\, R_B \,||\, [Text_3])$ را با استفاده از کلید امضا محاسبه می‌کند.

۴) $MAC_{AB} = mac_{MK}([Cert_G] \| R_A \| [Text_4] \| gsS_{AG}(R_A \| R_B \| [Text_3]))$ را با استفاده از کلید MAC MK محاسبه می‌کند.

۵) $Token_{AB}$ را به B ارسال می‌کند.

c') B مراحل زیر را انجام می‌دهد:

۱) $g^{ab} = (R_A)^b$ را محاسبه می‌کند.

۲) MAC، کلید $MK = kdf(g^{ab})$ را محاسبه می‌کند.

۳) $gsS_{BG'}(R_B \| R_A \| [Text_5])$ را با استفاده از کلید امضا محاسبه می‌کند.

۴) $MAC_{BA} = macMK([Cert_G'] \| R_B \| [Text_6] \| gsS_{BG'}(R_B \| R_A \| [Text_5]))$ را با استفاده از کلید MAC MK محاسبه می‌کند.

۵) $Token_{BA}$ را به A ارسال می‌کند.

d) A و B مراحل زیر را انجام می‌دهند:

۱) $Token_{AB}$ و $Token_{BA}$ را به شرح زیر تصدیق می‌کنند:

أ) امضای گروهی موجود در نشان را تصدیق می‌کنند.

ب) وارسی می‌کنند کلیدهای عمومی موقت R_A و R_B در امضاهای گروهی گنجانده شده است.

ج) A وارسی می‌کند که کلید عمومی موقت R_B موجود در $Token_{BA}$ برابر با کلید عمومی موقت R_B دریافت‌شده در مرحله a') است و R_A امضاشده در امضای گروهی $Token_{BA}$ برابر با کلید عمومی موقت R_A ارسال‌شده در مرحله a) است.

د) B وارسی می‌کند که کلید عمومی موقت R_A موجود در $Token_{AB}$ برابر با کلید عمومی موقت R_A دریافت‌شده در مرحله a) است و R_B امضاشده در امضای گروهی $Token_{AB}$ برابر با کلید عمومی موقت R_B ارسال‌شده در مرحله a') است.

ه) مقادیر MAC_{AB} و MAC_{BA} را با استفاده از MK وارسی می‌کنند.

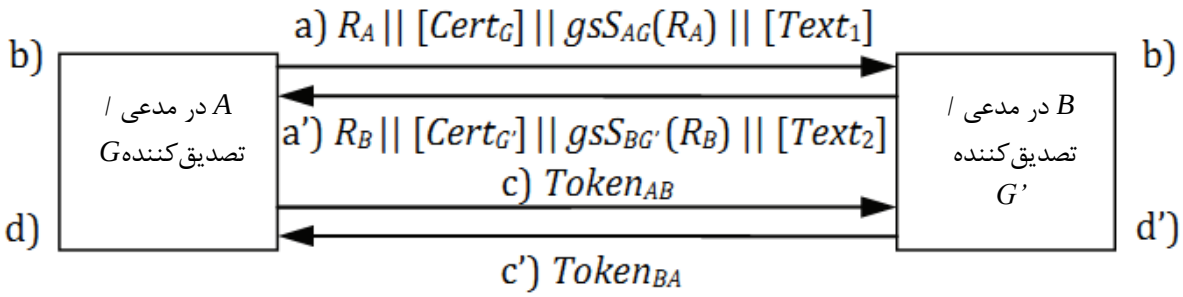
۷-۵-۵ سازوکار ۱۲ - اصالت‌سنجی ناشناس متقابل امضای اول موازی دو مرحله‌ای

در این پروتکل اصالت‌سنجی ناشناس متقابل موازی دو مرحله‌ای با خصوصیت انقیاد، اولین پیام، امضای گروه را شامل می‌شود. اصالت‌سنجی ناشناس موازی با هستار A در G و هستار B در G' انجام می‌شود و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی اعداد تصادفی کنترل می‌شود (به پیوست ب استاندارد ملی ایران شماره ۱-۱۰۸۲۵ سال: ۱۳۹۱ مراجعه شود.)

سازوکار دارای الزامات زیر است.

- قبل از استفاده از سازوکارها، هستارهای A و B باید در استفاده از گروه دوری $\boldsymbol{G}$، q ترتیبی و تولیدکننده g از G، با توجه به این که کدام مسئله DDH دشوار است به توافق برسند.

پیام‌های پروتکل و اطلاعات افزوده مورد نیاز به شرح زیر است:



شکل ۱۱ - اصالت‌سنجی ناشناس متقابل امضای اول موازی دو مرحله‌ای

کلید عمومی موقت R_B برای کلید خصوصی موقت b در Z_q، g^b است.

کلید عمومی موقت R_A برای کلید خصوصی موقت a در Z_q، g^a است.

نشان‌های تبادل‌شده در سازوکار به شکل زیر است:

$Token_{AB} = MAC_{AB} \| [Text_3]$
$Token_{BA} = MAC_{BA} \| [Text_4]$

که در آن MAC_{AB} و MAC_{BA} به شرح زیر است:

$MAC_{AB} = mac_{MK}(R_A \| gsS_{AG}(R_A) \| R_B \| gsS_{BG}(R_B) \| [Text_5])$.
$MAC_{BA} = mac_{MK}(R_B \| gsS_{BG'}(R_B) \| R_A \| gsS_{AG}(R_A) \| [Text_6])$.

سازوکار به صورت زیر انجام می‌شود:

a) A مراحل زیر را انجام می‌دهد:

۱) کلید خصوصی موقت a را از Z_q انتخاب می‌کند و کلید عمومی موقت $R_A = g^a$ را محاسبه می‌کند.

۲) $gsS_{AG}(R_A)$ را با استفاده از کلید امضا محاسبه می‌کند.

۳) g^a، $gsS_{AG}(R_A)$ و به صورت اختیاری $Cert_G$ و فیلد متنی $Text_1$ را به B ارسال می‌کند.

a') B مراحل زیر را انجام می‌دهد:

۱) کلید خصوصی موقت b را از Z_q انتخاب می‌کند و کلید عمومی موقت $R_B = g^b$ را محاسبه می‌کند.

۲) $gsS_{BG'}(R_B)$ را با استفاده از کلید امضا محاسبه می‌کند.

۳) g^b، $gsS_{BG'}(R_B)$ و به صورت اختیاری $Cert_{G'}$ و فیلد متنی $Text_2$ را به A ارسال می‌کند.

b) A و B اطمینان حاصل می‌کنند که در موقعیت کلید عمومی گروهی معتبری هستند که هستار دیگر متعلق به آن است. این کار با تصدیق گواهی کلید عمومی گروهی مرتبط یا با ابزارهای دیگر انجام می‌شود. هر یک از آنها امضای گروهی دریافت‌شده را تصدیق می‌کنند.

c) A مراحل زیر را انجام می‌دهد:

۱) $g^{ab} = (R_B)^a$ را محاسبه می‌کند.

۲) کلید MAC $MK = kdf(g^{ab})$ را محاسبه می‌کند.

۳) $MAC_{AB} = mac_{MK}(R_A \| gsS_{AG}(RA) \| R_B \| gsS_{BG'}(R_B) \| [Text_5])$ را با استفاده از کلید MAC MK محاسبه می‌کند.

۴) $Token_{AB}$ را به B ارسال می‌کند.

c') B مراحل زیر را انجام می‌دهد:

۱) $g^{ab} = (R_A)^b$ را محاسبه می‌کند.

۲) کلید MAC $MK = kdf(g^{ab})$ را محاسبه می‌کند.

۳) $MAC_{BA} = mac_{MK}(R_B \| gsS_{BG'}(R_B) \| R_A \| gsS_{AG}(R_A) \| [Text_6])$ را با استفاده از کلید MAC MK محاسبه می‌کند.

۴) $Token_{BA}$ را به A ارسال می‌کند.

d) A مراحل زیر را انجام می‌دهد:

۱) کلید عمومی موقت R_B و $gsS_{BG'}(R_B)$ در مرحله *a'*) را بازیابی می‌کند.

۲) $MAC_{BA} = mac_{MK}(R_B \| gsS_{BG'}(R_B) \| R_A \| gsS_{AG}(R_A) \| [Text_6])$ را با استفاده از کلید MAC MK محاسبه می‌کند.

۳) اعتبار MAC_{BA} در نشان مرحله *c'*) را با استفاده از مقدار محاسبه‌شده در مرحله فرعی ۲) وارسی می‌کند.

d') B مراحل زیر را انجام می‌دهد:

۱) کلید عمومی موقت R_A و $gsS_{AG}(R_A)$ را در مرحله *a*) بازیابی می‌کند.

۲) $MAC_{AB} = mac_{MK}(R_A \| gsS_{AG}(R_A) \| R_B \| gsS_{BG'}(R_B) \| [Text_5])$ را با استفاده از کلید MAC MK محاسبه می‌کند.

۳) اعتبار MAC_{AB} در نشان مرحله *c*) را با استفاده از مقدار محاسبه‌شده در مرحله فرعی ۲) وارسی می‌کند.

۷-۶ اصالت‌سنجی متقابل یک سویه ناشناس با خصوصیت انقیاد

۷-۶-۱ کلیات

اصالت‌سنجی متقابل یک سویه ناشناس با خصوصیت انقیاد بدان معنی است که دو هستار ارتباطی برای یکدیگر اصالت‌سنجی شده‌اند و هویت یک هستار برای هستار دیگر ناشناس است اما خصوصیت انقیاد تضمین شده است.

بند ۷-۶ جزییات مربوط به سازوکارهای اصالت‌سنجی متقابل ناشناس یک سویه با خصوصیت انقیاد را ارائه می‌کند. در سازوکارها، هستار A در G توسط هستار B به صورت ناشناس با استفاده از طرح‌های امضای گروهی مشخص‌شده در استاندارد *ISO/IEC 20008-2* اصالت‌سنجی می‌شود. هستار B توسط هستار A با استفاده از طرح‌های امضای دیجیتال (رقمی) مشخص‌شده در استاندارد *ISO/IEC 14888* یا *ISO/IEC 9796* اصالت‌سنجی می‌شود.

یادآوری- به صورت اختیاری، در سازوکارهای ۷-۶، هستارهای A و B می‌توانند کلید جلسه را از کلید مخفی به اشتراک گذاشته برای ارتباط امن آتی بین آنها برگیرند. این موضوع خارج از دامنه کاربرد این استاندارد است.

۷-۶-۲ سازوکار ۱۳ - اصالت‌سنجی متقابل ناشناس یک سویه امضای آخر سه مرحله‌ای

در این پروتکل اصالت‌سنجی متقابل یک سویه ناشناس سه مرحله‌ای با خصوصیت انقیاد، اولین پیام، امضای گروه را شامل می‌شود. هستار A در G پروتکل اصالت‌سنجی با هستار B را شروع می‌کند و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی اعداد تصادفی کنترل می‌شود (به پیوست ب استاندارد ملی ایران شماره ۱-۱۰۸۲۵ سال: ۱۳۹۱ مراجعه شود). پروتکل در شکل ۸ نشان داده شده است.

سازوکار دارای الزامات زیر است.

- قبل از استفاده از سازوکارها، هستارهای A و B باید در استفاده از گروه دوری $\boldsymbol{G}$، q ترتیبی و تولیدکننده g از G، با توجه به این که کدام مسئله DDH دشوار است به توافق برسند.

اطلاعات افزوده مورد نیاز به شرح زیر است:

کلید عمومی موقت R_A برای کلید خصوصی موقت به طور تصادفی انتخاب‌شده a در Z_q، g^a است.

کلید عمومی موقت R_B برای کلید خصوصی موقت به طور تصادفی انتخاب‌شده b در Z_q، g^b است.

نشان‌های تبادل‌شده در سازوکار به شکل زیر است:

$$Token_{BA} = R_B \,||\, [Text_3] \,||\, sS_B\,(R_B \,||\, R_A \,||\, [Text_2]) \,||\, MAC_{BA}$$
$$Token_{AB} = R_A \,||\, [Text_5] \,||\, gsS_{AG}\,(R_A \,||\, R_B \,||\, [Text_4]) \,||\, MAC_{AB}$$

که MAC_{AB} و MAC_{BA} به شرح زیر است:

$$MAC_{BA} = mac_{MK}\,([Cert_B] \,||\, R_B \,||\, [Text_3] \,||\, sS_B\,(R_B \,||\, R_A \,||\, [Text_2]))$$
$$MAC_{AB} = mac_{MK}\,([Cert_G\,] \,||\, R_A \,||\, [\,Text_5] \,||\, gsS_{AG}\,(R_A \,||\, R_B \,||\, [Text_4]))$$

سازوکار به صورت زیر انجام می‌شود:

a) A مراحل زیر را انجام می‌دهد:

۱) کلید خصوصی موقت a را از Z_q انتخاب می‌کند و کلید عمومی موقت $R_A = g^a$ را محاسبه می‌کند.

۲) g^a و به صورت اختیاری فیلد متنی $Text_1$ را به B ارسال می‌کند.

b) B مراحل زیر را انجام می‌دهد:

۱) کلید خصوصی موقت b را از Z_q انتخاب می‌کند و کلید عمومی موقت $R_B = g^b$ را محاسبه می‌کند.

۲) $g^{ab} = (R_A)^b$ را محاسبه می‌کند.

۳) کلید MAC $MK = kdf(g^{ab})$ را محاسبه می‌کند.

۴) $sS_B(R_B \,||\, R_A \,||\, Text_2)$ را با استفاده از کلید امضا محاسبه می‌کند.

۵) $MAC_{BA} = mac_{MK}([Cert_B] \,||\, R_B \,||\, [Text_3] \,||\, sS_B(R_B \,||\, R_A \,||\, [Text_2]))$ را با استفاده از کلید MAC MK محاسبه می‌کند.

۶) $Token_{BA}$ و به صورت اختیاری گواهی کلید عمومی $Cert_B$ آن را به A ارسال می‌کند.

c) در دریافت پیام حاوی $Token_{BA}$، A مراحل زیر را انجام می‌دهد:

۱) $g^{ab} = (R_B)^a$ را محاسبه می‌کند.

۲) کلید MAC $MK = kdf(g^{ab})$ را محاسبه می‌کند.

۳) با تصدیق گواهی کلید عمومی B یا با ابزارهای دیگر اطمینان حاصل می‌کند که در موقعیت کلید عمومی B است.

۴) $Token_{BA}$ را به شرح زیر تصدیق می‌کند.

أ) امضای B موجود در نشان را تصدیق می‌کند.

ب) وارسی می‌کند که کلید عمومی موقت R_B و R_A در امضا گنجانده شده است.

ج) وارسی می‌کند که کلید عمومی موقت R_A موجود در $Token_{BA}$ برابر با کلید عمومی موقت R_A ارسال‌شده در مرحله a) است.

د) مقدار MAC_{BA} را با استفاده از MK وارسی می‌کند.

۵) $gsS_{AG}\ (R_A \| R_B \| [Text_4])$ را با استفاده از کلید امضای آن محاسبه می‌کند.

۶) $MAC_{AB} = mac_{MK}\ ([Cert_G] \| R_A \| [Text_5] \| gsS_{AG}\ (R_A \| R_B \| [Text_4]))$ را با استفاده از کلید MAC MK محاسبه می‌کند.

d) A، $Token_{AB}$ و به صورت اختیاری گواهی کلید عمومی گروهی $Cert_G$ آن را به B ارسال می‌کند.

e) در دریافت پیام حاوی $Token_{AB}$، B مراحل زیر را انجام می‌دهد:

۱) با تصدیق گواهی کلید عمومی گروهی G یا با ابزارهای دیگر اطمینان حاصل می‌کند در موقعیت کلید عمومی گروهی معتبر G است.

۲) $Token_{AB}$ را به شرح زیر تصدیق می‌کند:

أ) امضای گروهی A موجود در نشان را تصدیق می‌کند.

ب) وارسی می‌کند کلیدهای عمومی موقت R_A و R_B در امضای گروهی گنجانده شده است.

ج) وارسی می‌کند که کلید عمومی موقت R_A موجود در $Token_{AB}$ برابر با کلید عمومی موقت R_A دریافت‌شده در مرحله a) است.

د) وارسی می‌کند که کلید عمومی موقت R_B امضاشده در امضای گروهی $Token_{AB}$ برابر با کلید عمومی موقت R_B ارسال‌شده در مرحله b) است.

ه) مقدار MAC_{AB} را با استفاده از MK وارسی می‌کند.

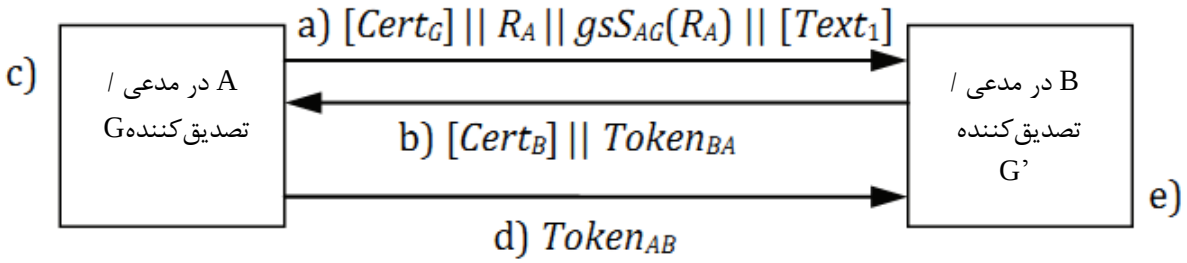
۳-۶-۷ سازوکار ۱۴ - اصالت‌سنجی متقابل ناشناس یک سویه امضای اول سه مرحله‌ای

در این پروتکل اصالت‌سنجی متقابل ناشناس یک سویه سه مرحله‌ای با خصوصیت انقیاد، اولین پیام، امضای گروه را شامل می‌شود. هستار A در G پروتکل اصالت‌سنجی با هستار B را شروع می‌کند و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی اعداد تصادفی کنترل می‌شود (به پیوست ب استاندارد ملی ایران شماره ۱-۱۰۸۲۵ سال: ۱۳۹۱ مراجعه شود).

سازوکار دارای الزامات زیر است.

- قبل از استفاده از سازوکار، هستارهای A و B باید در استفاده از گروه دوری $\boldsymbol{G}$، q ترتیبی و تولیدکننده g از G، با توجه به این که کدام مسئله DDH دشوار است به توافق برسند.

پیام‌های پروتکل و اطلاعات افزوده مورد نیاز به شرح زیر است:



شکل ۱۲ – اصالت‌سنجی متقابل ناشناس یک سویه امضای اول سه مرحله‌ای

کلید عمومی موقت R_A برای کلید خصوصی موقت به طور تصادفی انتخاب‌شده a در Z_q، g^a است.
کلید عمومی موقت R_B برای کلید خصوصی موقت به طور تصادفی انتخاب‌شده b در Z_q، g^b است.
نشان‌های تبادل‌شده در سازوکار به شکل زیر است:

$Token_{AB} = MAC_{AB} \mid\mid [Text_2]$
$Token_{BA} = R_B \mid\mid sS_B(R_B) \mid\mid MAC_{BA} \mid\mid [Text_3]$

که MAC_{AB} و MAC_{BA} به شرح زیر است:

$MAC_{AB} = mac_{MK}(R_A \mid\mid gsS_{AG}(R_A) \mid\mid R_B \mid\mid sS_B(R_B) \mid\mid [Text_4])$.
$MAC_{BA} = mac_{MK}(R_B \mid\mid sS_B(R_B) \mid\mid R_A \mid\mid gsS_{AG}(R_A) \mid\mid [Text_5])$.

سازوکار به صورت زیر انجام می‌شود:

a) A مراحل زیر را انجام می‌دهد:

۱) کلید خصوصی موقت a را از Z_q انتخاب می‌کند و کلید عمومی موقت $R_A = g^a$ را محاسبه می‌کند.
۲) $gsS_{AG}(R_A)$ را با استفاده از کلید امضا محاسبه می‌کند.
۳) g^a، $gsS_{AG}(R_A)$ و به صورت اختیاری فیلد متنی $Text_1$ را به B ارسال می‌کند.

b) B مراحل زیر را انجام می‌دهد:

۱) با تصدیق گواهی کلید عمومی گروهی G یا با ابزارهای دیگر اطمینان حاصل می‌کند که در موقعیت کلید عمومی گروهی معتبر G است.
۲) امضای گروهی A را تصدیق می‌کند.
۳) کلید خصوصی موقت b را از Z_q انتخاب می‌کند و کلید عمومی موقت $R_B = g^b$ را محاسبه می‌کند.
۴) $sS_B(R_B)$ را با استفاده از کلید امضا محاسبه می‌کند.
۵) $g^{ab} = (R_A)^b$ را محاسبه می‌کند.
۶) MAC، کلید $MK = kdf(g^{ab})$ را محاسبه می‌کند.
۷) $MAC_{BA} = mac_{MK}(R_B \mid\mid sS_B(R_B) \mid\mid R_A \mid\mid gsS_{AG}(R_A) \mid\mid [Text_5]))$ را با استفاده از کلید MAC MK محاسبه می‌کند.
۸) $Token_{BA}$ و به صورت اختیاری گواهی کلید عمومی $Cert_B$ آن را به A ارسال می‌کند.

c) در دریافت پیام حاوی $Token_{BA}$، A مراحل زیر را انجام می‌دهد:

۱) با تصدیق گواهی کلید عمومی B یا با ابزارهای دیگر اطمینان حاصل می‌کند در موقعیت کلید عمومی معتبر B است.

۲) امضای B را تصدیق می‌کند.

۳) $g^{ab} = (R_B)^a$ را محاسبه می‌کند.

۴) کلید MAC، $MK = kdf(g^{ab})$ را محاسبه می‌کند.

۵) $MAC_{AB} = mac_{MK}(R_A \,||\, gsS_{AG}(R_A) \,||\, R_B \,||\, sS_B(R_B) \,||\, [Text_4])$ را با استفاده از کلید MAC MK محاسبه می‌کند.

۶) مقدار MAC_{BA} را با استفاده از MK وارسی می‌کند.

d) A، $Token_{AB}$ را به B ارسال می‌کند.

e) در دریافت پیام حاوی $Token_{AB}$، B مقدار MAC_{AB} را با استفاده از MK وارسی می‌کند.

۷-۶-۴ سازوکار ۱۵ - اصالت‌سنجی متقابل ناشناس یک سویه امضای آخر موازی دو مرحله‌ای

در این پروتکل اصالت‌سنجی متقابل ناشناس یک سویه موازی دو مرحله‌ای با خصوصیت انقیاد، اولین پیام، امضای گروه را شامل می‌شود. اصالت‌سنجی ناشناس موازی با هستار A در G و هستار B انجام می‌شود و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی اعداد تصادفی کنترل می‌شود (به پیوست ب استاندارد ملی ایران شماره ۱-۱۰۸۲۵ سال: ۱۳۹۱ مراجعه شود). پروتکل در شکل ۹ نشان داده شده است.

سازوکار دارای الزامات زیر است.

- قبل از استفاده از سازوکار، هستارهای A و B باید در استفاده از گروه دوری $\boldsymbol{G}$، q ترتیبی و تولیدکننده g از G، با توجه به این که کدام مسئله DDH دشوار است به توافق برسند.

اطلاعات افزوده مورد نیاز به شرح زیر است:

کلید عمومی موقت R_B برای کلید خصوصی موقت به طور تصادفی انتخاب‌شده b در Z_q، g^b است.

کلید عمومی موقت R_A برای کلید خصوصی موقت به طور تصادفی انتخاب‌شده a در Z_q، g^a است.

نشان‌های تبادل‌شده در سازوکار به شکل زیر است:

$Token_{AB} = R_A \,||\, [Text_4] \,||\, gsS_{AG}\,(R_A \,||\, R_B \,||\, [Text_3]) \,||\, MAC_{AB}$
$Token_{BA} = R_B \,||\, [Text_6] \,||\, sS_B\,(R_B \,||\, R_A \,||\, [Text_5]) \,||\, MAC_{BA}$

که MAC_{AB} و MAC_{BA} به شرح زیر است:

$MAC_{AB} = mac_{MK}\,([Cert_G] \,||\, R_A \,||\, [Text_4] \,||\, gsS_{AG}\,(R_A \,||\, R_B \,||\, [Text_3]))$
$MAC_{BA} = mac_{MK}\,([Cert_B] \,||\, R_B \,||\, [Text_6] \,||\, sS_B\,(R_B \,||\, R_A \,||\, [Text_5]))$

سازوکار به صورت زیر انجام می‌شود:

a) A مراحل زیر را انجام می‌دهد:

۱) کلید خصوصی موقت a را از Z_q انتخاب می‌کند و کلید عمومی موقت $R_A = g^a$ را محاسبه می‌کند.

۲) R_A و به صورت اختیاری $Cert_G$ و فیلد متنی $Text_1$ را به B ارسال می‌کند.

a') B مراحل زیر را انجام می‌دهد:

۱) کلید خصوصی موقت b را از Z_q انتخاب می‌کند و کلید عمومی موقت $R_B = g^b$ را محاسبه می‌کند.

۲) R_B و به صورت اختیاری $Cert_B$ و فیلد متنی $Text_2$ را به A ارسال می‌کند.

b) A با تصدیق گواهی کلید عمومی مرتبط یا با ابزارهای دیگر اطمینان حاصل می‌کند در موقعیت کلید عمومی معتبر هستار B است. B اطمینان حاصل می‌کند که در موقعیت کلید عمومی گروهی معتبر است که هستار A متعلق به آن است، این کار با تصدیق گواهی کلید عمومی گروهی مرتبط یا با ابزارهای دیگر انجام می‌شود.

c) A مراحل زیر را انجام می‌دهد:

۱) $g^{ab} = (R_B)^a$ را محاسبه می‌کند.

۲) MAC، کلید $MK = kdf(g^{ab})$ را محاسبه می‌کند.

۳) $gsS_{AG}(R_A \| R_B \| [Text_3])$ را با استفاده از کلید امضا محاسبه می‌کند.

۴) $MAC_{AB} = mac_{MK}([Cert_G] \| R_A \| [Text_4] \| gsS_{AG}(R_A \| R_B \| [Text_3]))$ را با استفاده از کلید MAC MK محاسبه می‌کند.

۵) $Token_{BA}$ را به B ارسال می‌کند.

c') B مراحل زیر را انجام می‌دهد:

۱) $g^{ab} = (R_A)b$ را محاسبه می‌کند.

۲) MAC، کلید $MK = kdf(g^{ab})$ را محاسبه می‌کند.

۳) $sS_B(R_B \| R_A \| [Text_5])$ را با استفاده از کلید امضا محاسبه می‌کند.

۴) $MAC_{BA} = mac_{MK}([Cert_B] \| R_B \| [Text_6] \| sS_B(R_B \| R_A \| [Text_5]))$ را با استفاده از کلید MAC MK محاسبه می‌کند.

۵) $Token_{BA}$ را به A ارسال می‌کند.

d) A و B مراحل زیر را انجام می‌دهند:

۱) $Token_{AB}$ و $Token_{BA}$ را به شرح زیر تصدیق می‌کنند:

أ) امضا یا امضای گروهی موجود در نشان را تصدیق می‌کنند.

ب) وارسی می‌کنند کلیدهای عمومی موقت R_A و R_B در امضا یا امضای گروهی گنجانده شده است.

ج) A وارسی می‌کند که کلید عمومی موقت R_B موجود در $Token_{BA}$ برابر با کلید عمومی موقت R_B دریافت‌شده در مرحله a') است و R_A امضاشده در امضای $Token_{BA}$ برابر با کلید عمومی موقت R_A ارسال‌شده در مرحله a) است.

د) B وارسی می‌کند که کلید عمومی موقت R_A موجود در $Token_{AB}$ برابر با کلید عمومی موقت R_A دریافت‌شده در مرحله a) است و R_B امضاشده در امضای گروهی $Token_{AB}$ برابر با کلید عمومی موقت R_B ارسال‌شده در مرحله a') است.

ه) مقادیر MAC_{AB} و MAC_{BA} را با استفاده از MK وارسی می‌کند.

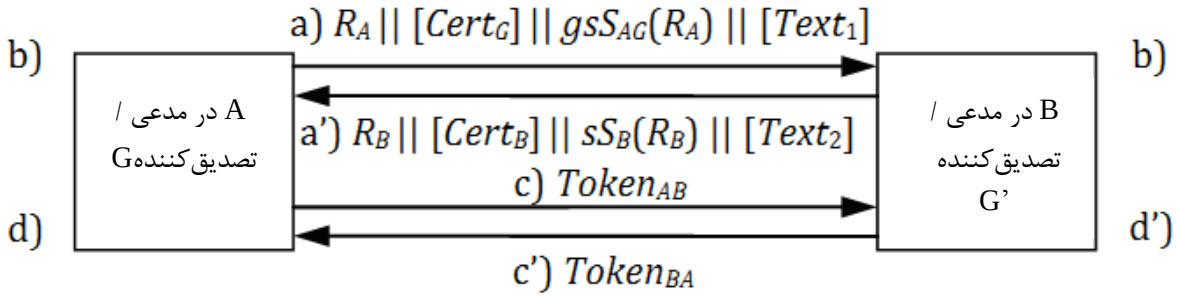
۵-۶-۷ سازوکار ۱۶ - اصالت‌سنجی متقابل ناشناس یک سویه امضای اول موازی دو مرحله‌ای

در این پروتکل اصالت‌سنجی متقابل ناشناس یک سویه موازی دو مرحله‌ای با خصوصیت انقیاد، اولین پیام، امضای گروه را شامل می‌شود. اصالت‌سنجی ناشناس موازی با هستار A در G و هستار B انجام می‌شود و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی اعداد تصادفی کنترل می‌شود (به پیوست ب استاندارد ملی ایران شماره ۱-۱۰۸۲۵ سال: ۱۳۹۱ مراجعه شود).

سازوکار دارای الزامات زیر است.

- قبل از استفاده از سازوکار، هستارهای A و B باید در استفاده از گروه دوری $\boldsymbol{G}$، q ترتیبی و تولیدکننده g از G، با توجه به این که کدام مسئله DDH دشوار است به توافق برسند.

پیام‌های پروتکل و اطلاعات افزوده مورد نیاز به شرح زیر است:



شکل ۱۳ - اصالت‌سنجی متقابل ناشناس یک سویه امضای اول موازی دو مرحله‌ای

کلید عمومی موقت R_B برای کلید خصوصی موقت به طور تصادفی انتخاب‌شده b در Z_q، g^b است.

کلید عمومی موقت R_A برای کلید خصوصی موقت به طور تصادفی انتخاب‌شده a در Z_q، g^a است.

نشان‌های تبادل‌شده در سازوکار به شکل زیر است:

$Token_{AB} = MAC_{AB} \,||\, [Text_3]$
$Token_{BA} = MAC_{BA} \,||\, [Text_4]$

که MAC_{AB} و MAC_{BA} به شرح زیر است:

$MAC_{AB} = mac_{MK}\,(R_A \,||\, gsS_{AG}\,(R_A) \,||\, R_B \,||\, sS_B\,(R_B) \,||\, [Text_5]).$
$MAC_{BA} = mac_{MK}\,(R_B \,||\, sS_B\,(R_B) \,||\, R_A \,||\, gsS_{AG}\,(R_A) \,||\, [Text_6]).$

سازوکار به صورت زیر انجام می‌شود:

a) A مراحل زیر را انجام می‌دهد:

۱) کلید خصوصی موقت a را از Z_q انتخاب می‌کند و کلید عمومی موقت $R_A = g^a$ را محاسبه می‌کند.

۲) $gsS_{AG}(R_A)$ را با استفاده از کلید امضای آن محاسبه می‌کند.

۳) g^a، $gsS_{AG}(R_A)$ و به صورت اختیاری $Cert_G$ و فیلد متنی $Text_1$ را به B ارسال می‌کند.

a') B مراحل زیر را انجام می‌دهد:

۱) کلید خصوصی موقت b را از Z_q انتخاب می‌کند و کلید عمومی موقت $R_B = g^b$ را محاسبه می‌کند.

۲) $sSB(R_B)$ را با استفاده از کلید امضا محاسبه می‌کند.

۳) g^b، $sSB(R_B)$ و به صورت اختیاری $Cert_B$ و فیلد متنی $Text_2$ را به A ارسال می‌کند.

b) A با تصدیق گواهی کلید عمومی مرتبط یا با ابزارهای دیگر اطمینان حاصل می‌کند در موقعیت کلید عمومی گروهی معتبر هستار B است. B اطمینان حاصل می‌کند که در موقعیت کلید عمومی گروهی معتبر است که هستار A متعلق به آن است، این کار با تصدیق گواهی کلید عمومی گروهی مرتبط یا با ابزارهای دیگر انجام می‌شود. A امضای دریافت‌شده و B امضای گروهی دریافت‌شده را تصدیق می‌کند.

c) A مراحل زیر را انجام می‌دهد:

۱) $g^{ab} = (R_B)^a$ را محاسبه می‌کند.

۲) MAC، کلید $MK = kdf(g^{ab})$ را محاسبه می‌کند.

۳) $MAC_{AB} = mac_{MK}(R_A \,||\, gsS_{AG}(R_A) \,||\, R_B \,||\, sS_B(R_B) \,||\, [Text_5])$ را با استفاده از کلید MAC MK محاسبه می‌کند.

۴) $Token_{AB}$ را به B ارسال می‌کند.

c') B مراحل زیر را انجام می‌دهد:

۱) $g^{ab} = (R_A)^b$ را محاسبه می‌کند.

۲) MAC، کلید $MK = kdf(g^{ab})$ را محاسبه می‌کند.

۳) $MAC_{BA} = mac_{MK}(R_B \,||\, sS_B(R_B) \,||\, R_A \,||\, gsS_{AG}(R_A) \,||\, [Text_6])$ را با استفاده از کلید MAC MK محاسبه می‌کند.

۴) $Token_{BA}$ را به A ارسال می‌کند.

d) A مراحل زیر را انجام می‌دهد:

۱) کلید عمومی موقت R_B و $sS_B(R_B)$ در مرحله *a'*) را بازیابی می‌کند.

۲) $MAC_{BA} = mac_{MK}(R_B \,||\, sS_B(R_B) \,||\, R_A \,||\, gsS_{AG}(R_A) \,||\, [Text_6])$ را با استفاده از کلید MAC MK محاسبه می‌کند.

۳) اعتبار MAC_{BA} در نشان مرحله *c'*) را با استفاده از مقدار محاسبه‌شده در مرحله فرعی ۲) وارسی می‌کند.

d') B مراحل زیر را انجام می‌دهد:

۱) کلید عمومی موقت R_A و $gsS_{AG}(R_A)$ را در مرحله *a*) بازیابی می‌کند.

۲) $MAC_{AB} = mac_{MK}(R_A \,||\, gsS_{AG}(R_A) \,||\, R_B \,||\, sS_B(R_B) \,||\, [Text_5])$ را با استفاده از کلید MAC MK محاسبه می‌کند.

۳) اعتبار MAC_{AB} را در نشان مرحله *c*) با استفاده از مقدار محاسبه‌شده در مرحله فرعی ۲) وارسی می‌کند.

۸ سازوکارهای دربرگیرنده TTP برخط

۸-۱ مقدمه

بند ۸ سازوکارهای اصالت‌سنجی هستار ناشناس دربرگیرنده TTP برخط را مشخص می‌کند.

سازوکارهای اصالت‌سنجی ناشناس در بند ۸، نیاز به دو هستار A در G و/ یا B در G' دارند تا کلیدهای عمومی گروهی یکدیگر را با استفاده طرف سوم مورد اعتماد برخط (TP) اعتبارسنجی کنند. این طرف سوم مورد اعتماد باید رونوشت‌های[1] قابل طمینان کلیدهای عمومی گروهی G (گروهی که A متعلق به آن است) و G' (گروهی که B متعلق به آن است) را پردازش کند. هستارهای A و B باید رونوشت قابل اطمینان کلید عمومی TP را پردازش کنند.

پیاده‌سازی‌های سازوکارها باید از یکی از طرح‌های امضای گروهی مشخص‌شده در *ISO/IEC 20008-2* استفاده کند.

۸-۲ اصالت‌سنجی ناشناس یک سویه

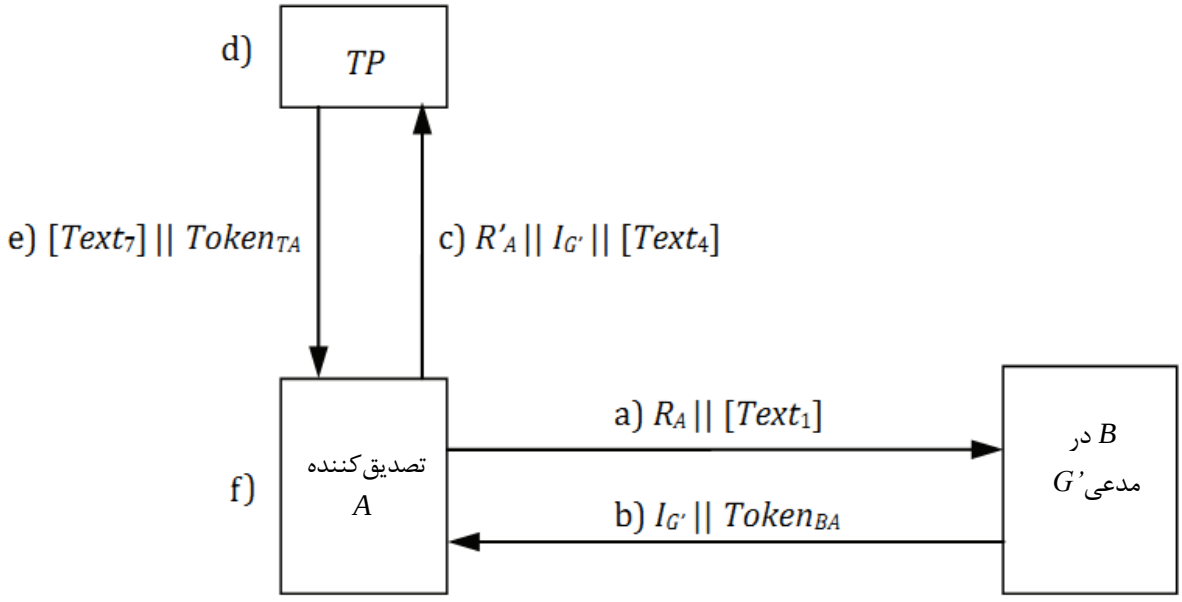
۸-۲-۱ کلیات

اصالت‌سنجی ناشناس یک سویه بدان معنی است که تنها یکی از دو هستار با استفاده از سازوکار اصالت‌سنجی می‌شود و هویت هستار اصالت‌سنجی‌شده برای هستار دیگر ناشناس است.

۸-۲-۲ سازوکار ۱۷ - اصالت‌سنجی ناشناس یک سویه چهار مرحله‌ای (شروع‌شده توسط A)

در این سازوکار، هستار A پروتکل اصالت‌سنجی را با هستار B در G' شروع می‌کند و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی عدد تصادفی کنترل می‌شود (به پیوست ب استاندارد ملی ایران شماره ۱-۱۰۸۲۵ سال: ۱۳۹۱مراجعه شود.

این سازوکار اصالت‌سنجی در شکل ۱۴ نشان داده شده است.



شکل ۱۴ - اصالت‌سنجی ناشناس یک سویه چهار مرحله‌ای (شروع‌شده توسط A)

نشان‌ها باید به شرح زیر ایجاد شود.

$$Token_{BA} = [Text_3] \,||\, gsS_{BG'}(A \,||\, R_A \,||\, [Text_2])$$

1 - Copies

$Token_{TA} = Res_{G'} \,||\, sST\,(R'_A \,||\, Res_{G'} \,||\, [Text_6])$

مقادیر فیلدهای $I_{G'}$، $Res_{G'}$ ، *Status* و *Failure* باید به شکل‌های زیر باشد:

G' : گروهی که هستار B متعلق به آن است.

$I_{G'} = G'$ یا $Cert_{G'}$, G' هویت

$Res_{G'}$= $(Cert_{G'} \,||\, Status)$, $(G' \,||\, P_{G'})$ یا *Failure*

Status = *True* یا *False*. مقدار فیلد باید اگر گواهی لغوشده شناخته شده باشد، *False* تنظیم شود. در غیر این صورت باید *True* تنظیم شود.

Failure: $Res_{G'}$ اگر کلید عمومی یا گواهی G' نتواند توسط *TP* یافت شود، *Failure* تنظیم خواهد شد.

در سازوکار، اگر *TP* نگاشت بین هویت G' و $P_{G'}$ را بداند، باید $I_{G'} = G'$ را تنظیم کند. در غیر این صورت، باید $I_{G'} = Cert_{G'}$ را تنظیم کند و G' باید برابر تنظیم فیلدهای هویت متمایز در $Cert_{G'}$ تنظیم شود. اگر G' یا $Cert_{G'}$ مجاز به استفاده به عنوان یک هویت باشد، باید ابزارهایی را از پیش ترتیب دهند تا به *TP* اجازه تمایز دو نوع نشانه هویت را بدهند. مقدار $Res_{G'}$ باید با توجه به جدول ۱ مشخص شود.

جدول ۱ – مقدار $Res_{G'}$

فیلد	گزینه ۱	گزینه ۲
$I_{G'}$	G'	$Cert_{G'}$
$Res_{G'}$	*Failure* یا $(G' \,||\, P_{G'})$	*Failure* یا $(Cert_{G'} \,||\, Status)$

سازوکار به صورت زیر انجام می‌شود:

a) A، عدد تصادفی R_A و به صورت اختیاری فیلد متنی $Text_1$ را به B ارسال می‌کند.

b) B نشان $Token_{BA}$ و $I_{G'}$را به A ارسال می‌کند.

c) A عدد تصادفی R'_A، همراه با $I_{G'}$و به صورت اختیاری فیلد متنی $Text_4$ را به *TP* ارسال می‌کند.

d) در دریافت پیام مرحله *c*) از A، *TP* مراحل زیر را انجام می‌دهد. اگر $I_{G'} = G'$ باشد، *TP*، $P_{G'}$را بازیابی می‌کند؛ اگر $I_{G'} = Cert_{G'}$ باشد، *TP* اعتبار $Cert_{G'}$ را وارسی می‌کند.

e) سپس *TP*، $Token_{TA}$ و به صورت اختیاری فیلد متنی $Text_7$ را به Aارسال می‌کند. فیلد $Res_{G'}$ در $Token_{TA}$ باید: گواهی G' و *Status* (وضعیت) آن، شناسانه تمایز G' و کلید عمومی آن یا نشانه‌ای از *Failure* (مردودی) باشد.

f) در دریافت پیام در مرحله *e*) از *TP*، A مراحل زیر را انجام می‌دهد:

۱) $Token_{TA}$ را با وارسی امضای *TP* موجود در نشان و با وارسی این که عدد تصادفی R'_A، ارسال‌شده به *TP* در مرحله *c*) مشابه عدد تصادفی R'_A موجود در داده امضاشده $Token_{TA}$ است، تصدیق می‌کند.

۲) اعتبار G' را با وارسی $Res_{G'}$ تصدیق می‌کند.

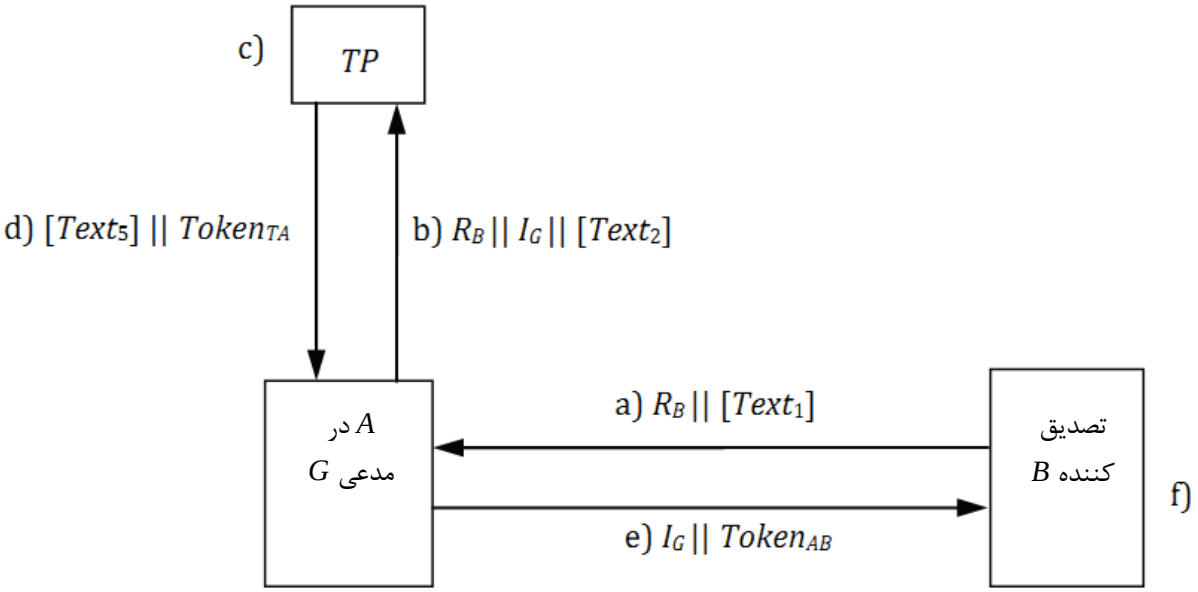
۳) کلید عمومی G' را از پیام بازیابی می‌کند، $Token_{BA}$ دریافت‌شده در مرحله *b*) را با وارسی امضای ناشناس B موجود در نشان و وارسی این که مقدار فیلد شناسانه (A) در پیامی از $Token_{BA}$ که باید

امضا شود برابر شناسانه A است و سپس وارسی این که عدد تصادفی R_A، ارسال‌شده به B در مرحله a) مشابه عدد تصادفی R_A موجود در $Token_{BA}$ است، تصدیق می‌کند.

۸-۲-۳ سازوکار ۱۸ - اصالت‌سنجی ناشناس یک سویه چهار مرحله‌ای (شروع‌شده توسط B)

در این سازوکار، هستار B پروتکل اصالت‌سنجی را با هستار A در G شروع می‌کند و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی عدد تصادفی کنترل می‌شود (به پیوست ب استاندارد ملی ایران شماره ۱-۱۰۸۲۵ سال: ۱۳۹۱ مراجعه شود)

این سازوکار اصالت‌سنجی در شکل ۱۵ نشان داده شده است.



شکل ۱۵ - اصالت‌سنجی ناشناس یک سویه چهار مرحله‌ای (شروع‌شده توسط B)

نشان‌ها باید به شرح زیر ایجاد شود.

$Token_{AB} = Res_G \,||\, sS_T\,(R_B \,||\, Res_G \,||\, [Text_3]) \,||\, gsS_{AG}\,(R_B \,||\, B \,||\, [Text_6])$

$Token_{TA} = Res_G \,||\, sS_T\,(R_B \,||\, Res_G \,||\, [Text_3])$

مقادیر فیلدهای $I_{G'}$، $Res_{G'}$، $Status$ و $Failure$ باید به شکل‌های زیر باشد:

G: گروهی که هستار A متعلق به آن است.

I_G = هویت G، یا $Cert_{G'}$

Res_G = $(Cert_G \,||\, Status)$, $(G \,||\, P_G)$ یا $Failure$

$Status$ = $True$ یا $False$. مقدار این فیلد باید اگر گواهی لغوشده شناخته شده باشد، $False$ تنظیم شود. در غیر این صورت باید $True$ تنظیم شود.

$Failure$: Res_G باید اگر کلید عمومی یا گواهی هستار G نتواند با TP یافت شود، $Failure$ تنظیم شود.

در سازوکار، اگر TP نگاشت بین هویت G و P_G را بداند، باید I_G = G را تنظیم کند. در غیر این صورت، باید I_G = $Cert_G$ را تنظیم کند و G باید برابر تنظیم فیلدهای هویت متمایز در $Cert_G$ تنظیم شود. اگر G یا

$Cert_G$ مجاز به استفاده به عنوان یک هویت باشند، باید ابزارهایی را از پیش ترتیب دهند تا به TP اجازه تمایز دو نوع نشانه هویت را بدهند. مقدار Res_G باید با توجه به جدول ۲ تعیین شود.

جدول ۲ – مقدار Res_G

فیلد	گزینه ۱	گزینه ۲
I_G	G	$Cert_G$
Res_G	$Failure$ یا $(G \mid\mid P_G)$	$Failure$ یا $(Cert_G \mid\mid Status)$

سازوکار به صورت زیر انجام می‌شود:

a) B، عدد تصادفی R_B و به صورت اختیاری فیلد متنی $Text_1$ را به A ارسال می‌کند.

b) A، R_B، I_G و به صورت اختیاری، فیلد متنی $Text_2$ را به TP ارسال می‌کند.

c) در دریافت پیام مرحله *b*) از A، TP مراحل زیر را انجام می‌دهد. اگر $I_G = G$ باشد، TP، P_G را بازیابی می‌کند؛ اگر $I_G = Cert_G$ باشد، TP اعتبار $Cert_G$ را وارسی می‌کند.

d) سپس TP، $Token_{TA}$ و به صورت اختیاری فیلد متنی $Text_5$ را به A ارسال می‌کند. فیلد Res_G در $Token_{TA}$ باید گواهی G و $Status$ (وضعیت) آن، شناسانه تمایز G و کلید عمومی آنها یا نشانه‌ای از $Failure$ (مردودی) باشد.

e) A، نشان $Token_{AB}$ و I_G را به B ارسال می‌کند.

f) در دریافت پیام در مرحله *e*) از A، B مراحل زیر را انجام می‌دهد:

۱) امضای TP در $Token_{AB}$ را با وارسی امضای TP موجود در نشان و با وارسی این که عدد تصادفی R_B، ارسال‌شده به A در مرحله *a*) مشابه عدد تصادفی R_B موجود در داده امضاشده $Token_{AB}$ است، تصدیق می‌کند.

۲) اعتبار G' را با وارسی $Res_{G'}$ تصدیق می‌کند.

۳) کلید عمومی G را از پیام بازیابی می‌کند، $Token_{AB}$ را با وارسی امضای ناشناس A موجود در نشان و وارسی این که مقدار فیلد شناسانه (B) در پیامی از $Token_{AB}$ که باید امضا شود برابر شناسانه B است و سپس وارسی این که عدد تصادفی R_B، ارسال‌شده به A در مرحله *a*) مشابه عدد تصادفی R_B موجود در داده امضاشده A، $Token_{AB}$ است، تصدیق می‌کند.

۸-۳ اصالت‌سنجی ناشناس متقابل

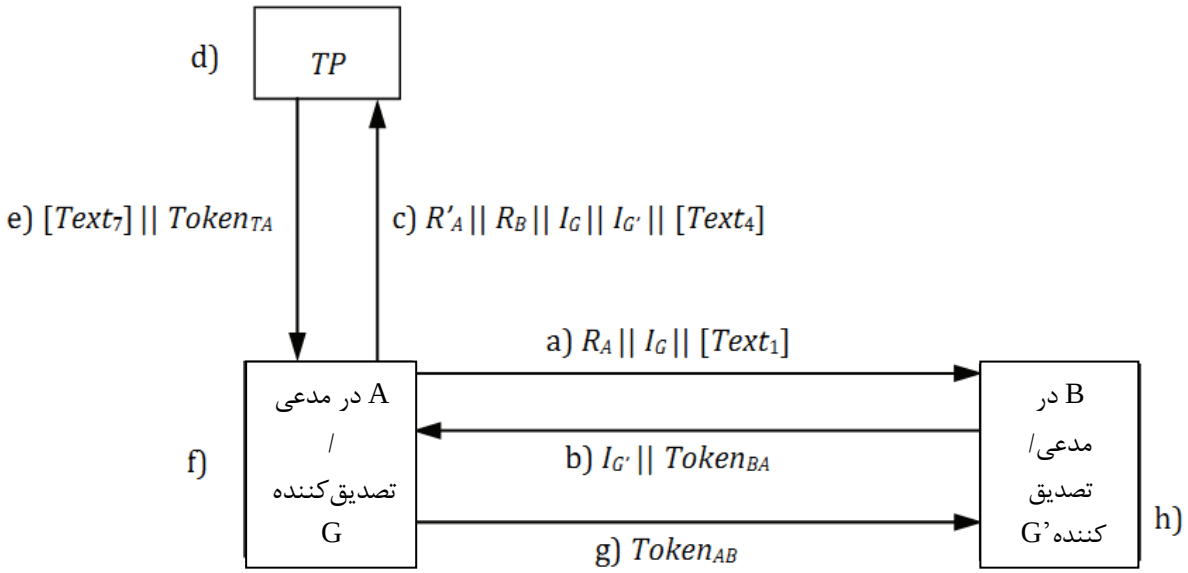
۸-۳-۱ کلیات

اصالت‌سنجی ناشناس متقابل بدان معنی است که دو هستار ارتباطی برای یکدیگر اصالت‌سنجی شده‌اند و هویت دو هستار برای یکدیگر ناشناس است.

۸-۳-۲ سازوکار ۱۹ – اصالت‌سنجی ناشناس متقابل پنج مرحله‌ای (شروع‌شده توسط A)

در این سازوکار، هستار A در G، پروتکل اصالت‌سنجی با هستار B را در G' شروع می‌کند و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی عدد تصادفی کنترل می‌شود (به پیوست ب استاندارد ملی ایران شماره ۱-۱۰۸۲۵ سال: ۱۳۹۱ مراجعه شود)

این سازوکار اصالت‌سنجی در شکل ۱۶ نشان داده شده است.



شکل ۱۶ – اصالت‌سنجی متقابل ناشناس پنج مرحله‌ای (شروع‌شده توسط A)

نشان‌ها باید با توجه به یکی از دو گزینه زیر ایجاد شود.

گزینه ۱:

$Token_{BA} = R_A \,||\, R_B \,||\, [Text_3] \,||\, gsS_{BG'}\,(G' \,||\, R_A \,||\, R_B \,||\, G \,||\, [Text_2])$
$Token_{TA} = Res_G \,||\, Res_{G'} \,||\, sS_T\,(R'_A \,||\, Res_{G'} \,||\, [Text_6]) \,||\, sST\,(R_B \,||\, Res_G \,||\, [Text_5])$
$Token_{AB} = [Text_9] \,||\, Res_G \,||\, sS_T\,(R_B \,||\, Res_G \,||\, [Text_5]) \,||\, gsS_{AG}\,(R_B \,||\, R_A \,||\, G' \,||\, G \,||\, [Text_8])$

گزینه ۲:

$Token_{BA} = R_A \,||\, R_B \,||\, [Text_3] \,||\, gsS_{BG'}\,(G' \,||\, R_A \,||\, R_B \,||\, G \,||\, [Text_2])$
$Token_{TA} = Res_G \,||\, Res_{G'} \,||\, sS_T\,(R'_A \,||\, R_B \,||\, Res_G \,||\, Res_{G'} \,||\, [Text_5])$
$Token_{AB} = R'_A \,||\, [Text_9] \,||\, Token_{TA} \,||\, gsS_{AG}\,(R_B \,||\, R_A \,||\, G' \,||\, G \,||\, [Text_8])$

مقادیر فیلدهای I_G، $I_{G'}$، Res_G ، $Res_{G'}$ ، $Status$ و $Failure$ باید به شکل‌های زیر باشد:

$I_G = G$ یا $Cert_G$

$I_{G'} = G'$ یا $Cert_{G'}$

$Res_G = (Cert_G \,||\, Status), (G \,||\, P_G)$ یا $Failure$

$Res_{G'} = (Cert_{G'} \,||\, Status), (G' \,||\, P_{G'})$ یا $Failure$

$Status = True$ یا $False$. مقدار فیلد باید اگر گواهی کلید عمومی گروهی لغوشده شناخته شده است، $False$ تنظیم شود. در غیر این صورت باید $True$ تنظیم شود.

$Failure$: Res_G اگر کلید عمومی گروهی یا گواهی کلید عمومی گروهی G نتواند توسط TP یافت شود، به $Failure$ تنظیم شود.

در سازوکار، اگر TP نگاشت بین شناسانه G و کلید عمومی گروهی P_G را بداند، باید $I_G = G$ را تنظیم کند. در غیر این صورت، باید $I_G = Cert_G$ را تنظیم کند و G باید برابر تنظیم فیلدهای هویت متمایز در $Cert_G$

تنظیم شود. اگر G یا $Cert_G$ مجاز به استفاده به عنوان یک هویت باشند، باید ابزارهایی را از پیش ترتیب دهند تا به TP اجازه تمایز دو نوع نشانه هویت را بدهند. مقدار Res_G باید با توجه به جدول ۳ مشخص شود.

جدول ۳ – مقدار Res_G

فیلد	گزینه ۱	گزینه ۲
I_G	G	$Cert_G$
Res_G	$Failure$ یا $(G \mid\mid P_G)$	$Failure$ یا $(Cert_G \mid\mid Status)$

سازوکار به صورت زیر انجام می‌شود:

a) A، عدد تصادفی R_A، هویت G، I_G و به صورت اختیاری فیلد متنی $Text_1$ را به B ارسال می‌کند.

b) B، نشان $Token_{BA}$ و $I_{G'}$ را به A ارسال می‌کند.

c) A، عدد تصادفی R'_A همراه با R_B، I_G، $I_{G'}$ و به صورت اختیاری، فیلد متنی $Text_4$ را به TP ارسال می‌کند.

d) در دریافت پیام مرحله *c*) از A، TP مراحل زیر را انجام می‌دهد. اگر $I_G = G$ و $I_{G'} = G'$ باشد، TP، P_G و $P_{G'}$ را بازیابی می‌کند؛ اگر $I_G = Cert_G$ و $I_{G'} = Cert_{G'}$ باشد، TP اعتبار $Cert_G$ و $Cert_{G'}$ را وارسی می‌کند.

e) سپس TP، $Token_{TA}$ و به صورت اختیاری فیلد متنی $Text_7$ را به A ارسال می‌کند. فیلدهای Res_G، $Res_{G'}$ در $Token_{TA}$ باید: گواهی‌های کلید عمومی گروهی G و G' و $Status$ (وضعیت) آن‌ها، شناسانه G و G' و کلیدهای عمومی گروهی آن‌ها یا نشانه‌ای از $Failure$ (مردودی) باشد.

f) در دریافت پیام در مرحله *e*) از TP، A مراحل زیر را انجام می‌دهد:

۱) $Token_{TA}$ را با وارسی امضای TP موجود در نشان و با وارسی این که عدد تصادفی R'_A، ارسال‌شده به TP در مرحله *c*) مشابه عدد تصادفی R'_A موجود در پیامی از $Token_{TA}$ که باید امضا شود است، تصدیق می‌کند.

۲) کلید عمومی گروهی G' را از پیام بازیابی می‌کند، $Token_{BA}$ دریافت‌شده در مرحله *b*) را با وارسی امضای گروهی B موجود در نشان و وارسی این که مقدار فیلد شناسانه (G) در پیامی از $Token_{BA}$ که باید امضا شود برابر شناسانه G است و سپس وارسی این که عدد تصادفی R_A، ارسال‌شده به B در مرحله *a*) مشابه عدد تصادفی R_A موجود در $Token_{BA}$ است، تصدیق می‌کند.

g) A، $Token_{AB}$ را به B ارسال می‌کند.

h) در دریافت پیام در مرحله *g*) از A، B مراحل زیر را انجام می‌دهد:

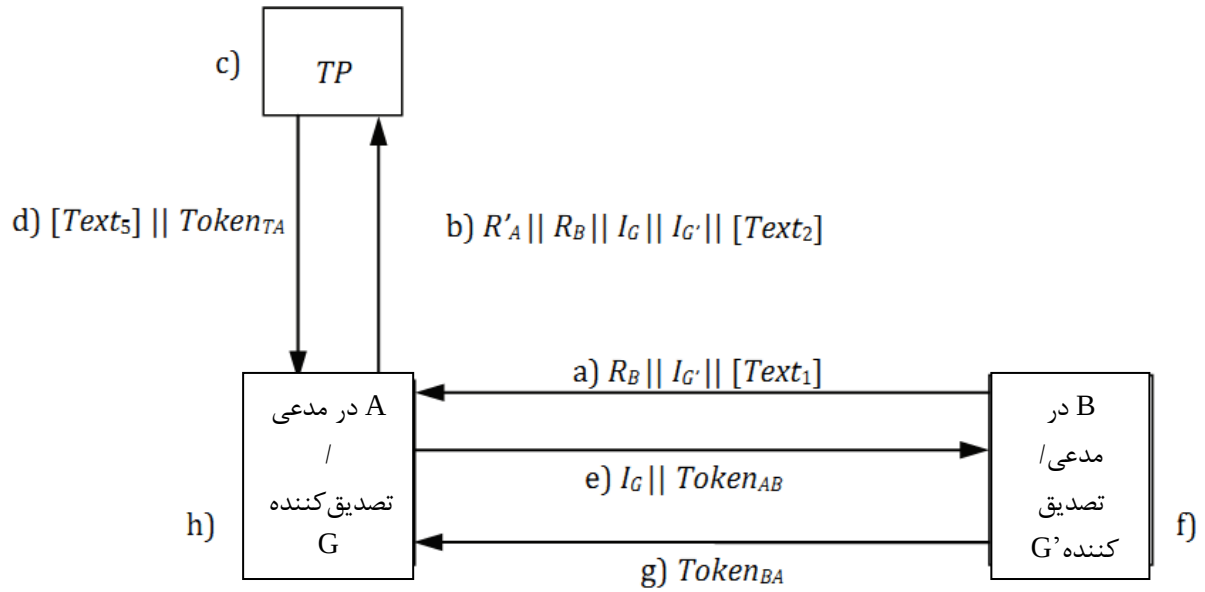
۱) $Token_{TA}$ را با وارسی امضای TP موجود در نشان و با وارسی این که عدد تصادفی R_B، ارسال‌شده به A در مرحله *b*) مشابه عدد تصادفی R_B موجود در پیامی از $Token_{TA}$ که باید امضا شود است، تصدیق می‌کند.

۲) کلید عمومی گروهی G را از پیام بازیابی می‌کند، $Token_{AB}$ را با وارسی امضای گروهی G موجود در نشان و وارسی این که مقدار فیلد شناسانه (G') در پیامی از $Token_{AB}$ که باید امضا شود برابر شناسانه G' است و سپس وارسی این که عدد تصادفی R_B، موجود در پیامی از $Token_{AB}$ که باید امضا شود برابر عدد تصادفی R_B ارسال‌شده به A در مرحله *b*) است، تصدیق می‌کند.

۸-۳-۳ سازوکار ۲۰ - اصالت‌سنجی ناشناس متقابل پنج مرحله‌ای (شروع‌شده توسط B)

در این سازوکار، هستار B در G' پروتکل اصالت‌سنجی با هستار A در G را شروع می‌کند و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی عدد تصادفی کنترل می‌شود (به پیوست ب استاندارد ملی ایران شماره ۱-۱۰۸۲۵ سال: ۱۳۹۱ مراجعه شود).

این سازوکار اصالت‌سنجی در شکل ۱۷ نشان داده شده است.



شکل ۱۷ - اصالت‌سنجی ناشناس متقابل پنج مرحله‌ای (شروع‌شده توسط B)

نشان‌ها باید با توجه به یکی از دو گزینه زیر ایجاد شود.

گزینه ۱:

$Token_{BA} = R_A \| R_B \| [Text_9] \| gsS_{BG'} (G \| R_A \| R_B \| G' \| [Text_8])$
$Token_{TA} = Res_G \| Res_{G'} \| sST (R'_A \| Res_{G'} \| [Text_4]) \| sS_T (R_B \| Res_G \| [Text_3])$
$Token_{AB} = [Text_7] \| R_A \| Res_G \| sS_T (R_B \| Res_G \| [Text3]) \| gsS_{AG} (R_B \| R_A \| G' \| G \| [Text6])$

گزینه ۲:

$Token_{BA} = R_A \| R_B \| [Text_9] \| gsS_{BG'} (R_A \| R_B \| G \| G' \| [Text_8])$
$Token_{TA} = Res_G \| Res_G' \| sS_T (R'_A \| R_B \| Res_G \| Res_G' \| [Text_3])$
$Token_{AB} = R'_A \| [Text_7] \| Token_{TA} \| gsS_{AG} (R_B \| R_A \| G' \| G \| [Text_6])$

مقادیر فیلدهای I_G، $I_{G'}$، Res_G، $Res_{G'}$، *Status* و *Failure* باید به شکل‌های زیر باشد:

$I_G = G$ یا $Cert_G$

$I_{G'} = G'$ یا $Cert_{G'}$

$Res_G = (Cert_G \| Status), (G \| P_G)$ یا *Failure*

$Res_{G'} = (Cert_{G'} \| Status), (G' \| P_{G'})$ یا *Failure*

Status = *True* یا *False*. مقدار این فیلد اگر گواهی کلید عمومی گروهی لغوشده شناخته شود باید *False* تنظیم شود. در غیر این صورت باید *True* تنظیم شود.

Failure: Res_G اگر کلید عمومی گروهی یا گواهی گروه کلید عمومی گروهی G نتواند با TP یافت شود به *Failure* تنظیم خواهد شد.

در سازوکار، اگر TP نگاشت بین شناسانه G و کلید عمومی گروهی P_G را بداند، باید $I_G = G$ را تنظیم کند. در غیر این صورت، باید $I_G = Cert_G$ را تنظیم کند و G باید برابر تنظیم فیلدهای هویت متمایز در $Cert_G$ تنظیم شود. اگر G یا $Cert_G$ مجاز به استفاده به عنوان یک هویت باشند، باید ابزارهایی را از پیش ترتیب دهند تا به TP اجازه تمایز دو نوع نشانه هویت را بدهند. مقدار Res_G باید با توجه به جدول ۴ مشخص شود.

جدول ۴ – مقدار Res_G

فیلد	گزینه ۱	گزینه ۲
I_G	G	$Cert_G$
Res_G	*Failure* یا $(G \mid\mid P_G)$	*Failure* یا $(Cert_G \mid\mid Status)$

سازوکار به صورت زیر انجام می‌شود:

a) B، عدد تصادفی R_B هویت G'، $I_{G'}$ و به صورت اختیاری فیلد متنی $Text_1$ را به A ارسال می‌کند.

b) A، عدد تصادفی R'_A را همراه با R_B، I_G، $I_{G'}$ و به صورت اختیاری، فیلد متنی $Text_2$ را به TP ارسال می‌کند.

c) در دریافت پیام در مرحله *b*) از A، TP مراحل زیر را انجام می‌دهد. اگر $I_G = G$ و $I_{G'} = G'$ باشد، TP، PG و $P_{G'}$ را بازیابی می‌کند؛ اگر $I_G = Cert_G$ و $I_{G'} = Cert_{G'}$ باشد، TP اعتبار $Cert_G$ و $Cert_{G'}$ را وارسی می‌کند.

d) سپس TP، $Token_{TA}$ و به صورت اختیاری فیلد متنی $Text_5$ را به A ارسال می‌کند. فیلدهای Res_G و $Res_{G'}$ در $Token_{TA}$ باید: گواهی‌های کلید عمومی G و G' و *Status* (وضعیت) آن‌ها، شناسانه‌های تمایز G و G' و کلیدهای عمومی گروهی آن‌ها یا نشانه‌ای از *Failure* (مردودی) باشد.

e) A، نشان $Token_{AB}$ و I_G را به B ارسال می‌کند.

f) در دریافت پیام در مرحله *e*) از A، B مراحل زیر را انجام می‌دهد:

۱) امضای TP در $Token_{AB}$ را با وارسی امضای TP موجود در نشان و با وارسی این که عدد تصادفی R_B، ارسال‌شده به A در مرحله *a*) مشابه عدد تصادفی R_B موجود در پیامی از TP از $Token_{AB}$ که باید امضا شود است، تصدیق می‌کند.

۲) کلید عمومی گروهی G را از پیام بازیابی می‌کند. $Token_{AB}$ را با وارسی امضای گروهی A موجود در نشان و وارسی این که مقدار فیلد شناسانه (G') در پیامی از $Token_{AB}$ که باید امضا شود برابر شناسانه G' است، تصدیق می‌کند و سپس وارسی می‌کند که عدد تصادفی R_B ارسال‌شده به A در مرحله *a*) مشابه عدد تصادفی R_B موجود در پیامی از A از $Token_{AB}$ است،

g) B، $Token_{BA}$ را به A ارسال می‌کند.

h) در دریافت پیام در مرحله *g*) از B، A مراحل زیر را انجام می‌دهد:

۱) $Token_{TA}$ را با وارسی امضای TP موجود در نشان و با وارسی این که عدد تصادفی R'_A، ارسال‌شده به TP در مرحله b) مشابه عدد تصادفی R'_A موجود در پیامی از $Token_{TA}$ که باید امضا شود است، تصدیق می‌کند.

۲) کلید عمومی گروهی G' از پیام را بازیابی می‌کند، $Token_{BA}$ را با وارسی امضای گروهی B موجود در نشان و وارسی این که مقدار فیلد شناسانه (G) در پیامی از $Token_{BA}$ که باید امضا شود برابر شناسانه G است، تصدیق می‌کند و سپس وارسی می‌کند که عدد تصادفی RA، موجود در پیامی از $Token_{BA}$ که باید امضا شود برابر عدد تصادفی R_A ارسال‌شده به B در مرحله e) است،

۸-۴ اصالت‌سنجی متقابل ناشناس یک سویه

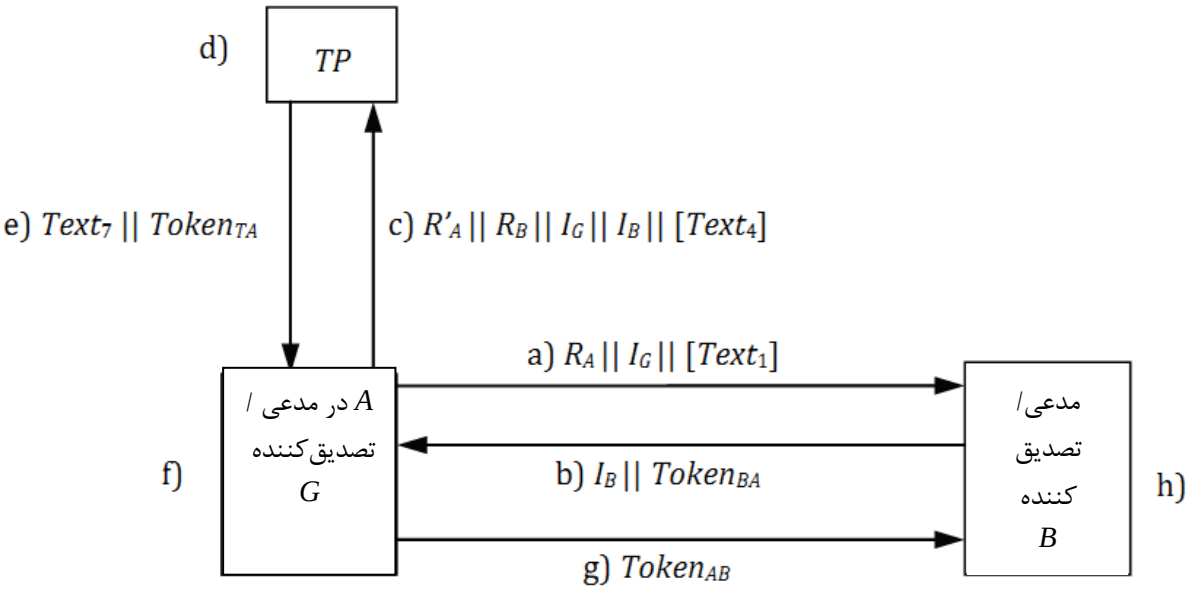
۸-۴-۱ کلیات

اصالت‌سنجی متقابل ناشناس یک سویه بدان معنی است که دو هستار ارتباطی برای یکدیگر اصالت‌سنجی شده‌اند و هویت یک هستار برای هستار دیگر ناشناس است.

۸-۴-۲ سازوکار ۲۱ - اصالت‌سنجی متقابل ناشناس یک سویه پنج مرحله‌ای شروع‌شده توسط هستار ناشناس A

در این سازوکار، هستار A در G پروتکل اصالت‌سنجی با هستار B را شروع می‌کند و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی عدد تصادفی کنترل می‌شود (به پیوست ب استاندارد ملی ایران شماره ۱-۱۰۸۲۵ سال: ۱۳۹۱ مراجعه شود)

این سازوکار اصالت‌سنجی در شکل ۱۸ نشان داده شده است.



شکل ۱۸ - اصالت‌سنجی متقابل ناشناس یک سویه پنج مرحله‌ای شروع‌شده توسط هستار ناشناس A

نشان‌ها باید با توجه به یکی از دو گزینه زیر ایجاد شود.

گزینه ۱:

$Token_{AB} = [Text_9] \,||\, Res_G \,||\, sS_T\,(R_B \,||\, Res_G \,||\, [Text_5]) \,||\, gsS_{AG}\,(R_B \,||\, R_A \,||\, B \,||\, G \,||\, [Text_8])$
$Token_{BA} = R_A \,||\, R_B \,||\, [Text_3] \,||\, sS_B\,(B \,||\, R_A \,||\, R_B \,||\, G \,||\, [Text_2])$
$Token_{TA} = Res_G \,||\, Res_B \,||\, sS_T\,(R'_A \,||\, Res_B \,||\, [Text_6]) \,||\, sS_T\,(R_B \,||\, Res_G \,||\, [\,Text_5])$

گزینه ۲:

$Token_{AB} = R_A \,||\, [Text_9] \,||\, Token_{TA} \,||\, gsS_{AG}\,(R_B \,||\, R_A \,||\, B \,||\, G \,||\, [Text_8])$
$Token_{BA} = R_A \,||\, R_B \,||\, [Text_3] \,||\, sS_B\,(B \,||\, R_A \,||\, R_B \,||\, G \,||\, [Text_2])$
$Token_{TA} = Res_G \,||\, Res_B \,||\, sS_T\,(R'_A \,||\, R_B \,||\, Res_G \,||\, Res_B \,||\, [\,Text_5])$

مقادیر فیلدهای I_G، I_B، Res_G ، Res_B، *Status* و *Failure* باید به شکل‌های زیر باشد:

G: گروهی که هستار A متعلق به آن است.

I_G= G یا $Cert_G$,G هویت

I_B= B یا $Cert_B$,Bهویت

$Res_G = (Cert_G \,||\, Status), (G \,||\, P_G)$ یا *Failure*

$Res_B = (Cert_B \,||\, Status), (B \,||\, P_B)$ یا *Failure*

Status = *True* یا *False*. مقدار فیلد اگر گواهی لغوشده شناخته شده باشد باید *False* تنظیم شود. در غیر این صورت باید *True* تنظیم شود.

Failure: اگر کلید عمومی یا گواهی G نتواند با *TP* یافت شود، Res_G، *Failure* تنظیم خواهد شد. اگر نه کلید عمومی و نه گواهی B نتواند با *TP* یافت شود، Res_Bبه *Failure* تنظیم خواهد شد.

در سازوکار، اگر *TP* نگاشت بین شناسانه G و PG را بداند، باید $I_G = G$ را تنظیم کند. در غیر این صورت، باید $I_G = Cert_G$را تنظیم کند و G باید برابر تنظیم فیلد هویت متمایز در $Cert_G$ تنظیم شود. اگر G یا $Cert_G$ مجاز به استفاده به عنوان یک هویت باشند، باید ابزارهایی را از پیش ترتیب دهند تا به *TP* اجازه تمایز دو نوع نشانه هویت را بدهند. مقدار Res_G باید با توجه به جدول ۵ مشخص شود.

در سازوکار، اگر *TP* نگاشت بین هویت B و P_Bرا بداند، باید $I_B = B$ را تنظیم کند. در غیر این صورت، باید $I_B = Cert_B$را تنظیم کند و B باید برابر تنظیم فیلد هویت متمایز در $Cert_B$ تنظیم شود. اگر B یا $Cert_B$ مجاز به استفاده به عنوان یک هویت باشند، باید ابزارهایی را از پیش ترتیب دهند تا به *TP* اجازه تمایز دو نوع نشانه هویت را بدهند. مقدار Res_Bباید با توجه به جدول ۶ مشخص شود.

جدول ۵ – مقدار Res_G

فیلد	گزینه ۱	گزینه ۲
I_G	G	$Cert_G$
Res_G	*Failure* یا $(G \,||\, P_G)$	*Failure* یا $(Cert_G \,||\, Status)$

جدول ۶ – مقدار *ResB*

فیلد	گزینه ۱	گزینه ۲
I_B	B	$Cert_B$
Res_B	*Failure* یا $(B \,||\, P_B)$	*Failure* یا $(Cert_B \,||\, Status)$

سازوکار به صورت زیر انجام می‌شود:

a) A، عدد تصادفی R_A، هویت G، I_G و به صورت اختیاری فیلد متنی $Text_1$ را به B ارسال می‌کند.

b) B، نشان $Token_{BA}$ و I_B را به A ارسال می‌کند.

c) A، عدد تصادفی R'_A همراه با R_B، I_G، I_B و به صورت اختیاری، فیلد متنی $Text_4$ را به TP ارسال می‌کند.

d) در دریافت پیام در مرحله *c*) از A، TP مراحل زیر را انجام می‌دهد. اگر $I_G = G$ و $I_B = B$ باشد، TP، P_G و P_B را بازیابی می‌کند. اگر $I_G = Cert_G$ و $I_B = Cert_B$ باشد، TP، اعتبار $Cert_G$ و $Cert_B$ را وارسی می‌کند.

e) سپس TP، $Token_{TA}$ و به صورت اختیاری فیلد متنی $Text_7$ را به A ارسال می‌کند. فیلدهای Res_G و Res_B در $Token_{TA}$ باید: گواهی‌های G و B و $Status$ (وضعیت) آن‌ها، شناسانه‌های متمایز G و B و کلیدهای عمومی آن‌ها یا نشانه‌ای از $Failure$ باشد.

f) در دریافت پیام در مرحله *e*) از TP، A مراحل زیر را انجام می‌دهد:

۱) $Token_{TA}$ را با وارسی امضای TP موجود در نشان و با وارسی این که عدد تصادفی R'_A، ارسال‌شده به TP در مرحله *c*) مشابه عدد تصادفی R'_A موجود در داده امضاشده $Token_{TA}$ است، تصدیق می‌کند.

۲) اعتبار B را با وارسی Res_B تصدیق می‌کند.

۳) کلید عمومی B از پیام را بازیابی می‌کند، $Token_{BA}$ دریافت‌شده در مرحله *b*) را با وارسی امضای ناشناس B موجود در نشان و وارسی این که مقدار فیلد شناسانه (G) در پیامی از $Token_{BA}$ که باید امضا شود برابر شناسانه G است، تصدیق می‌کند و سپس وارسی می‌کند که عدد تصادفی R_A ارسال‌شده به B در مرحله *a*) برابر عدد تصادفی R_A موجود در $Token_{BA}$ است.

g) A، $Token_{AB}$ را به B ارسال می‌کند.

h) در دریافت پیام در مرحله *g*) از A، B مراحل زیر را انجام می‌دهد:

۱) $Token_{TA}$ را با وارسی امضای TP موجود در نشان و با وارسی این که عدد تصادفی R_B، ارسال‌شده به A در مرحله *b*) مشابه عدد تصادفی R_B موجود در داده امضاشده $Token_{TA}$ است، تصدیق می‌کند.

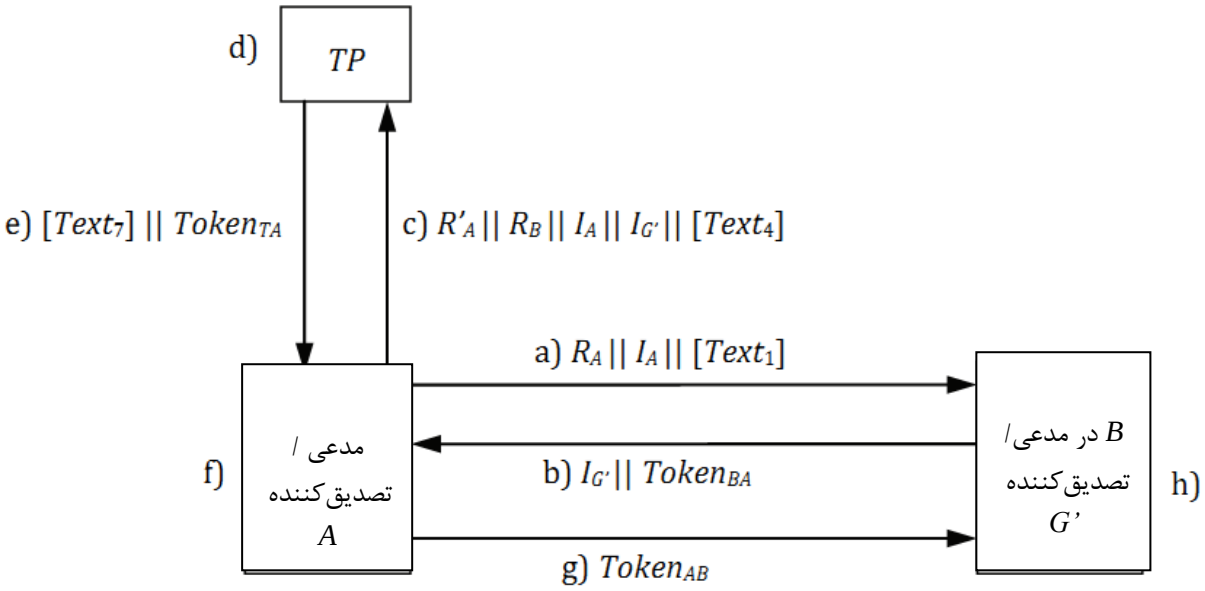
۲) اعتبار G را با وارسی Res_G تصدیق می‌کند.

۳) کلید عمومی G از پیام را بازیابی می‌کند، $Token_{AB}$ را با وارسی امضای ناشناس G موجود در نشان و وارسی این که مقدار فیلد شناسانه (B) در پیامی از $Token_{AB}$ که باید امضا شود برابر شناسانه تمایز B است، تصدیق می‌کند و سپس وارسی می‌کند که عدد تصادفی R_B موجود در داده امضاشده $Token_{AB}$ برابر عدد تصادفی R_B ارسال‌شده به A در مرحله *b*) است.

۸-۴-۳ سازوکار ۲۲ – اصالت‌سنجی متقابل ناشناس یک‌سویه پنج مرحله‌ای شروع‌شده توسط هستارهای ناشناس A و B

در این سازوکار، هستار A پروتکل اصالت‌سنجی را با هستار B در G' شروع می‌کند و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی عدد تصادفی کنترل می‌شود (به پیوست ب استاندارد ملی ایران شماره ۱-۱۰۸۲۵ سال: ۱۳۹۱ مراجعه شود)

این سازوکار اصالت‌سنجی در شکل ۱۹ نشان داده شده است.



شکل ۱۹ - اصالت‌سنجی متقابل یک‌سویه ناشناس پنج مرحله‌ای شروع‌شده توسط هستارهای ناشناس A و B

نشان‌ها باید با توجه به یکی از دو گزینه زیر ایجاد شود.

گزینه ۱:

$Token_{AB} = [Text_9] \;||\; Res_A \;||\; sS_T\,(R_B \;||\; Res_A \;||\; [Text_5]) \;||\; sS_A\,(R_B \;||\; R_A \;||\; G' \;||\; [Text_8])$
$Token_{BA} = R_A \;||\; R_B \;||\; [Text_3] \;||\; gsS_{BG'}\,(G' \;||\; R_A \;||\; R_B \;||\; [Text_2])$
$Token_{TA} = Res_A \;||\; Res_{G'} \;||\; sS_T\,(R'_A \;||\; Res_{G'} \;||\; [Text_6]) \;||\; sS_T\,(R_B \;||\; Res_A \;||\; [Text_5])$

گزینه ۲:

$Token_{AB} = R_A \;||\; [Text_9] \;||\; Token_{TA} \;||\; sS_A\,(R_B \;||\; R_A \;||\; G' \;||A \;||\; [Text_8])$
$Token_{BA} = R_A \;||\; R_B \;||\; [Text_3] \;||\; gsS_{BG}\,(G' \;||\; R_A \;||\; R_B||A \;||\; [Text_2])$
$Token_{TA} = Res_A \;||\; Res_{G'} \;||\; sS_T\,(R'_A \;||\; R_B \;||\; Res_A \;||\; Res_{G'} \;||\; [Text_5])$

مقادیر فیلدهای I_A، $I_{G'}$، Res_A، $Res_{G'}$، *Status* و *Failure* باید به شکل‌های زیر باشد:

G': گروهی که هستار B متعلق به آن است.

I_A= A یا $Cert_A$ ، A هویت

$I_{G'}$= G' یا $Cert_{G'}$ ،G'هویت

$Res_A = (Cert_A \;||\; Status), (A \;||\; P_A)$ یا *Failure*

$Res_{G'} = (Cert_{G'} \;||\; Status), (G' \;||\; P_{G'})$ یا *Failure*

Status = *True* یا *False*. مقدار این فیلد اگر گواهی لغوشده شناخته شده است باید *False* تنظیم شود. در غیر این صورت باید *True* تنظیم شود.

Failure: Res_A اگر کلید عمومی یا گواهی A نتواند توسط *TP* یافت شود، *Failure* تنظیم خواهد شد. $Res_{G'}$ اگر کلید عمومی یا گواهی G' نتواند توسط *TP* یافت شود، *Failure* تنظیم خواهد شد.

در سازوکار، اگر *TP* نگاشت بین هویت A و P_A را بداند، باید I_A= A را تنظیم کند. در غیر این صورت، باید I_A= $Cert_A$ را تنظیم کند و A باید برابر تنظیم فیلد هویت متمایز در $Cert_A$ تنظیم شود. اگر A یا $Cert_A$مجاز

به استفاده به عنوان یک هویت باشند، باید ابزارهایی را از پیش ترتیب دهند تا بـه TP اجـازه تمـایز دو نـوع نشانه هویت را بدهند. مقدار Res_A باید با توجه به جدول ۷ تعیین شود.

در سازوکار، اگر TP نگاشت بین هویت G' و $P_{G'}$ را بداند، باید $I_{G'}= G'$ را تنظیم کند. در غیر ایـن صـورت، باید $IG'= Cert_{G'}$ را تنظیم کند و G' باید برابر تنظیم فیلد هویت متمایز در $Cert_{G'}$ تنظیم شود. اگر G' یا $Cert_{G'}$ مجاز به استفاده به عنوان یک هویت باشند، باید ابزارهایی را از پیش ترتیب دهنـد تـا بـه TP اجـازه تمایز دو نوع نشانه هویت را بدهند. مقدار $Res_{G'}$ باید با توجه به جدول ۸ مشخص شود.

جدول ۷ – مقدار Res_A

فیلد	گزینه ۱	گزینه ۲
I_A	A	$Cert_A$
Res_A	$Failure$ یا $(A \,\|\|\, P_A)$	$Failure$ یا $(Cert_A \,\|\|\, Status)$

جدول ۸ – مقدار $Res_{G'}$

فیلد	گزینه ۱	گزینه ۲
$I_{G'}$	G'	$Cert_{G'}$
$Res_{G'}$	$Failure$ یا $(G' \,\|\|\, P_{G'})$	$Failure$ یا $(Cert_{G'} \,\|\|\, Status)$

سازوکار به صورت زیر انجام می‌شود:

a) A عدد تصادفی R_A، I_A، هویت A و به صورت اختیاری، فیلد متنی $Text_1$ را به B ارسال می‌کند.

b) B نشان $Token_{BA}$ و $I_{G'}$ را به A ارسال می‌کند.

c) A، عدد تصادفی R'_A، همراه با R_B، I_A، $I_{G'}$ و به صورت اختیاری، فیلد متنی $Text_4$ را به TP ارسال می‌کند.

d) در دریافت پیام در مرحله *c*) از A، TP مراحل زیر را انجام می‌دهد. اگر $I_A = A$ و $I_{G'}= G'$، TP، P_A و $P_{G'}$ را بازیابی می‌کند؛ اگر $I_A = Cert_A$ و $I_{G'} = Cert_{G'}$، TP اعتبار $Cert_A$ و $Cert_G$ را وارسی می‌کند.

e) سپس TP، $Token_{TA}$ و به صورت اختیاری فیلد متنی $Text7$ را به A ارسال می‌کنـد، فیلـد Res_A و $Res_{G'}$ در $Token_{TA}$ باید: گواهی‌های A و G و $Status$ آن‌ها، شناسانه‌های تمایز A و G' و کلیدهای عمومی آن‌ها یـا نشانه‌ای از $Failure$ باشد.

f) در دریافت پیام در مرحله *e*) از TP، A مراحل زیر را انجام می‌دهد:

۱) $Token_{TA}$ را با وارسی امضای TP موجود در نشان و با وارسی این که عدد تصادفی R'_A، ارسال‌شده به TP در مرحله *c*) مشـابه عـدد تصـادفی R'_A موجـود در داده امضاشـده $Token_{TA}$ اسـت، تصـدیق می‌کند.

۲) اعتبار G' را با وارسی $Res_{G'}$ تصدیق می‌کند.

۳) کلید عمومی G' را از پیام بازیابی می‌کند، $Token_{BA}$ دریافت‌شده در مرحله *b*) را با وارسی امضای ناشناس B موجود در نشان و وارسی این که مقدار فیلد شناسانه (A) در پیامی از $Token_{BA}$ که بایـد امضا شود برابر شناسانه تمایز A است، تصدیق می‌کند و سپس وارسی می‌کند که عدد تصـادفی R_A ارسال‌شده به B در مرحله *a*) برابر عدد تصادفی R_A موجود در $Token_{BA}$ است.

g) A، $Token_{AB}$ را به B ارسال می‌کند.

h) در دریافت پیام در مرحله g) از A، B مراحل زیر را انجام می‌دهد:

۱) $Token_{TA}$ را با وارسی امضای TP موجود در نشان و با وارسی این که عدد تصادفی R_B، ارسال‌شده به A در مرحله b) مشابه عدد تصادفی R_B موجود در داده امضاشده $Token_{TA}$ است، تصدیق می‌کند.

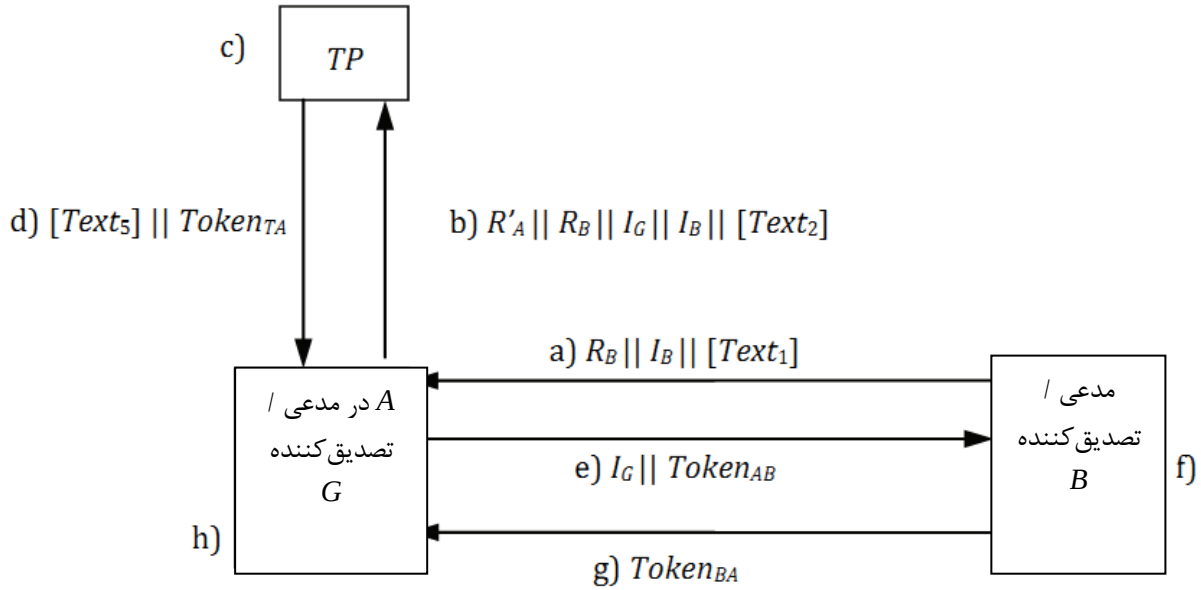
۲) اعتبار A را با وارسی Res_A تصدیق می‌کند.

۳) کلید عمومی A از پیام را بازیابی می‌کند، $Token_{AB}$ را با وارسی امضای ناشناس A موجود در نشان و وارسی این که مقدار فیلد شناسانه (G') در پیامی از $Token_{AB}$ که باید امضا شود برابر شناسانه تمایز G' است ، تصدیق می‌کند و سپس وارسی می‌کند که عدد تصادفی R_B موجود در داده امضاشده $Token_{AB}$ برابر عدد تصادفی R_B ارسال‌شده به A در مرحله b) است.

۸-۴-۴ سازوکار ۲۳ – اصالت‌سنجی متقابل ناشناس یک‌سویه پنج مرحله‌ای شروع‌شده توسط هستارهای ناشناس A و B

در این سازوکار، هستار B پروتکل اصالت‌سنجی را با هستار A در G شروع می‌کند و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی عدد تصادفی کنترل می‌شود (به پیوست ب استاندارد ملی ایران شماره ۱-۱۰۸۲۵ سال: ۱۳۹۱ مراجعه شود)

این سازوکار اصالت‌سنجی در شکل ۲۰ نشان داده شده است.



شکل ۲۰ – اصالت‌سنجی متقابل ناشناس یک سویه پنج مرحله‌ای شروع‌شده توسط هستارهای ناشناس A و B

نشان‌ها باید با توجه به یکی از دو گزینه زیر ایجاد شود.

گزینه ۱:

$Token_{AB} = R_A \,||\, [Text_7] \,||\, Res_G \,||\, sS_T\,(R_B \,||\, Res_A \,||\, [Text_3]) \,||\, gsS_{AG}\,(R_B \,||\, R_A \,||\, B \,||\, G \,||\, [Text_6])$

$Token_{BA} = R_A \,||\, R_B \,||\, [Text_9] \,||\, sS_B\,(G \,||\, R_A \,||\, R_B \,||\, B \,||\, [Text_8])$

$Token_{TA} = Res_G \,||\, Res_B \,||\, sS_T\,(R'_A \,||\, Res_B \,||\, [Text_4]) \,||\, sS_T\,(R_B \,||\, Res_G \,||\, [Text_3])$

گزینه ۲:

$Token_{AB} = R_A \,||\, [Text_7] \,||\, Token_{TA} \,||\, gsS_{AG}\,(R_B \,||\, R_A \,||\, B \,||\, G \,||\, [Text_6])$
$Token_{BA} = R_A \,||\, R_B \,||\, [Text_9] \,||\, sS_B\,(R_A \,||\, R_B \,||\, G \,||\, B \,||\, [Text_8])$
$Token_{TA} = Res_G \,||\, Res_B \,||\, sS_T\,(R'_A \,||\, R_B \,||\, Res_G \,||\, Res_B \,||\, [Text_3])$

مقادیر فیلدهای I_G، I_B، Res_G، Res_B، *Status* و *Failure* باید به شکل‌های زیر باشد:

G: گروهی که هستار A متعلق به آن است.

$I_G = G$ یا $Cert_G$, G هویت

$I_B = B$ یا $Cert_B$, B هویت

$Res_G = (Cert_G \,||\, Status), (G \,||\, PG)$ یا *Failure*

$Res_B = (Cert_B \,||\, Status), (B \,||\, PB)$ یا *Failure*

Status = *True* یا *False*. مقدار فیلد باید اگر گواهی لغوشده شناخته شده باشد، به *False* تنظیم شود. در غیر این صورت باید به *True* تنظیم شود.

Failure: Res_G اگر کلید عمومی یا گواهی G نتواند با *TP* یافت شود، باید *Failure* تنظیم شود. Res_B اگر کلید عمومی یاگواهی B نتواند با *TP* یافت شود، باید *Failure* تنظیم شود.

در سازوکار، اگر *TP* نگاشت بین هویت G و P_G را بداند، باید $I_G = G$ را تنظیم کند. در غیر این صورت، باید $I_G = Cert_G$ را تنظیم کند و G باید برابر تنظیم فیلد هویت متمایز در $Cert_G$ تنظیم شود. اگر هر دوی G یا $Cert_G$ مجاز به استفاده به عنوان یک هویت باشند، باید ابزارهایی را از پیش ترتیب دهند تا به *TP* اجازه تمایز دو نوع نشانه هویت را بدهند. مقدار Res_G باید با توجه به جدول ۹ مشخص شود.

در سازوکار، اگر *TP* نگاشت بین هویت B و P_B را بداند، باید $I_B = B$ را تنظیم کند. در غیر این صورت، باید $I_B = Cert_B$ را تنظیم کند و B باید برابر تنظیم فیلد هویت متمایز در $Cert_B$ تنظیم شود. اگر هر دوی B یا $Cert_B$ مجاز به استفاده به عنوان یک هویت باشند، باید ابزارهایی را از پیش ترتیب دهند تا به *TP* اجازه تمایز دو نوع نشانه هویت را بدهند. مقدار Res_B باید با توجه به جدول ۱۰ مشخص شود.

جدول ۹ – مقدار Res_G

فیلد	گزینه ۱	گزینه ۲
I_G	G	$Cert_G$
Res_G	*Failure* یا $(G \,||\, P_G)$	*Failure* یا $(Cert_G \,||\, Status)$

جدول ۱۰– مقدار Res_B

فیلد	گزینه ۱	گزینه ۲
I_B	B	*CertB*
Res_B	*Failure* یا $(B \,||\, P_B)$	*Failure* یا $(Cert_B \,||\, Status)$

سازوکار به صورت زیر انجام می‌شود:

a) B، عدد تصادفی R_B، I_B هویت B و به صورت اختیاری فیلد متنی $Text_1$ را به A ارسال می‌کند.

b) A، عدد تصادفی R'_A، همراه با R_B، I_G، I_B و به صورت اختیاری، فیلد متنی $Text_2$ را به *TP* ارسال می‌کند.

c) در دریافت پیام در مرحله *b*) از *A*، *TP* مراحل زیر را انجام می‌دهد. اگر $I_G = G$ و $I_B = B$ باشد، *TP*، P_G و P_B را بازیابی می‌کند. اگر $I_G = Cert_G$ و $I_B = Cert_B$ باشد، *TP* اعتبار $Cert_G$ و $Cert_B$ را وارسی می‌کند.

d) سپس *TP*، $Token_{TA}$ و به صورت اختیاری فیلد متنی $Text_5$ را به *A* ارسال می‌کند، فیلدهای Res_G و Res_B در $Token_{TA}$ باید: گواهی‌های *G* و *B* و *Status* (وضعیت) آن‌ها، شناسانه‌های تمایز *G* و *B* و کلیدهای عمومی آن‌ها یا نشانه‌ای از *Failure* باشد.

e) *A*، نشان $Token_{AB}$ و I_G را به *B* ارسال می‌کند.

f) در دریافت پیام در مرحله *e*) از *B*، *A* مراحل زیر را انجام می‌دهد:

۱) امضای *TP* در $Token_{AB}$ را با وارسی امضای *TP* موجود در نشان و با وارسی این که عدد تصادفی R_B ارسال‌شده به *A* در مرحله *a*) مشابه عدد تصادفی R_B موجود در داده‌های امضاشده *TP* از $Token_{AB}$ است، تصدیق می‌کند.

۲) اعتبار *G* را با وارسی Res_G تصدیق می‌کند.

۳) کلید عمومی *G* از پیام را بازیابی می‌کند، $Token_{AB}$ را با وارسی امضای ناشناس *A* موجود در نشان و وارسی این که مقدار فیلد شناسانه (*B*) در پیامی از $Token_{AB}$ که باید امضا شود برابر شناسانه تمایز *B* است، تصدیق می‌کند و سپس وارسی می‌کند که عدد تصادفی R_B ارسال‌شده به *A* در مرحله *a*) مشابه عدد تصادفی R_B موجود در داده امضاشده $Token_{BA}$ است.

g) *B*، $Token_{BA}$ را به *A* ارسال می‌کند.

h) در دریافت پیام در مرحله *g*) از *B*، *A* مراحل زیر را انجام می‌دهد:

۱) $Token_{TA}$ را با وارسی امضای *TP* موجود در این نشان و با وارسی این که عدد تصادفی R'_A ارسال‌شده به *TP* در مرحله *b*) مشابه عدد تصادفی R'_A موجود در داده‌های امضاشده $Token_{TA}$ است، تصدیق می‌کند.

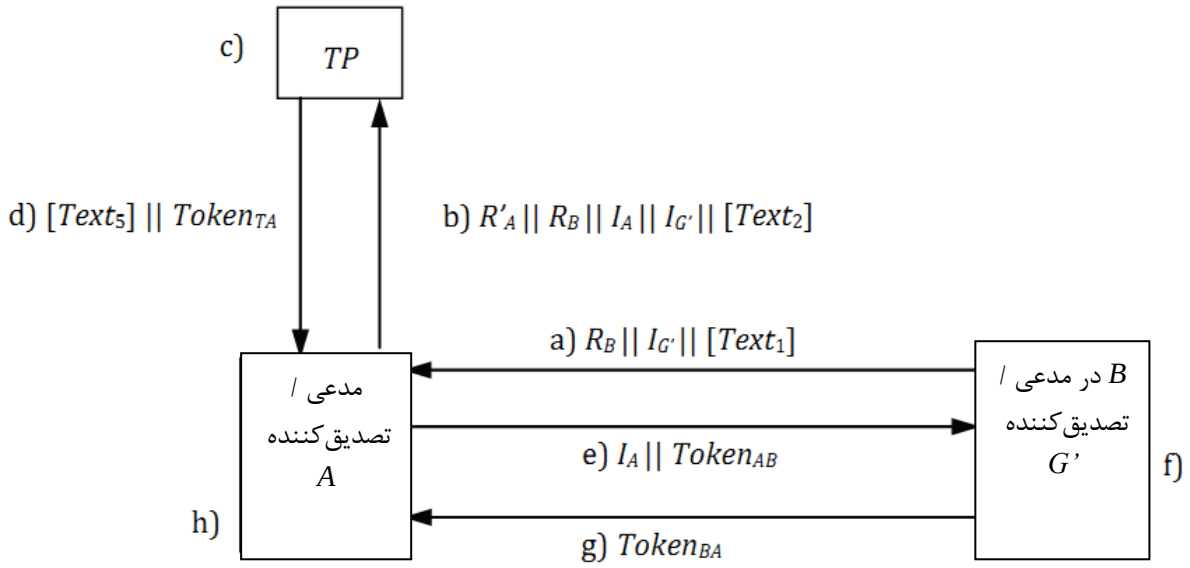
۲) اعتبار *B* را با وارسی Res_B تصدیق می‌کند.

۳) کلید عمومی *B* از پیام را بازیابی می‌کند، $Token_{BA}$ را با وارسی امضای ناشناس *B* موجود در نشان و وارسی این که مقدار فیلد شناسانه (*G*) در پیامی از $Token_{BA}$ که باید امضا شود برابر شناسانه تمایز *G* است و سپس وارسی این که عدد تصادفی R_A موجود در داده امضاشده $Token_{AB}$ برابر عدد تصادفی R_A ارسال‌شده به *B* در مرحله *e*) است، تصدیق می‌کند.

۸-۴-۵ سازوکار ۲۴ - اصالت‌سنجی متقابل یک‌سویه ناشناس پنج مرحله‌ای شروع‌شده توسط هستار ناشناس *B*

در این سازوکار، هستار *B* در G' پروتکل اصالت‌سنجی با هستار *A* را شروع می‌کند و منحصر به فردی/ به‌هنگام بودن با تولید و وارسی عدد تصادفی کنترل می‌شود (به پیوست ب استاندارد ISO/IEC 9798-1: 2010 مراجعه شود)

این سازوکار اصالت‌سنجی در شکل ۲۱ نشان داده شده است.



شکل ۲۱ - اصالت‌سنجی متقابل یک‌سویه ناشناس پنج مرحله‌ای شروع‌شده توسط هستار ناشناس B

نشان‌ها باید با توجه به یکی از دو گزینه زیر ایجاد شود.

گزینه ۱:

$Token_{AB} = [Text_7] \,||\, R_A \,||\, Res_A \,||\, sS_T\,(R_B \,||\, Res_A \,||\, [Text_3]) \,||\, sS_A\,(R_B \,||\, R_A \,||\, G' \,||\, [Text_6])$

$Token_{BA} = R_A \,||\, R_B \,||\, [Text_9] \,||\, gsS_{BG'}\,(A \,||\, R_A \,||\, R_B \,||\, G' \,||\, [Text_8])$

$Token_{TA} = Res_A \,||\, Res_{G'} \,||\, sS_T\,(R'_A \,||\, Res_{G'} \,||\, [Text_4]) \,||\, sS_T\,(R_B \,||\, Res_A \,||\, [Text_3])$

گزینه ۲:

$Token_{AB} = R_A \,||\, [Text_7] \,||\, Token_{TA} \,||\, sS_A\,(R_B \,||\, R_A \,||\, G' \,||\, A||\, [Text_6])$

$Token_{BA} = R_A \,||\, R_B \,||\, [Text_9] \,||\, gsS_{BG'}\,(R_A \,||\, R_B \,||A \,||\, G' \,||\, [Text_8])$

$Token_{TA} = Res_A \,||\, Res_{G'} \,||\, sS_T\,(R'_A \,||\, R_B \,||\, Res_A \,||\, Res_{G'} \,||\, [Text_3])$

مقادیر فیلدهای I_A، I_G، $ResA$، $Res_{G'}$ ، $Status$ و $Failure$ باید به شکل‌های زیر باشد:

G' : گروهی که هستار B متعلق به آن است.

$I_A = A$ یا $Cert_A$, A هویت

$I_{G'} = G'$ یا $Cert_{G'}$, G' هویت

$Res_A = (Cert_A \,||\, Status), (A \,||\, P_A)$ یا $Failure$

$Res_{G'} = (Cert_{G'} \,||\, Status), (G' \,||\, P_{G'})$ یا $Failure$

$Status = True$ یا $False$. مقدار فیلد باید اگر گواهی لغوشده شناخته شده باشد $False$ تنظیم شود. در غیر این صورت باید $True$ تنظیم شود.

$Failure$: Res_A اگر کلید عمومی یا گواهی A نتواند با TP یافت شود، باید $Failure$ تنظیم شود. $Res_{G'}$ اگر کلید عمومی یا گواهی G' نتواند با TP یافت شود، باید $Failure$ تنظیم شود.

در سازوکار، اگر TP نگاشت بین هویت A و P_A را بداند، باید $I_A = A$ را تنظیم کند. در غیر این صورت، باید $I_A = Cert_A$ را تنظیم کند و A باید برابر تنظیم فیلد هویت متمایز در $Cert_A$ تنظیم شود. اگر هر دوی A یا

$Cert_A$ مجاز به استفاده به عنوان یک هویت باشند، باید ابزارهایی را از پیش ترتیب دهند تا به TP اجازه تمایز دو نوع نشانه هویت را بدهند. مقدار Res_A باید با توجه به جدول ۱۱ مشخص شود.

در سازوکار، اگر TP نگاشت بین هویت G' و $P_{G'}$ را بداند، باید $I_{G'} = G'$ را تنظیم کند. در غیر این صورت، باید $I_{G'} = Cert_{G'}$ را تنظیم کند و G' باید برابر تنظیم فیلد هویت متمایز در $Cert_{G'}$ تنظیم شود. اگر هر دوی G' یا $Cert_{G'}$ مجاز به استفاده به عنوان یک هویت باشند، باید ابزارهایی را از پیش ترتیب دهند تا به TP اجازه تمایز دو نوع نشانه هویت را بدهند. مقدار $Res_{G'}$ باید با توجه به جدول ۱۲ مشخص شود.

جدول ۱۱ – مقدار Res_A

فیلد	گزینه ۱	گزینه ۲
I_A	A	$Cert_A$
Res_A	$(A \mid\mid P_A)$ یا $Failure$	$(Cert_A \mid\mid Status)$ یا $Failure$

جدول ۱۲ – مقدار $Res_{G'}$

فیلد	گزینه ۱	گزینه ۲
$I_{G'}$	G'	$Cert_{G'}$
$Res_{G'}$	$(G' \mid\mid P_{G'})$ یا $Failure$	$(Cert_{G'} \mid\mid Status)$ یا $Failure$

سازوکار به صورت زیر انجام می‌شود:

a) B، عدد تصادفی R_B، هویت $I_{G'}$، G' و به صورت اختیاری فیلد متنی $Text_1$ را به A ارسال می‌کند.

b) A عدد تصادفی R'_A، همراه با R_B، I_A، $I_{G'}$ و به صورت اختیاری، فیلد متنی $Text_2$ را به TP ارسال می‌کند.

c) در دریافت پیام در مرحله *b*) از A، TP مراحل زیر را انجام می‌دهد. اگر $I_A = A$ و $I_{G'} = G'$ باشد، TP، P_A و $P_{G'}$ را بازیابی می‌کند؛ اگر $I_A = Cert_A$ و $I_{G'} = Cert_{G'}$ باشد، TP اعتبار $Cert_A$ و $Cert_{G'}$ را وارسی می‌کند.

d) سپس TP، $Token_{TA}$ و به صورت اختیاری فیلد متنی $Text_5$ را به A ارسال می‌کند، فیلدهای Res_A و $Res_{G'}$ در $Token_{TA}$ باید: گواهی‌های A و G' و $Status$ آن‌ها، شناسانه‌های تمایز A و G' و کلیدهای عمومی آن‌ها یا نشانه‌ای از $Failure$ باشد.

e) A، $Token_{AB}$ و I_A را به B ارسال می‌کند.

f) در دریافت پیام در مرحله *e*) از A، B مراحل زیر را انجام می‌دهد:

۱) امضای TP در $Token_{AB}$ را با وارسی امضای TP موجود در نشان و با وارسی این که عدد تصادفی R_B، ارسال‌شده به A در مرحله *a*) مشابه عدد تصادفی R_B موجود در داده امضاشده TP، $Token_{AB}$ است، تصدیق می‌کند.

۲) اعتبار A را با وارسی Res_A تصدیق می‌کند.

۳) کلید عمومی A را از پیام بازیابی می‌کند، $Token_{AB}$ را با وارسی امضای ناشناس A موجود در نشان و وارسی این که مقدار فیلد شناسانه (G') در پیامی از $Token_{AB}$ که باید امضا شود برابر شناسانه تمایز G' است، تصدیق می‌کند و سپس وارسی می‌کند که عدد تصادفی R_B ارسال‌شده به A در مرحله *a*) مشابه عدد تصادفی R_B موجود در داده امضاشده A، $Token_{AB}$ است.

g) B، $Token_{BA}$ را به A ارسال می‌کند.

h) در دریافت پیام در مرحله g) از B، A مراحل زیر را انجام می‌دهد:

۱) $Token_{TA}$ را با وارسی امضای TP موجود در نشان و با وارسی این که عدد تصادفی R'_A، ارسال‌شده به TP در مرحله b) مشابه عدد تصادفی R'_A موجود در داده امضاشده $Token_{TA}$ است، تصدیق می‌کند.

۲) اعتبار G' را با وارسی $Res_{G'}$ تصدیق می‌کند.

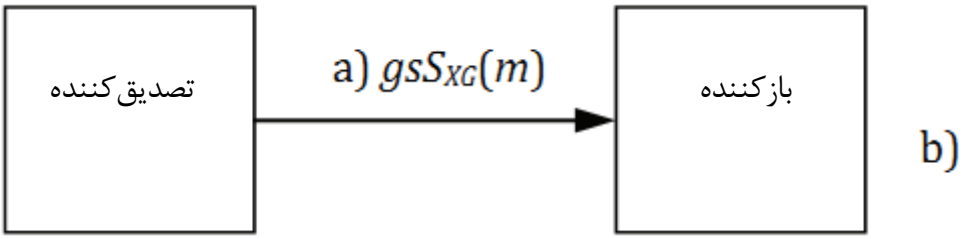
۳) کلید عمومی G' از پیام را بازیابی می‌کند، $Token_{BA}$ را با وارسی امضای ناشناس B موجود در نشان و وارسی این که مقدار فیلد شناسانه (A) در پیامی از $Token_{BA}$ که باید امضا شود برابر شناسانه تمایز A است و سپس وارسی این که عدد تصادفی R_A موجود در داده امضاشده $Token_{BA}$ برابر عدد تصادفی R_A ارسال‌شده به B در مرحله e) است، تصدیق می‌کند.

۹ فرآیند بازکردن عضویت گروهی

۹-۱ کلیات

این فرایند اختیاری است. فرآیند بازکردن درصورتی که طرح امضای گروهی استفاده‌شده از باز کردن پشتیبانی کند، امکان‌پذیر است. فرآیند بازکردن توسط بازکننده‌ای که دارای یک کلید بازکردن است، اجرا می‌شود. منظور از فرآیند بازکردن، آشکار کردن شناسانه تمایز هستاری است که امضای گروهی داده‌شده را تولید می‌کند. اگر اصالت‌سنجی ناشناس از فرآیند بازکردن پشتیبانی کند، نیمه اصالت‌سنجی ناشناس[1] نامیده می‌شود.

یادآوری- اطلاعات مربوط به فرآیند بازکردن می‌تواند در فیلد متنی گنجانده شود.



شکل ۲۲ - فرآیند بازکردن

این فرایند شامل مراحل a) و b) است که در شکل ۲۲ نشان داده شده است. این فرآیند امضای گروهی، کلید بازکردن عضویت گروهی، کلید عمومی گروهی و پارامترهای عمومی گروهی را به عنوان ورودی می‌گیرد و شناسانه تمایز را بر می‌گرداند. به صورت اختیاری، می‌تواند *شواهد انقیاد*[2] را نیز بازگرداند.

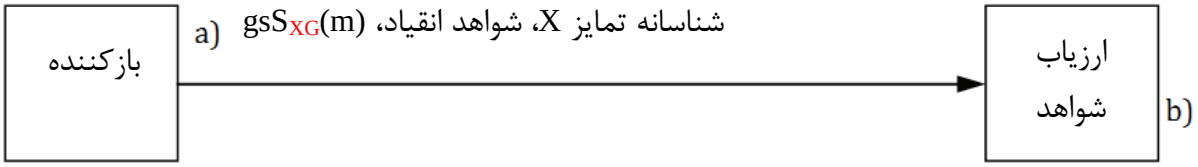
1 - Partially anonymous authentication
2 - Evidence of binding

a) تصدیق‌کننده، امضای گروهی دریافت‌شده ناشناس $gsS_{XG}(m)$ را از مدعی X در G به بازکننده ارسال می‌کند.

b) بازکننده، شناسانه تمایز را با استفاده از کلید باز کردن عضویت گروهی پیدا می‌کند. به صورت اختیاری می‌تواند *شواهد انقیاد* را نیز خروجی دهد.

۹-۲ فرآیند ارزیابی شواهد

این فرایند اختیاری است. فرآیند ارزیابی شواهد توسط ارزیاب شواهد اجرا می‌شود که هدف آن وارسی این موضوع است که امضا داده‌شده توسط امضاکننده خاص ایجاد شده یا خیر.



شکل ۲۳ - فرآیند ارزیابی شواهد

این فرایند شامل مراحل *a*) و *b*) است که در شکل ۲۳ نشان داده شده است. این فرآیند *شواهد انقیاد*، امضای گروهی و شناسانه تمایز را به عنوان ورودی می‌گیرد و اعتبار امضاکننده را بازمی‌گرداند.

a) بازکننده، شناسانه تمایز X، *شواهد انقیاد* و امضای گروهی $gsS_{XG}(m)$ دریافت‌شده ناشناس را از مدعی X در G به ارزیاب شواهد ارسال می‌کند.

b) ارزیاب شواهد تعیین می‌کند که این شواهد معتبر هستند یا خیر.

۱۰ فرآیند پیونددادن امضای گروهی

۱-۱۰ کلیات

فرآیند پیونددادن توسط پیونددهنده برای گروه اجرا می‌شود، که مجاز به اتصال چند امضای گروهی برای گروه امضاشده توسط امضاکننده مشابه است.

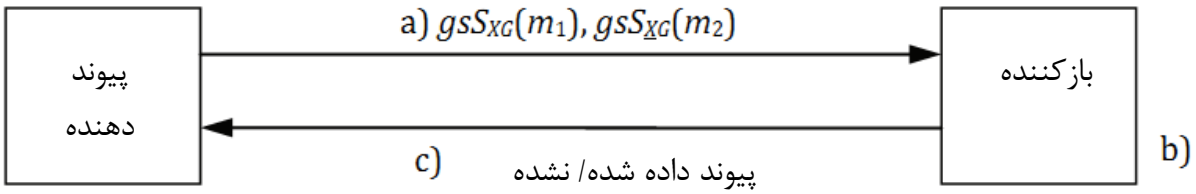
این فرایند به صورت اختیاری برای پیونددهنده‌ای که می‌خواهد بداند که امضاهای گروهی داده‌شده مشابه کاربر ناشناس است یا خیر، استفاده می‌شود. اگر امضاهای گروهی داده‌شده از یک کاربر ناشناس مشابه باشد، امضاهای گروهی پیوند داده می‌شوند، اگر نه، امضاهای گروهی پیوند داده نمی‌شوند.

یادآوری- اطلاعات مربوط به فرآیند پیونددادن می‌تواند در فیلد متنی گنجانده شود.

۲-۱۰ فرآیند پیونددادن با بازکننده

برای این فرآیند، امضا گروهی باید از قابلیت بازکردن پشتیبانی کند که در آن بازکننده می‌تواند امضاکننده امضای گروهی داده‌شده را شناسایی کند.

این فرآیند شامل پیونددهنده‌ای است که توسط بازکننده اطلاع یافته است که دو امضای گروهی پیوند داده شده اند یا خیر.



شکل ۲۴ - فرآیند پیونددادن با بازکننده

این فرایند شامل مراحل *a*) تا *c*) است که در شکل ۲۴ نشان‌داده‌شده است. این فرآیند پس از اصالت‌سنجی انجام می‌شود و به شرح زیر ادامه می‌یابد:

a) پیونددهنده $gsS_{XG}(m_1)$ و $gsS_{\underline{X}G}(m_2)$ را به بازکننده ارسال می‌کند، که هستار X و $\underline{X}$ ممکن است هستارهای مشابه یا غیرمشابه باشند.

b) بازکننده با مقایسه شناسانه‌های تمایز امضاهای گروهی، وارسی می‌کند که آیا دو امضای گروهی برای اصالت‌سنجی از مدعی مشابه است یا خیر.

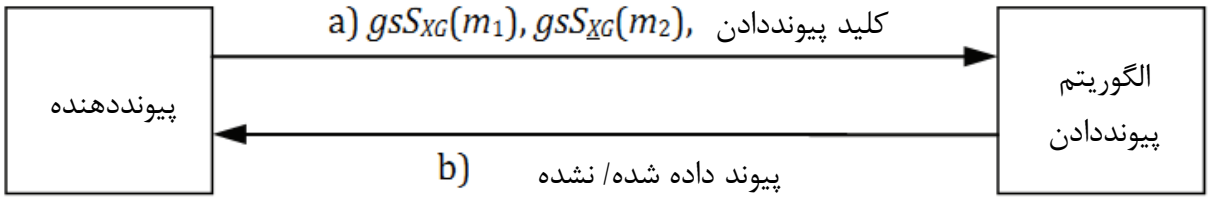
c) بازکننده به پیونددهنده پاسخ می‌دهد که امضاهای گروهی پیوند داده شده است یا خیر.

۳-۱۰ فرآیند پیونددادن با کلید پیونددادن

برای امکان‌پذیر بودن این فرآیند، طرح امضای گروه استفاده‌شده باید از قابلیت پیونددادن پشتیبانی کند که پیونددهنده بتواند تعیین کند امضاهای گروهی داده‌شده بدون ارتباط با بازکننده پیوند داده شده است یا خیر (برای جزئیات بیشتر به شماره [۹] کتابنامه مراجعه شود).

در این فرایند، تصدیق‌کننده باید پیونددهنده‌ای باشد که دارای کلید پیونددادن برای قابلیت پیونددادن محلی است.

از طریق این فرایند، پیونددهنده می‌تواند بداند که دو جفت امضاهای گروهی داده‌شده با استفاده از کلید پیونددادن، پیوند داده شده است یا خیر.



شکل ۲۵ - فرآیند پیونددادن با کلید پیونددادن

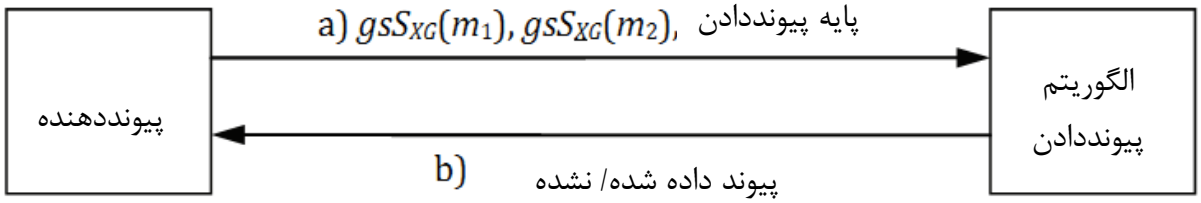
این فرایند شامل مراحل *a*) و *b*) است که در شکل ۲۵ نشان‌داده‌شده است. این فرآیند پس از فرآیند اصالت‌سنجی انجام می‌شود و به شرح زیر ادامه می‌یابد:

a) پیونددهنده الگوریتم پیونددادن را با $gsS_{XG}(m_1)$، $gsS_{\underline{X}G}(m_2)$، کلید پیونددادن و پارامترهای عمومی گروهی به عنوان ورودی فرا می‌خواند، که در آن هستار X و $\underline{X}$ ممکن است ممکن است هستارهای مشابه یا غیرمشابه باشند.

b) الگوریتم پیونددادن به پیونددهنده خروجی می‌دهد که امضاهای گروهی پیوند داده شده است یا خیر.

۴-۱۰ فرآیند پیونددادن با پایه پیونددادن

برای امکان‌پذیر بودن این فرآیند، طرح امضای گروهی مورد استفاده باید از قابلیت پیونددادن پشتیبانی کند که در آن امضاهای ایجادشده توسط امضاکننده با استفاده از پایه پیوندادن قابل پیوند هستند، اما با امضاکننده متفاوت یا با استفاده از پایه پیونددادن متفاوت قابل پیوند نیستند. برای فعال کردن قابلیت پیونددادن، تصدیق‌کننده به ارسال پایه پیونددادن به مدعی به عنوان بخشی از متن اختیاری در پروتکل‌های اصالت‌سنجی هستار ناشناس نیاز دارد. مدعی از پایه پیونددادن و همچنین کلید خصوصی عضو گروه خود برای ایجاد امضای گروهی استفاده می‌کند. الگوریتم پیوند به هیچ کلید پیونددادنی بستگی ندارد و می‌تواند توسط هر هستاری اجرا شود. از طریق فرآیند پیونددادن، پیونددهنده می‌تواند بداند که دو یا چند جفت امضاهای گروهی ارائه‌شده پیوند داده شده است یا خیر (برای جزئیات بیشتر به شماره [۸] کتابنامه مراجعه شود)



شکل ۲۶ - فرآیند پیونددادن با پایه پیونددادن

این فرایند شامل مراحل *a*) و *b*) است، در شکل ۲۶ نشان داده شده است. این فرایند پس از اصالت‌سنجی انجام می‌شود و به شرح زیر ادامه می‌یابد:

a) پیونددهنده الگوریتم پیونددادن را با $gsS_{XG}(m_1)$، $gsS_{\underline{X}G}(m_2)$، پایه پیونددادن و پارامترهای عمومی گروهی به عنوان ورودی فرا می‌خواند، که در آن هستار X و $\underline{X}$ ممکن است هستار مشابه یا غیر مشابه باشد.

b) الگوریتم پیونددادن به پیونددهنده خروجی می‌دهد که امضاها پیوند داده شده است یا خیر.

پیوست الف

(الزامی)

شناسانه‌های شی

این پیوست شناسانه‌های شی تخصیص‌یافته به سازوکارهای اصالت‌سنجی ناشناس مشخص‌شده در این استاندارد ملی را فهرست می‌کند.

```
AnonymousEntityAuthenticationMechanisms-2 {
 iso(1)         standard(0)         anonymous-entity-authentication-
mechanisms(20009) part2(2)
 asn1-module(0) object-identifiers(0) }
 DEFINITIONS EXPLICIT TAGS ::= BEGIN
 -- EXPORTS All; --
 -- IMPORTS None; --
 OID ::= OBJECT IDENTIFIER -- alias
 -- Synonyms --
 Is20009-2   OID   ::=   {   iso(1)   standard(0)   anonymous-entity-
authentication-mechanisms (20009)
part2(2) }
 mechanism OID ::= { is20009-2 mechanisms(2) }
 -- mechanisms not involving a trusted third party --
 anony-ua-one-pass OID ::= { mechanism 1 }
 anony-ua-two-pass OID ::= { mechanism 2 }
 anony-ma-two-pass OID ::= { mechanism 3 }
 anony-ma-three-pass OID ::= { mechanism 4 }
 anony-ma-two-pass-Parallel OID ::= { mechanism 5 }
 uni-anony-ma-two-pass OID ::= { mechanism 6 }
 uni-anony-ma-three-pass OID ::= { mechanism 7 }
 uni-anony-ma-two-pass-Parallel OID ::= { mechanism 8 }
 anony-ma-three-pass-bind-sig-later OID ::= { mechanism 9 }
 anony-ma-three-pass-bind-sig-first OID ::= { mechanism 10 }
 anony-ma-two-pass-Parallel-bind-sig-later OID ::= { mechanism 11 }
 anony-ma-two-pass-Parallel-bind-sig-first OID ::= { mechanism 12 }
 anony-uni-anony-ma-three-pass-bind-sig-later OID ::= { mechanism 13
}
 anony-uni-anony-ma-three-pass-bind-sig-first OID ::= { mechanism 14
}
 anony-uni-anony-ma-two-pass-Parallel-bind-sig-later   OID   ::=   {
mechanism 15 }
 anony-uni-anony-ma-two-pass-Parallel-bind-sig-first   OID   ::=   {
mechanism 16 }
 -- mechanisms involving a trusted third party –
ttp-anony-ua-four-pass-by-A OID ::= { mechanism 17 }
 ttp-anony-ua-four-pass-by-B OID ::= { mechanism 18 }
 ttp-anony-ma-five-pass-by-A OID ::= { mechanism 19 }
 ttp-anony-ma-five-pass-by-B OID ::= { mechanism 20 }
 ttp-uni-anony-ma-five-pass-by-A-A OID ::= { mechanism 21 }
 ttp-uni-anony-ma-five-pass-by-A-B OID ::= { mechanism 22 }
 ttp-uni-anony-ma-five-pass-by-B-A OID ::= { mechanism 23 }
```

```
ttp-uni-anony-ma-five-pass-by-B-B OID ::= { mechanism 24 }
END -- AnonymousEntityAuthenticationMechanisms- 2 -
```

پیوست ب

(اطلاعاتی)

اطلاعات در مورد سازوکارها با خصوصیت انقیاد

این پیوست، لزوم خصوصیت انقیاد در فرانامه‌های[1] استفاده معین را توضیح می‌دهد و همچنین شامل راهنمایی در مورد انتخاب پارامتر است.

ابتدا، سه نمونه از حمله انقیاد نادرست توضیح داده شده است.

مثال ۱ در سازوکار ۴ بند ۷-۳-۳، هستار B، پروتکل اصالت‌سنجی با هستار A با ارسال پیام $R_B \,||\, [Text_1]$ شروع می‌کند. هستار A با پیام $Token_{AB} \,||\, [Cert_G]$ پاسخ می‌دهد. اکنون هستار متفاوت B' در گروه مشابه B است که می‌تواند پیام $Token_{BA} \,||\, [Cert_{G'}]$ را برای هستار A بدون این که شناسایی شود تولید کند. بنابراین، A، B' را اصالت‌سنجی می‌کند اما هستار B که پروتکل را شروع کرده، اصالت‌سنجی نمی‌کند.

مثال ۲ در سازوکار ۵ بند ۷-۳-۴، هستار A، $R_A \,||\, [Cert_G] \,||\, [Text1]$ را به هستار B ارسال می‌کند و به صورت موازی، هستار B، $R_B \,||\, [Cert_{G'}] \,||\, [Text_2]$ را به هستار A ارسال می‌کند. اکنون هستار متفاوت B' در گروه مشابه B است که می‌تواند پیام $Token_{BA}$ را برای هستار A بدون این که شناسایی شود، تولید کند. بنابراین، A، B' را اصالت‌سنجی می‌کند اما هستار B که اولین پیام پروتکل را ارسال کرده، اصالت‌سنجی نمی‌کند.

مثال ۳ در سازوکار ۴ بند ۷-۳-۳، هستار B از G' پروتکل اصالت‌سنجی را با هستار A توسط ارسال پیام $R_B \,||\, [Text_1]$ شروع می‌کند. هستار A با پیام $Token_{AB} \,||\, [Cert_G]$ پاسخ می‌دهد. اگر G' در $Token_{AB}$ گنجانده نشده باشد، هستار متفاوت B' از گروه متفاوت G'' می‌تواند پیام نهایی را جایگزین کند و $[Cert_{G''}] \,||$ $Token_{BA}$ را به هستار A بدون این که شناسایی شود، ارسال کند. بنابراین، A، B' را اصالت‌سنجی می‌کند اما هستار B که پروتکل را شروع کرده را اصالت‌سنجی نمی‌کند.

در تمام مثال‌های بالا، در پایان پروتکل، هستار B، هستار A را اصالت‌سنجی می‌کند، در حالی که هستار A، هستار متفاوت B' را به جای هستار B که اولین پیام را ارسال کرده، اصالت‌سنجی می‌کند. در آخرین مثال بالا، هستار ممکن است هر چیزی که توسط B ارسال شده را (بر اساس نشانی یا محل B) که از عضوی در G'' می‌آید، در نظر گیرد، با این حال B در واقع عضوی از G' است. این حمله انقیاد نادرست، یکپارچگی پروتکل اصالت‌سنجی را تغییر می‌دهد. حمله امکان‌پذیر است چرا که هیچ انقیادی بین پیام‌های پروتکلی که توسط یک هستار ارسال می‌شود، وجود ندارد.

نوع دیگری از حمله انقیاد نادرست در سازوکار ۴ به شرح زیر است.

مثال ۴ در سازوکار ۴، هستار B، پروتکل اصالت‌سنجی با هستار A را با ارسال پیام $R_B \,||\, [Text_1]$ شروع می‌کند. هستار A با پیام $Token_{AB} \,||\, [Cert_G]$ پاسخ می‌دهد. هستار B، $Token_{BA} \,||\, [Cert_{G'}]$ را به عنوان

1 - Senarios

پیام نهایی ارسال می‌کند. اکنون هستار متفاوت B' در گروه مشابه B است که می‌تواند پیام نهایی را رهگیری کند و امضای گروهی $gsS_{BG'}$ $(R_B \,||\, R_A \,||\, [G] \,||\, [Text_4])$ در $Token_{BA}$ را با استفاده از امضای خود جایگزین کند. در پایان، پروتکل اصالت‌سنجی موفق خواهد بود. با این حال، هستار A، هستار B را با استفاده از امضایی از هستار B' اصالت‌سنجی می‌کند. چنین حمله‌ای برای سازوکارهای اصالت‌سنجی متعارف با امضاهای متعارف ممکن نیست، از آنجا که هستار A بلافاصله چنین جایگزینی تشخیص خواهد داد.

در مثال بالا، حمله انقیاد نادرست ممکن است مسئله نباشد و ممکن است برای هستار A مهم نباشد که A هستار B یا هستار B' را اصالت‌سنجی کرده است یا خیر. شاید A تنها اهمیت دهد که آیا عضوی از G' را اصالت‌سنجی کرده است یا خیر. با این حال، در برخی فرانامه‌های استفاده، چنین حمله انقیاد نادرستی ممکن است نگرانی تلقی شود. به طور مثال، اگر سازوکار امضای دیجیتال (رقمی) ناشناس استفاده‌شده در پروتکل اصالت‌سنجی قابلیت بازکردن داشته باشد، هستار A ممکن است تمام امضاهای گروهی که برای بازکننده به صورت دوره‌ای جمع آوری کرده است را اگر گرفتن برخی آمارها مجاز باشد، ارسال کند، به طور مثال این که هستار چند بار اصالت‌سنجی شده است. هستار A می‌تواند آمارهای کاملا اشتباهی در چنین حمله انقیاد نادرستی ارائه دهد.

خصوصیت انقیاد پروتکل اصالت‌سنجی هستار، خصوصیتی است که اطمینان حاصل شود تمام پیام‌ها از یک هستار ارتباطی با یکدیگر مرتبط شده‌اند. اگر یکی از پیام‌ها یا بخشی از پیام اصلاح یا جایگزین شده است، چنین اصلاحی می‌تواند با پروتکل شناسایی شود. بنابراین خصوصیت انقیاد تضمین بالاتری در مورد یکپارچگی پروتکل اصالت‌سنجی ارائه می‌دهد. برای رسیدن به خصوصیت انقیاد، اغلب اوقات، فن توافق کلید دیفی- هلمن استفاده می‌شود. هدف دیفی- هلمن برای مدیریت کلید بین دو هستار پروتکل نیست، بلکه برای اطمینان از یکپارچگی پیام‌های پروتکل است.

در سازوکارهایی با خصوصیت انقیاد در بند ۷-۵ و ۷-۶، گروه دوری $\boldsymbol{G}$، q ترتیبی که در آن مسئله DDH دشوار است و تولیدکننده g از G توسط هستار A و B انتخاب می‌شود. دو مثال از انتخاب $\boldsymbol{G}$ و g به شرح زیر توصیف می‌شود.

- سازوکار متعارف: عدد اول بزرگ p و q را انتخاب می‌کند به طوری که $p - 1$ مضربی از q است. G به عنوان زیرگروه q ترتیبی، ZP^* تعریف می‌شود. g، عددی که ضرب پیمانه‌ای p آن q است، انتخاب می‌شود.

برای اطلاعات بیشتر به استاندارد ISO/IEC 11770-3 [6] مراجعه شود. برای محاسبه g^a در سازوکارهای بند ۷-۵ و ۷-۶، g^a پیمانه p محاسبه شود.

- سازوکار بر اساس منحنی بیضوی: گروه منحنی بیضوی G از q ترتیبی نخست و تولیدکننده نقطه g انتخاب شود، برای اطلاعات در مورد تولید منحنی بیضوی به ISO/IEC 15946-1 [7] مراجعه شود. برای محاسبه g^a در سازوکارهای بند ۷-۵ و ۷-۶، ضرب نقطه‌ای $g[a]$ محاسبه شود.

کتابنامه

[1] ISO/IEC 8825-1:2008, Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) — Part 1

[2] ISO/IEC 9797-1:2011, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher

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

[4] ISO/IEC 9798-3:1998, Information technology — Security techniques — Entity authentication — Part 3: Mechanisms using digital signature techniques

[5] ISO/IEC 11770-1:2010, Information technology — Security techniques — Key management — Part 1: Framework

[6] ISO/IEC 11770-3:2008, Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques

[7] ISO/IEC 15946-1:2008, Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 1: General

[8] Brickell E., & Li J. A pairing-Based DAA scheme further reducing TPM resources, TRUST 2010 (LNCS 6101), pp. 181-195, 2010

[9] Hwang J. , Lee S. , Chung B. , Cho H. , Nyang D. Short Group Signatures with Controllable Likability, L IGHTSEC 2011, pp. 44–52, 2011

[10] Hwang J., Eom S., Chang K., Lee P., Nyang D. Anonymity-Based authenticated key Agreement with binding properties, WISA 2012, pp. 177–191, 2012

[11] Walker J., & Li J. Key Exchange with Anonymous Authentication using DAA-S IGMA Protocol, Proc. of 2nd International Conference on Trusted Systems (LNCS 6802), pp. 108–127, 2010