INSO
18722-1
1st. Edition
2015

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

استاندارد ملی ایران
۱۸۷۲۲-۱
چاپ اول
۱۳۹۴

فناوری اطلاعات- فنون امنیتی- امضاهای رقمی (دیجیتالی) ناشناس
قسمت ۱: کلیات

Information technology - Security techniques Anonymous digital signatures - Part 1: General

ICS: 35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2 - International Electrotechnical Commission
3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات- فنون امنیتی- امضاهای رقمی (دیجیتالی) ناشناس - قسمت ۱: کلیات»

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
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 میگون، 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- امضاهای رقمی (دیجیتالی) ناشناس - قسمت ۱: کلیات» که پیش‌نویس آن در کمیسیون‌های مربوط توسط مرکز آپا دانشگاه تربیت مدرس تهیه و تدوین شده است و در سیصد و هفتاد و یکمین اجلاس کمیته ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۴/۱/۱۸ 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، به‌عنوان 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 مورداستفاده قرار گرفته به شرح زیر است:

ISO/IEC 20008-1:2013, Information technology - Security techniques - Anonymous digital signatures - Part 1: General

فناوری اطلاعات- فنون امنیتی- امضاهای رقمی (دیجیتالی) ناشناس[1]- قسمت ۱: کلیات

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، مشخص کردن اصولی شامل مدل کلی، مجموعه‌ای از هستارها[2]، تعدادی فرآیند و الزامات کلی برای دو رده‌ی[3] سازوکارهای امضاهای دیجیتال ناشناس زیر است:

الف- سازوکارهای امضاء با استفاده از کلید عمومی گروهی،

ب- سازوکارهای امضاء با استفاده از کلیدهای عمومی چندگانه.

۲ اصطلاحات و تعاریف

برای این استاندارد، اصطلاحات و تعاریف زیر به کار می‌روند:

۱-۲

امضای دیجیتال ناشناس

امضایی که با استفاده از کلید عمومی گروهی یا کلید عمومی چندگانه، قابل درستی‌سنجی[4] است و با هر هستار غیرمجازی که تصدیق‌کننده‌ی امضاء دارد برای تشخیص شناسانه‌ی[5] امضاءکننده‌اش قابل ردگیری نیست.

یادآوری ۱- امضاهای دیجیتال ناشناس با عنوان امضاهای ناشناس یا امضاهای دیجیتال نیز شناخته می‌شوند.

۲-۲

میزان ناشناسی

عددی است که از احتمال اینکه هستاری غیرمجاز می‌تواند از امضای ارائه‌شده، درستی امضاءکننده‌ی واقعی را تعیین کند مشتق می‌شود.

یادآوری ۱- میزان ناشناسی n، به این معناست که احتمال اینکه یک هستار غیرمجاز بتواند به‌درستی امضاءکننده واقعی را از امضاء، حدس بزند، $1/n$ است.

۳-۲

تابع چکیده‌ساز[6] برخوردتاب[7]

این تابع خاصیت زیر را برآورده می‌کند: پیدا کردن دو ورودی متمایز که به خروجی یکسان نگاشت شوند از نظر محاسباتی، غیرعملی است.

---

1 - Anonymous digital signatures
2 - Entities
3 - Category
4 - Verified
5 - Identifier
6 - Hash function
7 - Collision resistance

[منبع: ISO/IEC 10118-1:2000]

یادآوری ۱ – امکان‌پذیری محاسباتی به محیط و الزامات امنیتی خاصی بستگی دارد.

۴-۲

عنصر داده

عدد صحیح، رشته بیتی، مجموعه‌ی اعداد صحیح یا مجموعه رشته‌های بیتی

[منبع: ISO/IEC 14888-1:2008]

۵-۲

شناسانه‌ی تشخیص‌دهنده

اطلاعاتی که به‌طور غیرمستقیم، هستاری را تشخیص می‌دهد.

[منبع: ISO/IEC 11770-2:2008]

۶-۲

دامنه

مجموعه هستارهایی که تحت خط‌مشی امنیتی تکی عمل می‌کنند.

[منبع: ISO/IEC 14888-1:2008]

مثال- گواهی‌های کلید عمومی ایجادشده توسط یک مرجع یا مراجعی که از خط‌مشی امنیتی یکسان استفاده می‌کنند.

۷-۲

پارامتر دامنه

عنصر داده‌ای که برای همه هستارهای درون دامنه، قابل‌دسترس یا شناخته‌شده یا مشترک است.

[منبع: ISO/IEC 14888-1:2008]

۸-۲

شواهد انقیاد[1]

عنصر داده‌ای که انقیاد رمزنگاشتی[2] بین امضاء کننده و امضاء را نشان می‌دهد و خروجی فرآیند آغازین عضویت گروه است.

۹-۲

فرآیند ارزیابی شواهد[3]

فرآیندی که شواهد انقیاد، امضای گروهی و کلید عمومی گروهی را به‌عنوان ورودی در نظر می‌گیرد و نتیجه-ی ارزیابی شواهد را به‌عنوان خروجی می‌دهد: معتبر یا نامعتبر

یادآوری ۱ – ورودی امضای گروهی به فرآیند ارزیابی شواهد باید معتبر باشد یعنی امضاء باید پیش‌تر به‌طور موفقیت‌آمیزی با استفاده از فرآیند درستی‌سنجی امضای گروهی، تصدیق شده باشد.

1 - Evidence of binding
2 - Cryptographic
3 - Evidence evaluation process

۱۰-۲
ارزیاب شواهد
هستاری که اعتبار شواهد انقیاد را وارسی می‌کند.

۱۱-۲
گروه
مجموعه هستارهایی که تحت یک خط‌مشی مدیریت عضویت تکی، عمل می‌کنند.
یادآوری ۱ - گروه شامل چندین عضو گروه است و هر عضو، گواهی عضویت دارد که توسط صادرکننده عضویت گروه به‌عنوان بخشی از فرآیند صدور عضویت گروه ایجاد شده است.

۱۲-۲
عضو گروه
هستاری که گواهی عضویت گروه دارد و می‌تواند امضای گروه را از طرف گروه ایجاد کند.

۱۳-۲
کلید خصوصی عضو گروه
عنصر داده‌ی خصوصی که بخشی از کلید امضای عضو گروه است، خاص عضو گروه است و فقط توسط عضو صادرکننده عضویت گروه و فرآیندهای امضای گروه، قابل‌استفاده است.

۱۴-۲
کلید امضای عضو گروه
مجموعه‌ای از عنصرهای داده‌ی خاص عضو گروه که شامل کلید خصوصی عضو گروه و گواهی عضویت گروه است و فقط توسط عضو فرآیند امضای گروهی، قابل‌استفاده است.

۱۵-۲
گواهی عضویت گروه
عنصر داده‌ی خاص عضو گروه که با استفاده از کلید صدور عضویت گروه، به‌طور غیرقابل انعطاف پردازش شده است و توسط عضو گروه در فرآیند امضای گروهی، قابل‌استفاده است.
یادآوری ۱- گواهی عضویت گروه، گواهی عضویت نیز نامیده می‌شود.
یادآوری ۲- گواهی عضویت گروه، بخشی از کلید امضای عضو گروه است.

۱۶-۲
صادرکننده عضویت گروه
هستاری که گواهی‌های عضویت گروه را ایجاد می‌کند.
یادآوری ۱ - صادرکننده عضویت گروه، صادرکننده گروه یا صادرکننده نیز نامیده می‌شود.

۱۷-۲
کلید صادرکننده عضویت گروه
عنصر داده خصوصی خاص صادرکننده عضویت گروه که فقط توسط صادرکننده در فرآیند صدور گروه، قابل‌استفاده است.

یادآوری ۱ - کلید صادرکننده عضویت گروه، کلید صادرکننده گروه یا کلید صادرکننده نیز نامیده می‌شود.

۲-۱۸

فرآیند صدور عضویت گروه

فرآیندی که کلید صدور عضویت گروه، کلید عمومی گروهی، پارامترهای عمومی گروه و به‌طور اختیاری شناسانه تمیز دهنده را به‌عنوان ورودی استفاده می‌کند و کلید امضای عضو گروه را به‌عنوان خروجی می‌دهد.

یادآوری ۱ - فرآیند صدور عضویت گروه، فرآیند صدور نیز نامیده می‌شود.

یادآوری ۲ - فرآیند صدور عضویت گروه، در محاوره به‌عنوان فرآیند اتصال عضویت گروه یا فرآیند اتصال نیز مورداشاره قرار می‌گیرد.

۲-۱۹

ابطال سراسری[1]

فرآیند ابطال امضای گروه که با به‌روزرسانی کلید عمومی گروهی، سایر پارامترهای عمومی گروه و/یا فهرست‌های ابطال مورداستفاده در محیط گروه، بر ابطال کلیدهای امضای برخی اعضای پیشین قانونی گروه تأثیر دارد و در نتیجه غیرقانونی شده‌اند.

یادآوری ۱ – فهرست ابطال مورداستفاده در فرآیند ابطال سراسری به فهرست ابطال سراسری گروه نیز معروف است.

یادآوری ۲ - کلیدهای امضای اعضای گروه، ممکن است در ابطال سراسری به‌روز شوند.

۲-۲۰

بازکننده[2] **عضویت گروه**

هستاری که از امضای گروه، شناسانه‌ی امضاءکننده را تعیین می‌کند.

یادآوری ۱ - بازکننده عضویت گروه، بازکننده یا بازکننده گروه نیز نامیده می‌شود.

۲-۲۱

کلید باز کردن عضویت گروه

عنصر داده خصوصی، ویژه‌ی بازکننده عضویت گروه که فقط توسط بازکننده در فرآیند باز کردن عضویت گروه، کاربرد دارد.

یادآوری ۱ - کلید باز کردن عضویت گروه، کلید بازکننده گروه یا کلید بازکننده نامیده می‌شود.

۲-۲۲

فرآیند باز کردن عضویت گروه

فرآیندی که امضای گروه، کلید باز کردن عضویت گروه، کلید عمومی گروهی و پارامترهای عمومی گروه را به‌عنوان ورودی در نظر می‌گیرد و شناسانه‌ی تشخیص‌دهنده‌ی امضاء کننده را به‌عنوان خروجی ارائه و به‌طور اختیاری شواهدی از انقیاد بین امضاءکننده و امضاء می‌دهد.

یادآوری ۱ - فرآیند باز کردن عضویت گروه، فرآیند باز کردن نیز نامیده می‌شود.

یادآوری ۲ - ضروری است که فرآیند باز کردن، امضای گروهی معتبر را به‌عنوان ورودی در نظر گیرد و به این معناست که امضاء به‌طور موفقیت‌آمیزی با استفاده فرآیند درستی‌سنجی امضای گروهی، تصدیق شده باشد.

---

1 - Global revocation

2 - Opener

۲۳-۲
کلید عمومی گروهی
عنصر داده عمومی که از نظر ریاضی با کلید عضویت گروهی مرتبط است و در فرآیند عضویت گروه، فرآیند امضای گروهی، فرآیند تصدیق گروهی و به‌طور اختیاری در هر فرآیند دیگر سازوکار امضای ناشناس که از کلید عمومی گروهی استفاده می‌کند، درگیر است.
یادآوری ۱ - کلید عمومی گروهی می‌تواند در برخی سازوکارها برای فعال‌سازی ابطال، به‌روزرسانی شود.

۲۴-۲
پارامتر عمومی گروه
عنصر داده‌ای که خاص گروه است و در تمامی هستارهای گروه، دسترس‌پذیر است و در تمامی فرآیندهای سازوکار امضای ناشناسی که از کلید عمومی گروهی استفاده می‌کنند، درگیر است.

۲۵-۲
امضای گروهی
عنصر داده‌ای که از فرآیند امضای گروهی، ناشی می‌شود.

۲۶-۲
پیونددهنده[1] امضای گروهی
هستاری که تعیین می‌کند که آیا دو امضای ناشناس با هم پیوند دارند یا خیر، یعنی توسط یک امضاءکننده ایجاد شده‌اند.
یادآوری ۱ - پیونددهنده امضای گروهی، پیونددهنده نیز نامیده می‌شود.
یادآوری ۲ - بسته به سازوکار، پیونددهنده ممکن است دارای کلید پیوند باشد یا نباشد.

۲۷-۲
پایه پیوند امضای گروهی
عنصر داده عمومی که به‌طور اختیاری، خاص پیوند امضای گروهی است و در فرآیند امضای گروهی درگیر است و اگر از این عنصر داده برای مرتبط ساختن چندین امضای ایجادشده توسط یک امضاءکننده استفاده کند، الزامی است.
یادآوری ۱- پایه پیوند امضای گروهی، پایه پیوند نیز نامیده می‌شود.
یادآوری ۲- پایه پیوند، گاهی اوقات در محاوره به‌عنوان پایه نام نیز به کار می‌رود. این عبارت در مشخصات دقیق امضای ناشناس که در ISO/IEC 20008-2 ارائه شد، استفاده می‌شود.

۲۸-۲
کلید پیونددهنده امضای گروهی
عنصر داده‌ای خصوصی که خاص پیونددهنده‌ی امضای گروهی است و فقط توسط پیونددهنده در فرآیند پیوند امضای گروهی، قابل‌استفاده است.
یادآوری ۱ - کلید پیونددهنده امضای گروهی، کلید پیوند نیز نامیده می‌شود.

---
1 - Linker

۲۹-۲

فرآیند پیونددهنده امضای گروهی

فرآیندی که دو امضای ناشناس، پارامترهای عمومی گروه و به‌طور اختیاری، کلید پیونددهنده امضای گروه را به‌عنوان ورودی در نظر می‌گیرد و نتیجه‌ی پیوند امضاء را به‌عنوان خروجی به‌صورت پیوندی یا غیر پیونـدی، ارائه می‌دهد.

یادآوری ۱ – فرآیند پیونددهنده امضای گروهی، فرآیند پیوند نیز نامیده می‌شود.

یادآوری ۲ – در برخی اسناد ISO/IEC به‌طور مثال ISO/IEC 20009-2 به فرآیند پیوند که از کلید پیونددهنده امضای گروهی استفاده می‌کند به‌عنوان ارائه‌دهنده قابلیت پیوند محلی، اشاره می‌شود.

یادآوری ۳ - امضاهای متمایز اگر تحت کلید امضای یکسان و با پارامترهای یکسان موردنیاز برای فرآیند پیوند، ایجاد شده باشند پیوند شده‌اند و اگر تحت دو کلید امضای متفاوت ایجاد شده باشند و از پارامترهای مشابه موردنیاز برای فرآیند پیوند استفاده نکرده باشند پیوند شده نیستند. برای مثال اگر تحت دو پایه پیوند امضای گروهی متفاوت ایجاد شده باشند.

۳۰-۲

فرآیند امضای گروهی

فرآیندی که پیام، کلید امضای عضو گروهی، کلید عمومی گروهـی، پارامترهـای عمـومی گروهـی و بـه‌طـور اختیاری، پایه پیوند را به‌عنوان ورودی در نظر می‌گیرد و امضای گروهی را به‌عنوان خروجی ارائه می‌دهد.

یادآوری ۱ - فرآیند امضای گروه، فرآیند امضاء نیز نامیده می‌شود.

۳۱-۲

فرآیند درستی‌سنجی امضای گروهی

فرآیندی که پیام امضاءشده‌ی گروه، کلید عمومی گروهی و پارامترهای عمومی گروهی را به‌عنوان ورودی در نظر می‌گیرد و نتیجه‌ی درستی‌سنجی امضای گروهی را به‌صورت معتبر یا نامعتبر، بـه‌عنـوان خروجـی ارائـه می‌دهد.

یادآوری ۱ - فرآیند درستی‌سنجی امضای گروه، فرآیند درستی‌سنجی نیز نامیده می‌شود.

۳۲-۲

فهرست ابطال امضای گروه

عنصر داده‌ای که می‌تواند برای تعریف امضای ناشناسی که توسط عضوی از گروه ایجاد شده است که مجاز به تولید چنین امضایی نبوده، استفاده شود.

یادآوری ۱ - فهرست ابطال امضای گروه می‌تواند شامل انواعی از محتوا مانند کلیدهای خصوصی اعضای گروه ابطال‌شده، مؤلفه‌های گواهی‌های باطل‌شده عضویت گروه و امضاهایی که قبلاً ایجاد شده‌اند و یا امضاهای ناقص باشد.

یادآوری ۲ - بسته به سازوکار، فهرست ابطال امضای گروه می‌تواند به‌عنوان فهرست ابطال کلید عمومی گروهی، فهرست ابطال سراسری گروه یا فهرست ابطال محلی تصدیق‌کننده، عمل کند.

۳۳-۲

فرآیند ابطال امضای گروه

فرآیندی که مجوز عضو گروه را برای ایجاد نوع خاص امضای گروهی، باطل می‌کند.

یادآوری ۱ - فرآیند ابطال امضای گروهی، می‌تواند شامل ابطال کل گروه، ابطال سراسری در سطح گروه و یا ابطال محلی تصدیق‌کننده اعضای گروه باشد.

۳۴-۲

پیام امضاءشده گروهی

پیام امضاءشده‌ای که در آن امضاء، امضای گروهی است که به‌طور اختیاری پایه پیوند را در برمی‌گیرد.

۳۵-۲

کد چکیده‌ساز[1]

رشته‌ای از بیت‌ها که خروجی تابع درهم است.

[منبع: ISO/IEC 10118-1:2000]

یادآوری ۱- ادبیات این موضوع، شامل انواع عباراتی است که معنای یکسان یا مشابهی را به‌عنوان کد درهم‌ساز دارند. کد تشخیص تغییر، کد تشخیص دست‌کاری، چکیده، نتیجه درهم، مقدار درهم و مهر زدن[2] نمونه‌هایی از آن هستند.

۳۶-۲

تابع چکیده‌ساز

تابعی که رشته‌های بیت‌ها را در رشته‌های بیت با طول ثابت نگاشت می‌کند و دو ویژگی زیر را تأمین می‌کند:

-برای یک خروجی معین، از نظر محاسباتی یافتن ورودی که به این خروجی نگاشت شود غیرممکن است.

-برای یک ورودی معین، از نظر محاسباتی یافتن ورودی دومی که به خروجی یکسانی نگاشت شود غیرممکن است.

[منبع: ISO/IEC 10118-1:2000]

یادآوری ۱ - امکان‌پذیری محاسباتی به محیط و الزامات امنیتی خاص، بستگی دارد.

۳۷-۲

کلید

توالی نمادهایی است که عملیات تبدیل رمزنگاشتی را واپایش می‌کند.

[منبع: ISO/IEC 9798-1:2010]

یادآوری ۱ - نمونه‌هایی از این عملیات موارد زیر را در برمی‌گیرد: رمزگذاری، رمزگشایی، محاسبه تابع وارسی رمزنگاشتی، تولید امضاء یا درستی‌سنجی امضاء.

۳۸-۲

ابطال محلی

فرآیند ابطال امضای گروه که تصدیق‌کننده‌ی امضاء را قادر می‌سازد تا امضای گروهی نامعتبر را بر اساس فهرست ابطال امضای گروه، رد کند.

---

1 - Hash code

2 - Imprint

یادآوری ۱- فهرست ابطال امضای گروه که در فرآیند ابطال محلی استفاده می‌شود، می‌تواند توسط خود تصدیق‌کننده یا منبع دیگری تولید شود. (به‌طور مثال می‌تواند بخشی از فهرست ابطال سراسری گروه باشد که توسط تصدیق‌کننده، پذیرفته‌شده است.)

یادآوری ۲- فهرست ابطال امضای گروه که در فرآیند ابطال محلی استفاده می‌شود به فهرست ابطال محلی تصدیق‌کننده نیز معروف است.

۳۹-۲

پیام

رشته بیت‌هایی با هر طول است.

[منبع: ISO/IEC 14888-1:2008]

۴۰-۲

پارامتر

عدد صحیح، رشته بیت یا تابع است.

[منبع: ISO/IEC 14888-1:2008]

۴۱-۲

امضاءکننده بالقوه

هستاری که کلید عمومی آن توسط امضاءکننده‌ی واقعی در فرآیند امضای حلقه استفاده می‌شود.

۴۲-۲

گروه

مجموعه هستارهایی که از امضاءکننده‌ی واقعی و امضاءکننده (گان) بالقوه تشکیل شده است.

۴۳-۲

پارامتر عمومی گروه

عنصر داده‌ای که خاص حلقه است و قابل‌دسترس برای تمامی هستارهای موجود در تمامی فرآیندهای سازوکارهای امضای ناشناس است که از کلید عمومی چندگانه استفاده می‌کنند.

۴۴-۲

امضاء گروه

عنصر داده‌ای که از فرآیند امضای حلقه ناشی می‌شود.

۴۵-۲

فرآیند امضای حلقه

فرآیندی که پیام، کلید امضاءکننده واقعی، کلید (کلیدهای) عمومی که متعلق به امضاءکننده (گان) بالقوه است و پارامترهای عمومی حلقه را به‌عنوان ورودی در نظر می‌گیرد و امضای حلقه را به‌عنوان خروجی می‌دهد.

۴۶-۲
فرآیند درستی‌سنجی امضای حلقه
فرآیندی که پیام امضاءشده حلقه، کلیدهای عمومی متعلق بـه امضـاءکننده‌ی واقعـی و امضـاءکننده (گـان) بالقوه و پارامترهای عمومی حلقه را به‌عنوان ورودی در نظر می‌گیرد و نتیجه درستی‌سنجی امضای حلقـه را به‌صورت معتبر یا نامعتبر، ارائه می‌دهد.

۴۷-۲
پیام امضاءشده‌ی حلقه
پیام امضاءشده‌ای که در آن امضاء، یک امضای حلقه است.

۴۸-۲
میزان امنیت
عدد مرتبط با میزان کار (تعداد عملیات) که برای شکستن الگوریتم رمزنگاشتی یا سامانه نیاز است.
یادآوری ۱ - میزان امنیت برحسب بیت مشخص شده است. میزان امنیت b بیت به این معناست که به تعداد 2^b عملیات برای شکستن امنیت سامانه نیاز است. مقادیر متداول برای میزان امنیت ۱۹۲،۱۲۸،۱۱۲،۸۰ و ۲۵۶ هستند.

۴۹-۲
امضاء
یک یا چند عنصر داده که از فرآیند امضاء، ناشی می‌شوند.
یادآوری ۱ – امضاء، امضای رقمی نیز نامیده می‌شود.

۵۰-۲
کلید امضاء
مجموعه‌ای از عنصرهای داده خصوصی خاص یک هستار و فقط قابل‌استفاده توسط همین هستار در فرآیند امضاء.
یادآوری ۱ - کلید امضاء در ISO/IEC 20008 و سایر استانداردها مثل ISO/IEC 9796-2 و ISO/IEC 9796-3، کلید امضاء خصوصی نامیده می‌شود.

۵۱-۲
جفت کلید امضاء
یک جفت کلید که شامل کلید امضاء و کلید درستی‌سنجی است که:
- کلید امضاء باید به‌طور ناقص یا کامل، مخفی نگهداری شود و فقط برای استفاده توسط امضاءکننده در نظر گرفته شده است.
- کلید درستی‌سنجی می‌تواند عمومی باشد و فقط برای استفاده توسط تصدیق‌کننده در نظر گرفته شده است.

۵۲-۲

فرآیند امضاء

فرآیندی که پیام، کلید امضاء و پارامترهای دامنه را به‌عنوان ورودی در نظر می‌گیرد و امضاء را به‌عنوان خروجی ارائه می‌دهد.

[منبع: ISO/IEC 14888-1:2008]

۵۳-۲

پیام امضاءشده

مجموعه‌ای از عناصر داده که از امضاء، بخشی از پیام که از امضاء نمی‌تواند بازیابی شود و یک فیلد متن اختیاری تشکیل شده است.

[منبع: ISO/IEC 14888-1:2008]

۵۴-۲

امضاءکننده

هستاری که امضای دیجیتالی را تولید می‌کند.

[منبع: ISO/IEC 13888-1:2009]

۵۵-۲

امضاءکننده‌ی واقعی

هستاری که یک امضای حلقه را در سمت حلقه ایجاد می‌کند.

یادآوری ۱ – امضاءکننده‌ی واقعی، امضاءکننده نیز نامیده می‌شود.

۵۶-۲

کلید درستی‌سنجی

مجموعه‌ای از عناصر داده عمومی که از نظر ریاضی با کلید امضاء هستار، مرتبط است و توسط تصدیق‌کننده در فرآیند درستی‌سنجی استفاده می‌شود.

یادآوری ۱ - کلید درستی‌سنجی در ISO/IEC 20008 و سایر استانداردها مثل ISO/IEC 9796-2 و ISO/IEC 9796-3، کلید درستی‌سنجی عمومی نامیده می‌شود.

۵۷-۲

فرآیند درستی‌سنجی

فرآیندی که پیام امضاءشده، کلید درستی‌سنجی و پارامترهای دامنه را به‌عنوان ورودی در نظر می‌گیرد و نتیجه درستی‌سنجی امضاء را به‌صورت معتبر یا نامعتبر، به‌عنوان خروجی ارائه می‌دهد.

[منبع: ISO/IEC 14888-1:2008]

۵۸-۲

تصدیق‌کننده

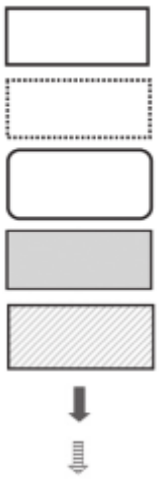
هستاری که اعتبار امضاء را وارسی می‌کند.

یادآوری ۱ - تصدیق‌کننده به تصدیق‌کننده‌ی امضاء نیز معروف است.

۳ کوته‌نوشت‌ها و راهنمای شکل‌ها

تصدیق ناشناس مستقیم	Direct Anonymous Attestation	DAA
پودمان بستر مورد اعتماد	Trusted Platform Module	TPM

راهنمای شکل‌های این بخش از استاندارد ISO/IEC 20008 به‌صورت زیر است:



داده

داده اختیاری

رویه

هستار در رویه

داده عبور یافته از یک رویه به رویه دیگر

جریان داده

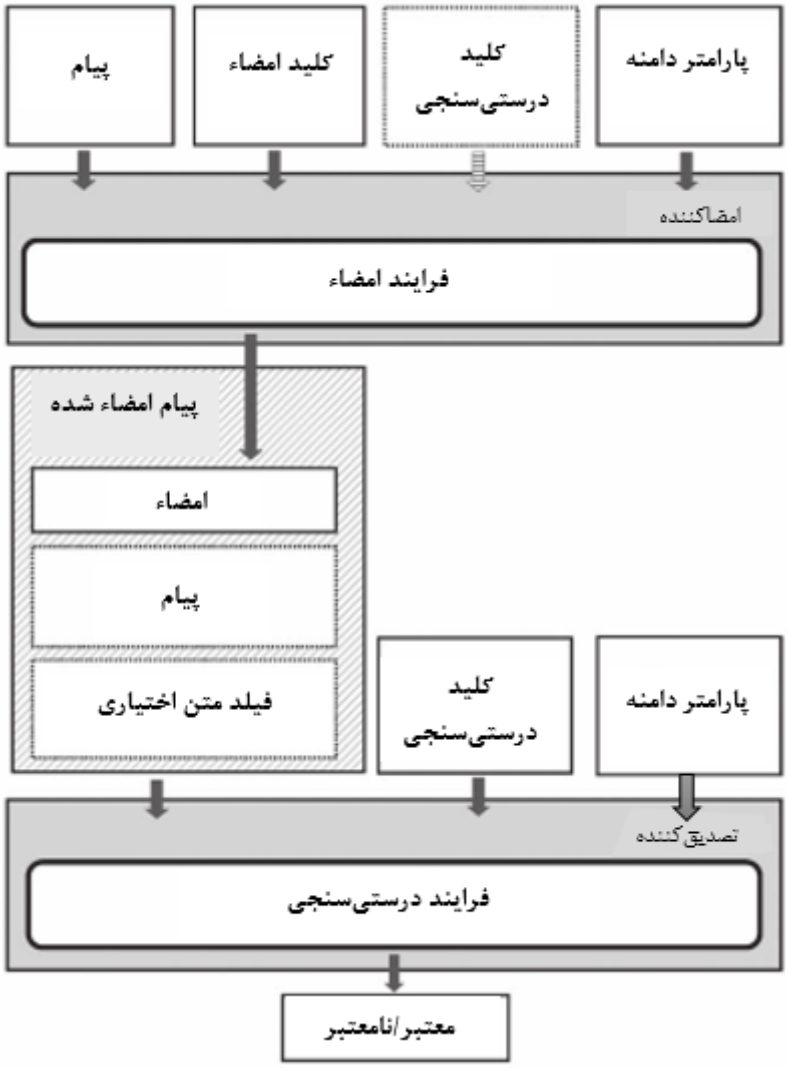
جریان داده اختیاری

۴ گزینه‌هایی برای کلید عمومی گروهی و کلید عمومی چندگانه

همان‌طور که در شکل ۱ نشان داده شده است در سازوکار رایج امضای دیجیتال، کلید امضای خصوصی و کلید درستی‌سنجی عمومی، جفت کلید امضاء را تشکیل می‌دهند. امضاء کننده از کلید امضای خصوصی در فرآیند امضاء برای ایجاد امضای پیامی معین، استفاده می‌کند. تصدیق‌کننده از کلید درستی‌سنجی عمومی در فرآیند درستی‌سنجی برای وارسی این‌که آیا امضاء، تحت کلید خصوصی متناظر، امضاء شده یا نشده است، استفاده می‌کند. اگر تصدیق‌کننده، متقاعد شود که امضاء با استفاده از کلید امضای متناظر با کلید درستی‌سنجی، ایجاد شده است، آن را معتبر اعلام می‌کند و در غیر این صورت آن را نامعتبر در نظر می‌گیرد. در نتیجه از نقطه‌نظر تصدیق‌کننده، امضاء از طریق کلید درستی‌سنجی عمومی به امضاء کننده محدود می‌شود که به‌عنوان شناسانه‌ی تشخیص‌دهنده برای امضاءکننده عمل می‌کند.

در سازوکار امضای دیجیتال ناشناس، ضروری نیست که کلید امضای خصوصی و کلید درستی‌سنجی عمومی، یک جفت کلید امضاء را شکل دهند که یکی در فرآیند امضاء و دیگری در فرآیند درستی‌سنجی به کار رود. این بخش از استاندارد ISO/IEC 20008، اصول و الزامات را برای دو نوع سازوکار امضای ناشناس مشخص می‌کند که از انواع مختلف کلیدهای درستی‌سنجی عمومی استفاده می‌کنند. این دو رده به‌عنوان

سازوکارهایی که از کلید عمومی گروه و سازوکارهایی که از کلید عمومی چندگانه استفاده می‌کنند، شناخته می‌شوند.



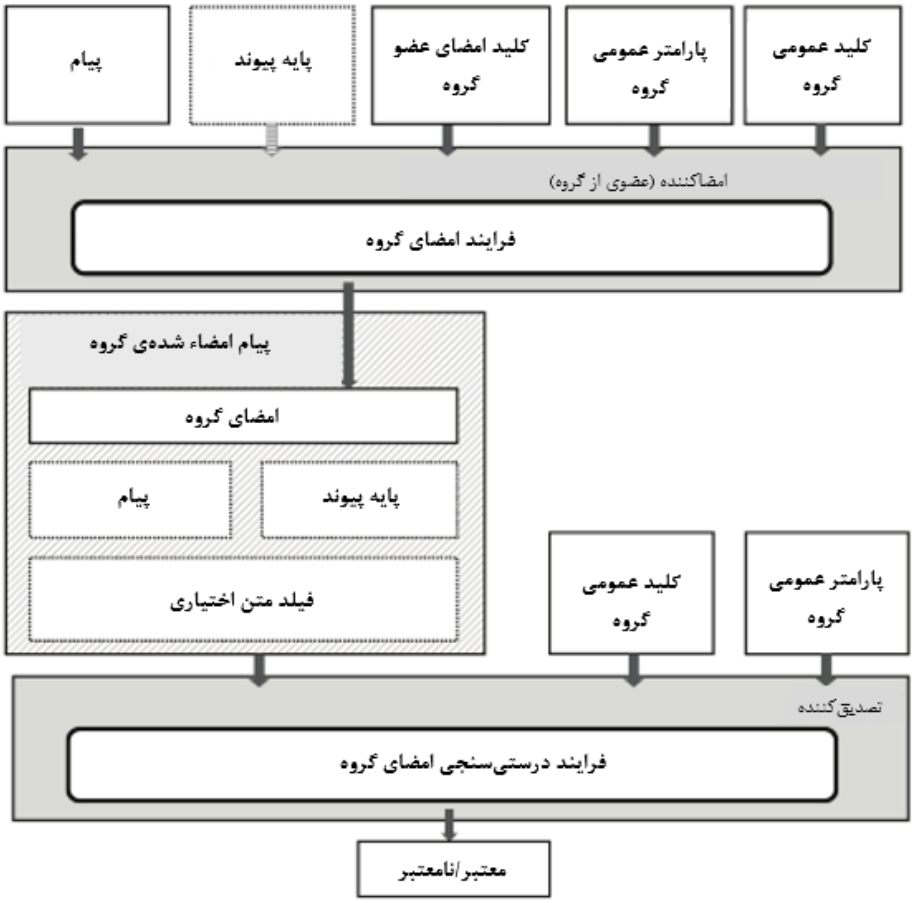
شکل ۱- فرآیندهای امضاء و درستی‌سنجی در سازوکار امضای متداول

همان‌طور که در شکل ۲ نشان داده شده است، در سازوکار امضای ناشناسی که از کلید عمومی گروه استفاده می‌کند، امضاءکننده عضوی از گروه است. گروه، یک کلید عمومی گروهی واحد دارد. هر عضو گروه یک امضای متمایز عضو گروه را دارد که از کلید خصوصی عضو گروه و گواهی عضویت مربوط، تشکیل شده است. امضاءکننده از کلید امضای عضو گروه در فرآیند امضاء استفاده می‌کند تا امضای گروهی را در یک پیام معین، ایجاد کند. تصدیق‌کننده از کلید عمومی گروه در فرآیند درستی‌سنجی امضاء استفاده می‌کند تا وارسی کند آیا امضای گروه، طبق کلید امضاء عضو گروه بوده است یا خیر، بدون اینکه نشان دهد کدام‌یک از کلیدهای امضاء عضو گروه، برای ایجاد امضاء استفاده شده است. اگر تصدیق‌کننده متقاعد شود که امضاء با استفاده از یکی از کلیدهای امضای اعضای گروه ایجاد شده است که متناظر با کلید عمومی گروه است آن را معتبر اعلام می‌کند و در غیر این صورت آن را نامعتبر می‌داند. در نتیجه از دیدگاه تصدیق‌کننده، امضای

گروه، به یک امضاءکننده‌ی منفرد محدود نیست و به‌جای آن با کلید عمومی گروه، به گروه، محدود می‌شود. میزان ناشناس بودن به اندازه گروه بستگی دارد.

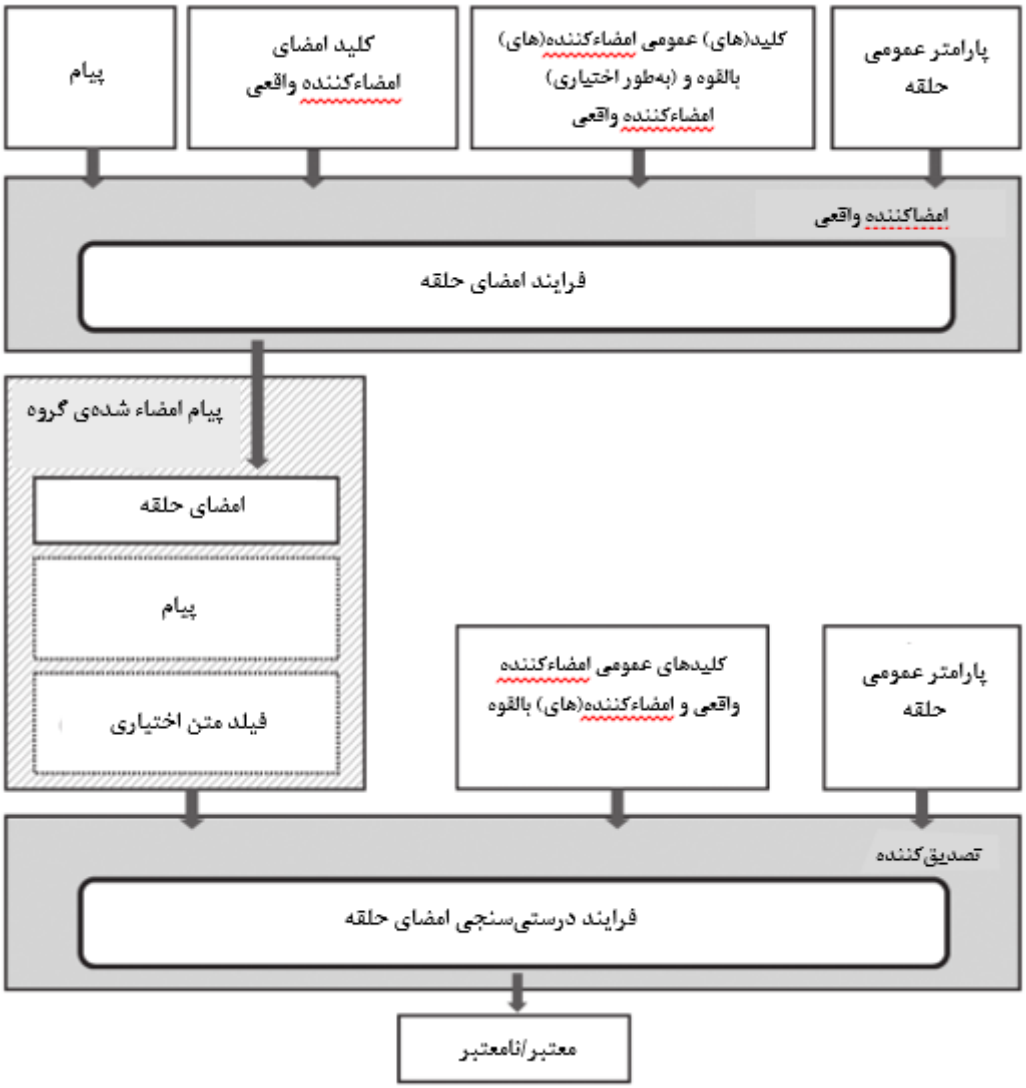
یادآوری- برخی از سازوکارها به‌منظور تولیدشده توسط تصدیق‌کننده نیاز دارند تا ورودی امضاء گروه و فرآیندهای درستی-سنجی امضاء گروه باشند. برای اهداف شکل ۲، هدف به‌عنوان بخشی از پیام، تلقی می‌شود.

در سازوکار امضای ناشناسی که از کلید عمومی چندگانه استفاده می‌کند (به سازوکار امضای حلقه نیز معروف است) و در شکل ۳ نشان داده شده است هر امضاءکننده شامل امضاءکننده واقعی است و هر امضاءکننده‌ی بالقوه، یک کلید امضای خصوصی و یک کلید درستی‌سنجی عمومی دارد که یک جفت کلید امضاء را به روش مشابه سازوکار امضای دیجیتال متداول، شکل می‌دهد. در فرآیند امضاء، امضاءکننده‌ی واقعی از کلید امضای خود به همراه کلید عمومی (مجموعه‌ای از کلیدهای عمومی) که متعلق به یک امضاءکننده‌ی بالقوه (مجموعه‌ای از امضاءکننده‌های بالقوه) است، برای ایجاد امضای معینی استفاده می‌کند. در فرآیند درستی‌سنجی، تصدیق‌کننده از مجموعه کلیدهای عمومی استفاده می‌کند که شامل امضاءکننده‌ی واقعی و همه امضاءکننده‌های بالقوه هستند تا وارسی کند که آیا امضاء طبق کلید امضای متناظر با کلید عمومی در مجموعه کلید عمومی بوده است یا خیر. در نتیجه از نقطه نظر تصدیق‌کننده، امضاء به امضاءکننده‌ی انفرادی محدود نیست بلکه به مجموعه‌ای از صاحبان کلیدهای عمومی محدود است. میزان ناشناس بودن به تعداد کلیدهای عمومی بستگی دارد.



شکل ۲-فرآیندهای امضاء و درستی‌سنجی در سازوکار امضای ناشناس با استفاده از کلید عمومی گروه

همان‌طور که در شکل‌های ۱ تا ۳ نشان داده شده است، ورود پیام به فرآیند امضاء ممکن است به دو بخش تقسیم شود. اگر تقسیم شود یک بخش می‌تواند از امضاء بازیابی شود و بخش دیگر نمی‌تواند از امضاء بازیابی شود. بخشی از پیام که در پیام امضاءشده در برگرفته‌شده است آن بخشی از امضاء است که قابل بازیابی نیست.



شکل ۳- فرآیندهای بررسی و امضاء برای سازوکار امضای حلقه

۵ الزامات کلی

هر هستار درگیر در سازوکار امضای دیجیتال ناشناس، باید از مجموعه متداول پارامترهای دامنه که برای محاسبه انواع کارکردهای سازوکار استفاده‌شده‌اند، آگاه باشد. در سازوکار امضای ناشناسی که از کلید عمومی گروهی استفاده می‌کند، دامنه به گروه وابسته است و پارامترهای دامنه نیز به‌عنوان پارامترهای عمومی گروه شناخته می‌شوند. در سازوکار امضای ناشناسی که از کلید عمومی چندگانه استفاده می‌کند، دامنه به حلقه وابسته است و پارامترهای دامنه (به‌عنوان پارامترهای عمومی حلقه نیز شناخته می‌شوند) شامل همه پارامترهای وابسته به مجموعه کلیدهای عمومی و فرآیندهای امضاء و درستی‌سنجی متناظر هستند.

هر تصدیق‌کننده‌ی امضاء باید به یک کپی معتبر از کلیدهای عمومی لازم، دسترسی داشته باشد. در سازوکار امضای ناشناسی که از کلید عمومی گروهی استفاده می‌کند، کلید عمومی به گروهی از امضاءکنندگان تعلق دارد تا به یک امضاء کننده‌ی منفرد. در سازوکار امضای ناشناسی که از کلید عمومی چندگانه استفاده می‌کند کلیدهای عمومی، مجموعه‌ای از کلیدهای عمومی منفرد هستند که هرکدام به یک امضاءکننده‌ی واقعی یا یک امضاءکننده‌ی بالقوه تعلق دارند. تصدیق‌کننده قادر به تشخیص امضاءکننده‌ی واقعی از امضاءکننده‌ی بالقوه نیست. هر امضاءکننده باید یک شناسانه‌ی تشخیص‌دهنده داشته باشد که به‌طور واضح به کلید خصوصی امضاءکننده محدود است. این اطلاعات باید هنگام اجرای فرآیندهای سازوکار، برای هستارهای مربوط در دسترس باشد. در سازوکار امضای ناشناسی که از کلید عمومی چندگانه استفاده می‌کند شناسانه‌ی تشخیص‌دهنده‌ی امضاءکننده می‌تواند کلید درستی‌سنجی عمومی امضاءکننده باشد. در سازوکار امضای ناشناسی که از کلید عمومی گروه استفاده می‌کند. شناسانه‌ی تشخیص‌دهنده‌ی امضاءکننده می‌تواند شکل‌های مختلفی داشته باشد.

در سازوکار امضای ناشناسی که از کلید عمومی گروه استفاده می‌کند، باید سازوکار اصالت‌سنجی هستار استفاده شود تا به اعضای گروه و صادرکننده‌ی عضویت گروه اجازه دهد فرآیند صدور عضویت گروه را با روشی معتبر، اداره کنند. این کار تضمین می‌کند که صادرکننده‌ی عضویت گروه، فقط گواهی عضویت گروه را برای اعضای قانونی گروه، فراهم می‌آورد. هنگامی که سازوکار اصالت‌سنجی این هستار، ناشناس نیست، استفاده از یکی از سازوکارهای مشخص‌شده در ISO/IEC 9798 [۳] توصیه می‌شود. هنگامی که سازوکار اصالت‌سنجی هستار ناشناس است، استفاده از یکی از سازوکارهای مشخص‌شده در ISO/IEC 20009 [۱۳] توصیه می‌شود.

استاندارد ISO/IEC 20008 سازوکارهایی را برای مدیریت کلید یا برای گواهی کلیدهای عمومی گروه یا کلیدهای عمومی منفرد مشخص نمی‌کند. انواع ابزارها برای به دست آوردن کپی قابل‌اطمینانی از یک کلید عمومی وجود دارند، به‌طور مثال، گواهی کلید عمومی، فنون مدیریت کلید و گواهی‌ها، خارج از دامنه‌ی ISO/IEC 20008 هستند. برای اطلاعات بیشتر به ISO/IEC 9594-8 [۱]، ISO/IEC 11770-2 [۵]، ISO/IEC 11770-3 [۶] و ISO/IEC 15945 [۱۰] رجوع شود.

برای سازوکارهای امضای ناشناسی که از کلید عمومی گروهی استفاده می‌کنند این استاندارد مشخص نمی‌کند که صادرکننده‌ی عضویت گروه، چگونه یک عضو گروه را اصالت‌سنجی می‌کند و در چه موقعیت‌هایی فرآیند باز کردن عضویت گروه یا فرآیند پیونددهنده امضای گروه استفاده می‌شود. علاوه بر این مشخص نمی‌کند که چطور یک صادرکننده عضویت گروه، بازکننده عضویت گروه یا هر هستار دیگری تصمیم می‌گیرد که یک عضو گروه، بیش از این برای ایجاد نوع خاصی از امضای گروهی اختیار ندارد اما هنگامی که سازوکار ابطال، استفاده می‌شود نیازمند این است که هر تصدیق‌کننده‌ی امضاء به آخرین کلید عمومی گروه و هرکدام از پارامترهای ضروری عمومی گروه دسترسی داشته باشد و اگر فهرست ابطال امضای گروه استفاده می‌شود، تصدیق‌کننده به آن دسترسی دارد.

۶ سازوکارهایی که از کلید عمومی گروهی استفاده می‌کنند

۶-۱ مدل کلی

هر سازوکار امضای دیجیتال ناشناسی که از کلید عمومی گروهی استفاده می‌کند به‌عنوان سازوکار امضای گروهی نیز شناخته می‌شود. این نوع سازوکار شامل گروه و مجموعه‌ای از اعضای گروه است. صادرکننده‌ی عضویت گروه نیز وجود دارد؛ هم‌چنین اگر ردیابی امضاء کننده‌ی یک امضاء نیاز باشد، بازکننده‌ی عضویت گروه نیز موردنیاز است. میزان ناشناس بودن سازوکار به تعداد اعضای قانونی گروه بستگی دارد.

بسته به سازوکار، مجاز است پیوند دو امضای ایجاد شده توسط یک امضاءکننده یکسان، امکان‌پذیر باشد. هستاری که قادر به پیوند است، به پیونددهنده امضای گروه نیز معروف است؛ ضروری نیست چنین هستاری عضوی از گروه باشد. در برخی سازوکارها هرکسی می‌تواند پیونددهنده باشد؛ این حالت معمولاً شامل پایه پیوند هست. در سایر سازوکارها، پیونددهنده‌ای باید کلید پیوند امضای گروه را نگه دارد؛ در این حالت پارامترهای عمومی مرتبط با کلید پیوند در امضاء وجود دارند.

بسته به سازوکار، ابطال کلید خصوصی عضو گروه یا گواهی عضویت گروه ممکن است امکان‌پذیر باشد. در هرکدام از این دو حالت، کلید امضای عضو گروه، باطل خواهد شد. امضای گروهی ایجاد شده تحت کلید امضای گروهی ابطال‌شده در طول فرآیند درستی‌سنجی امضای گروه، رد خواهد شد. سازوکار امضای دیجیتال ناشناسی که از کلید عمومی گروه استفاده می‌کند با مشخصات فرآیندهای زیر، تعریف شده است:

- فرآیند تولید کلید (شامل فرآیند صدور عضویت گروه)
- فرآیند امضای گروه
- فرآیند باز کردن امضای گروه (اختیاری)
- فرآیند پیونددهنده امضای گروه (اختیاری)
- فرآیند ابطال امضای گروه (اختیاری)

نمونه‌های خاص سازوکارهای امضای ناشناسی که از کلید عمومی گروهی استفاده می‌کنند در قسمت دوم مجموعه استاندارد ISO/IEC 20008 مشخص شده‌اند.

۶-۲ هستارها

تعدادی از انواع هستارها در سازوکار امضای ناشناسی که از کلید عمومی گروهی استفاده می‌کنند درگیر هستند که در بخش زیر، فهرست شده‌اند. برخی از انواع هستارها در هر سازوکاری وجود دارند درحالی‌که هستارهای دیگر فقط در سازوکارهایی که ویژگی‌های اختیاری را ارائه می‌دهند درگیر هستند.

- امضاءکننده: امضاءکننده، عضوی از گروه است که امضای دیجیتال تولید می‌کند. امضاءکننده، شناسانه‌ی تشخیص‌دهنده و کلید امضای اعضای گروه را دارد که از کلید خصوصی اعضای گروه و گواهی عضویت، تشکیل شده است.

یادآوری ۱- کلید امضای گروه، به‌عنوان کلید امضای امضاءکننده نیز شناخته می‌شود.

در برخی از سازوکارها، نقش امضاءکننده بین چندین هستار تقسیم می‌شود. به‌طور مثال در سازوکارهای تصدیق ناشناس مستقیم (DAA) که در بخش ۲ از استاندارد ISO/IEC 20008 مشخص شده است، نقش امضاءکننده می‌تواند بین امضاءکننده‌ی اصلی با قابلیت محاسباتی و ذخیره‌سازی محدود، به‌طور مثال پودمان بستر مورد اعتماد (TPM) و امضاء کننده‌ی کمکی با توان محاسباتی بیشتر و رواداری[1] امنیتی کمتر، مثل بستر کامپیوتر معمولی (میزبان دربرگیرنده‌ی TPM تعبیه‌شده) تقسیم شود.

یادآوری ۲- فناوری TPM، در استاندارد ISO/IEC 11889 [۷] مشخص می‌شود.

- تصدیق‌کننده: تصدیق‌کننده‌ی هستاری است که امضای دیجیتال را تصدیق می‌کند.
- صادرکننده عضویت گروه: هستاری است که گواهی عضویت گروه را برای امضاءکننده، صادر می‌کند. این هستار در تمامی سازوکارهای مشخص شده در قسمت دوم استاندارد ISO/IEC 20008 وجود دارد.
- بازکننده عضویت گروه: هستاری است که امضاءکننده‌ی امضاء را تعیین می‌کند. این هستار در برخی سازوکارهای مشخص‌شده در قسمت دوم استاندارد ISO/IEC 20008 وجود دارد. در برخی سازوکارها، صادرکننده عضویت گروه و بازکننده عضویت گروه، هستارهای یکسانی هستند. بسته به سازوکار، بازکننده‌ی عضویت گروه مجاز است شواهد انقیادی را نتیجه دهد که امضاء را به شناسانه‌ی تشخیص‌دهنده‌ی امضاءکننده‌اش محدود کند.
- ارزیاب شواهد: اعتبار شواهد انقیاد را وارسی می‌کند.
- پیونددهنده امضای گروه: هستاری است که قادر به پیوند دو امضای ایجاد شده توسط امضاءکننده‌ی یکسان است. این هستار، در برخی سازوکارهای مشخص‌شده در بخش ۲ از استاندارد ISO/IEC 20008 وجود دارد. در برخی سازوکارها، پیونددهنده، تصدیق‌کننده نیز هست. تعداد پیوند دهنده‌ها در سازوکار امضای ناشناس، ممکن است متغیر باشد.

۶-۳ فرآیند تولید کلید

اگر فرآیند تولید کلید، موردنیاز سازوکار باشد شامل الگوریتم‌های تولید کلید برای تولید کلید صدور عضویت گروه، کلید بازکننده‌ی عضویت گروه و کلید پیونددهنده‌ی امضای گروه است. یک الگوریتم معمول ایجاد کلید، پارامتر امنیت را به‌عنوان ورودی می‌گیرد که به میزان امنیت سازوکار بستگی دارد و جفت کلید عمومی و خصوصی را به‌عنوان خروجی ارائه می‌دهد.

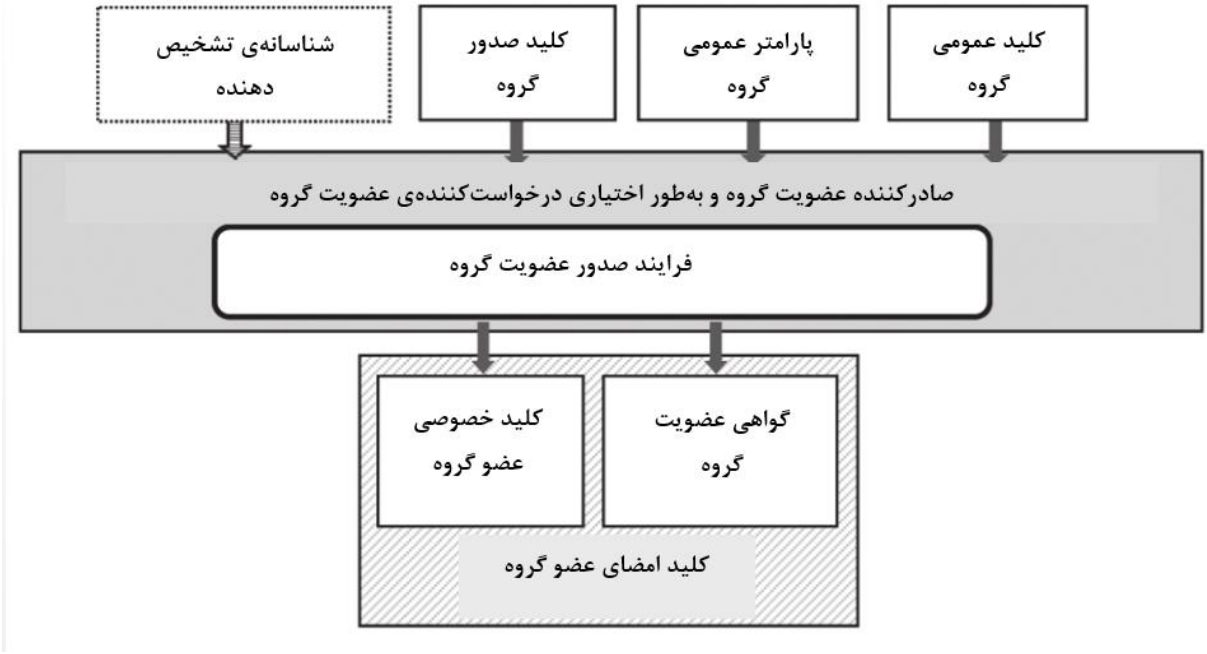
فرآیند تولید کلید شامل فرآیند صدور عضویت گروه نیز هست. بسته به سازوکار، فرآیند صدور عضویت گروه همان‌طور که در شکل ۴ نشان داده شده است مجاز است شامل پروتکل بین کاربری که می‌خواهد عضوی از گروه شود و صادرکننده عضویت گروه باشد یا نباشد.

اگر چنین پروتکلی موردنیاز باشد، هم عضو گروه و هم صادرکننده عضویت گروه، در ایجاد کلید امضای عضو گروه، نقش خواهند داشت. در تکمیل پروتکل، عضو گروه، کلید امضای عضو گروه را دارد که از کلید

1 - Tolerance

خصوصی اعضای گروه عضو و گواهی عضویت تشکیل شده است. صادرکننده عضویت گروه، گواهی عضویت و شناسانه تشخیص‌دهنده‌ی عضو را می‌شناسد که هر دو به یکدیگر وابسته هستند. ایجاد شناسانه‌ی تشخیص‌دهنده به سازوکار بستگی دارد و ممکن است ورودی فرآیند صدور عضویت گروه باشد. به‌طور متناوب، صادرکننده عضویت گروه به‌تنهایی کلید امضای عضو گروه را تولید می‌کند و آن را به عضو گروه ارائه می‌دهد. در این مورد کلید خصوصی اعضای گروه و گواهی عضویت جدا نیستند و هم صادرکننده و هم عضو، باید کلید امضاء را داشته باشند.

یادآوری- اگر صادرکننده عضویت گروه، کلید امضای عضو گروه امضاء کننده را بشناسد، باید به صادرکننده‌ی عضویت گروه اعتماد کند که عضو گروه را جعل هویت نمی‌کند، در غیر این صورت سازوکار امضای گروه، ویژگی سلب انکار[1] را پردازش نمی‌کند.



شکل ۴- فرآیند صدور عضویت گروه

۴-۶ فرآیند امضای گروه

فرآیند امضاء توسط عضوی از گروه که به‌عنوان امضاءکننده عمل می‌کند، انجام می‌شود. امضاءکننده از کلید امضای عضویت خود، برای محاسبه امضای گروه در یک پیام معین استفاده می‌کند.

اگر سازوکار از بازکننده‌ی عضویت گروه پشتیبانی کند، فرآیند امضای شناسانه‌ی تشخیص‌دهنده را در امضاء طوری مشخص می‌کند که بازکننده‌ی عضویت گروه بتواند آن را بازیابی کند نه بخش دیگری. این کار با رمزگذاری نامتقارن شناسانه‌ی تشخیص‌دهنده با استفاده از کلید عمومی بازکننده گروه، قبل از در برگرفتن امضاء حاصل می‌شود.

1 - Non-repudiation

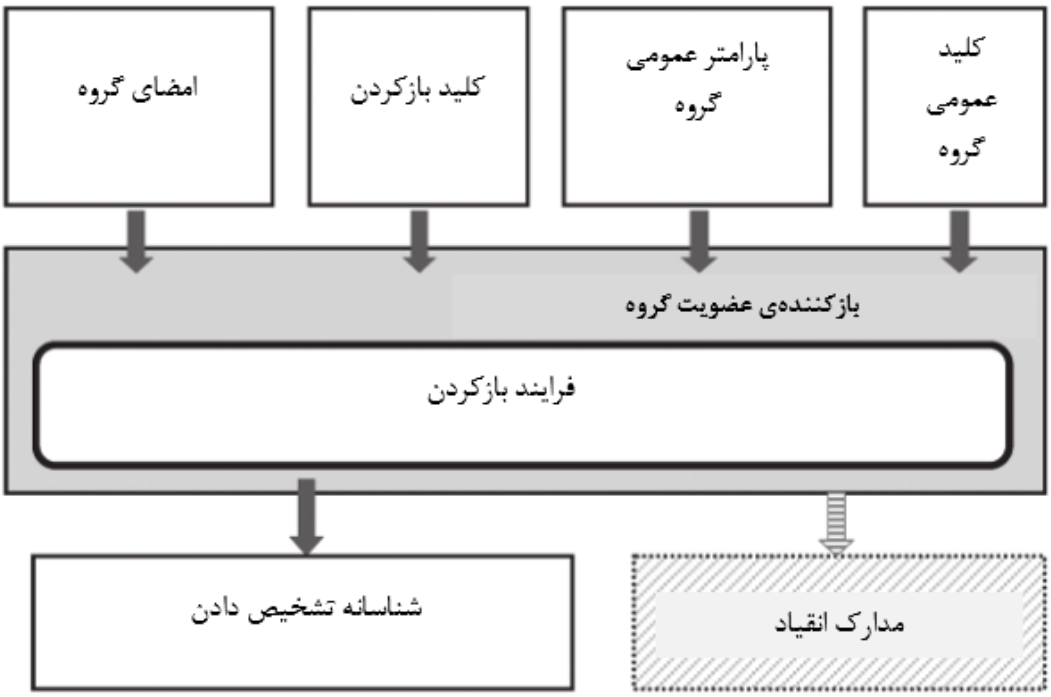
اگر سازوکار از پیوند امضای گروه پشتیبانی کند فرآیند امضاء از همان پایه پیوند یا کلید پیوند در زمان تولید دو امضایی که قابل پیوند هستند طوری استفاده می‌کند که پیونددهنده‌ی امضای گروه بتواند آن‌ها را پیوند دهد و نه بخش دیگری. بسته به سازوکار، پیونددهنده ممکن است تصدیق‌کننده‌ی امضاء باشد.
اگر سازوکار به امضاءکنندگان اجازه ابطال بدهد فرآیند امضاء باید شامل کارکردی باشد که تضمین کند تصدیق‌کننده می‌تواند بررسی کند که امضاء توسط امضاءکننده‌ی باطل نشده، ایجاد شده است.

۶-۵ فرآیند درستی‌سنجی امضای گروه

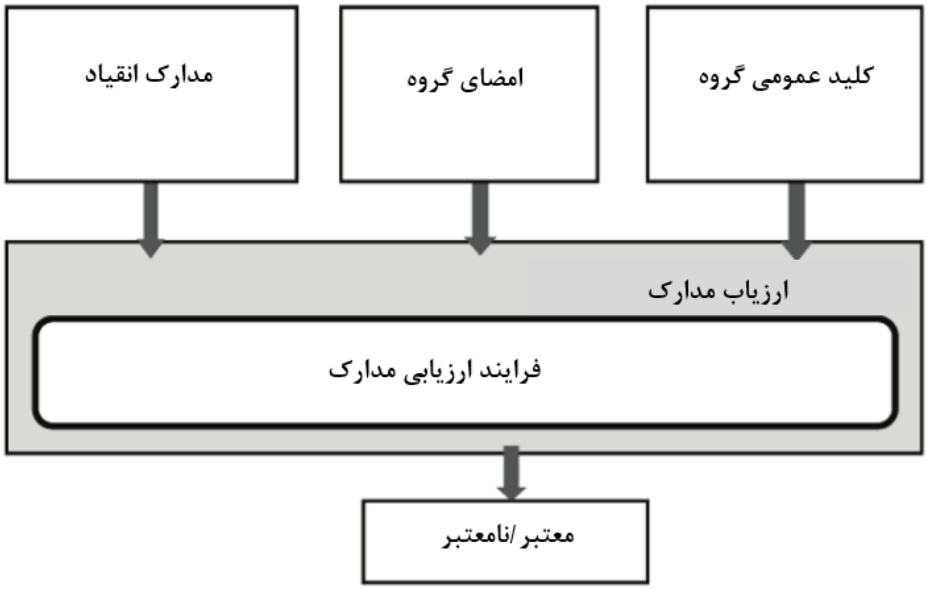
فرآیند درستی‌سنجی توسط تصدیق‌کننده‌ای صورت می‌گیرد که قادر است تا کلید عمومی صحیح گروه را با امضاء مرتبط سازد اما قادر به تعیین شناسانه‌ی امضاءکننده از امضاء نیست.
بسته به سازوکار، فرآیند درستی‌سنجی ممکن است مستقل از فرآیند پیونددهنده امضاء و/یا فرآیند ابطال امضاء باشد.

۶-۶ فرآیند باز کردن عضویت گروه

فرآیند باز کردن که در شکل ۵ نشان داده شده است توسط بازکننده عضویت گروه صورت می‌گیرد و بازکننده را قادر می‌سازد تا شناسانه تشخیص امضاءکننده‌ی امضای ناشناس را تعیین کند.



شکل ۵- فرآیند باز کردن عضویت گروه



شکل ۶- فرآیند ارزیابی شواهد

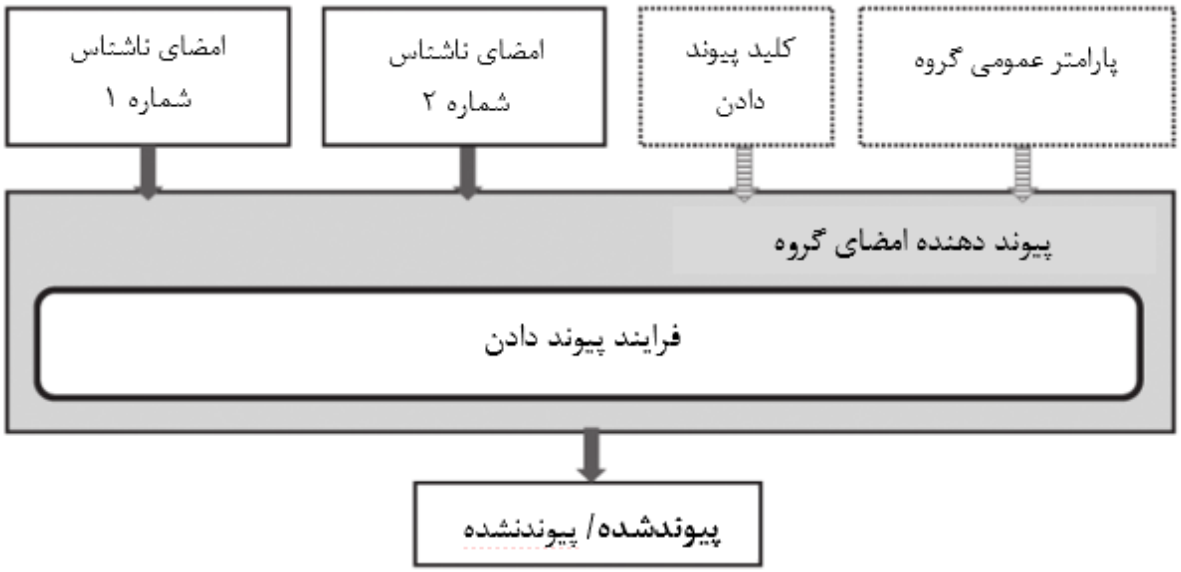
بسته به سازوکار، ممکن است فرآیند باز کردن شامل فرآیند ارزیابی شواهد باشد. اگر ارزیابی شواهد موردنیاز باشد، در فرآیند باز کردن، بازکننده عضویت گروه، شواهد انقیاد را ایجاد می‌کند که نشان می‌دهد که یک امضای معین از نظر رمزنگاشتی به شناسانه تشخیص امضاء کننده ملزم می‌شود. فرآیند ارزیابی شواهد که در شکل ۶ نشان داده شده است توسط ارزیاب شواهد صورت می‌گیرد که بر اساس شواهد انقیاد وارسی می‌کند که آیا بازکننده به‌درستی امضاءکننده را از امضای معین، شناسایی کرده است یا خیر. اگر ارزیاب متقاعد شود که امضاء با شواهد انقیاد هماهنگ است، آن را معتبر اعلام می‌کند در غیر این صورت آن را نامعتبر می‌داند.

یادآوری- دلایل مختلفی وجود دارند که چرا فرآیند بازکننده ممکن است شامل فرآیند ارزیابی شواهد باشد. در کل اگر لازم باشد نتیجه‌ی فرآیند باز کردن توسط ارزیاب بیرونی بررسی شود، فرآیند ارزیابی شواهد استفاده می‌شود. اینکه چگونه تصمیم گرفته شود که فرآیند ارزیابی سند به‌عنوان بخشی از فرآیند باز کردن در نظر گرفته شود، خارج از دامنه‌ی این قسمت از استاندارد ISO/IEC 20008 است.

۶-۷ فرآیند پیونددهنده امضای گروه

فرآیند پیونددهنده امضاء گروه که در شکل ۷ نشان داده شده است با پیوند امضای گروه انجام می‌شود که وارسی می‌کند آیا دو امضای معتبر ارائه‌شده توسط امضاءکننده‌ی یکسانی ایجاد شده‌اند یا خیر. بسته به سازوکار، پیونددهنده‌ی امضای گروه ممکن است کلید پیونددهنده داشته باشد. هم‌چنین بسته به سازوکار، فرآیند پیونددهنده امضای گروه ممکن است شامل پایه پیوند باشد که ممکن است توسط پیونددهنده امضای گروه ایجاد شده باشد. اگر چنین پایه پیوندی نیاز باشد، در فرآیند امضای گروه در زمان ایجاد هر دو امضاء استفاده می‌شود.

یادآوری- سازوکاری که در فرآیند پیونددهنده نقش دارد دارای ویژگی قابلیت پیوند کنترل‌شده توسط کاربر یا قابلیت پیوند قابل‌کنترل است (به‌طور مثال [۱۴]).



شکل ۷- فرآیند پیونددهنده امضای گروه

۶-۸ فرآیند ابطال امضای گروه

۶-۸-۱ کلیات

سه «سطح» مختلف ابطال می‌تواند برای سازوکار امضای دیجیتال ناشناسی که از کلید عمومی گروه استفاده می‌کند تعریف شود. این سه سطح اجازه ابطال انواع مختلفی از مجوزدهی را می‌دهند.

۶-۸-۲ ابطال سطح ۱

کل گروه باطل می‌شود. اگر نیاز باشد که مجوز کل گروه باطل شود، کلید عمومی گروهی مناسب باید به فهرست ابطال عمومی گروهی اضافه شود. هر امضای دیجیتال ناشناس مرتبط با کلید عمومی گروهی ابطال‌شده باید رد شود. این روش ابطال، مشابه همان روش استفاده‌شده در طرح امضای دیجیتال متداول است.

یادآوری- سازوکارهای این نوع ابطال، در ISO/IEC 20008-2 مشخص نشده‌اند.

۶-۸-۳ ابطال سطح ۲

عضویت عضو مشخص‌شده گروه باطل می‌شود و در نتیجه عضو باطل‌شده دیگر مجوز ایجاد امضاهای گروه را از طرف گروه ندارد. این کار با استفاده از یکی از روش‌های زیر انجام می‌شود.

الف- صادرکننده‌ی عضویت گروه، کلید عمومی گروه را به‌روزرسانی می‌کند (که ممکن است به‌روزرسانی کلید خصوصی خودش و/یا پارامترهای عمومی گروه را در بربگیرد یا نگیرد). صادرکننده سپس گواهی همه‌ی امضاء کنندگان قانونی را با استفاده از کلید عمومی جدید گروه به‌روزرسانی می‌کند. در کاربردهای بعدی فرآیند امضای گروه، فرآیند درستی‌سنجی، فرآیند بازکننده و فرآیند پیوند، کلیدها و گواهی‌های تازه به‌روز شده، استفاده خواهند شد. بسته به سازوکار، این روش به‌روزرسانی ممکن است هرگاه که صادرکننده عضویت گروه بخواهد تا اعضاء خاصی از گروه را ابطال کند یا در هر دو مورد به‌طور منظم صورت گیرد.

یادآوری ۱ - این روش ابطال به ابطال مبتنی بر کلید دهی مجدد یا ابطال به‌روزرسانی گواهی نیز شناخته می‌شود.

یادآوری ۲- بسته به سازوکار یکی از دو روش مختلف می‌توانند در این روش ابطال در برگرفته شوند. در روش اول، صادرکننده گروه با هر عضو قانونی گروه تعامل دارد تا کلید امضای عضویت اعضاء را به‌روزرسانی کند. در روش دوم، صادرکننده گروه اطلاعات عمومی معینی را ایجاد می‌کند و سپس هر عضو قانونی گروه کلید امضای عضویت گروهی خود را مطابق با این اطلاعات به‌روزرسانی می‌کند.

ب- روش دیگر از فهرست ابطال سراسری گروه استفاده می‌کند. محتوای چنین فهرست ابطالی به سازوکار بستگی دارد و تعدادی از موارد کلی در بخش زیر مشخص می‌شوند. امضای دیجیتال ناشناس مرتبط با مجوز مشخص‌شده در فهرست ابطال سراسری گروه، باید توسط تصدیق‌کننده‌ی امضای گروه رد شود.

این سطح ابطال همان‌طور که در شکل ۸ بخش الف نشان داده شده است به ابطال سراسری معروف است. تعدادی از سازوکارهای ابطال سراسری در ISO/IEC 20008-2 مشخص شده‌اند.

یادآوری- بسته به سازوکار، دو روش ابطال در این سطح مجاز است با هم استفاده شوند؛ برای مثال اطلاعات در مورد به‌روزرسانی کلید عمومی گروه و گواهی‌های عضویت گروه مجاز است در فهرست ابطال سراسری گروه در برگرفته شوند. چنین فهرست ابطال گروه توسط تصدیق‌کننده استفاده می‌شود تا کلید عمومی گروه را به‌روزرسانی کند یا توسط امضاء کننده به کار می‌رود تا کلید امضای عضویت گروه را به‌روزرسانی کند.

۶-۸-۴ ابطال سطح ۳

مجوز اعضای گروه برای ایجاد نوع خاص امضای ناشناس توسط تصدیق‌کننده‌ی امضاء ابطال می‌شود. تصدیق‌کننده می‌تواند با استفاده از فهرست ابطال محلی تصدیق‌کننده به سطح ابطال دست یابد. هر امضای دیجیتال ناشناسی که با مجوز مشخص‌شده در فهرست ابطال محلی تصدیق‌کننده مرتبط است، توسط تصدیق‌کننده‌ی خاصی، رد می‌شود. این سطح ابطال در شکل ۸ بخش ب نشان داده شده است. تعدادی از سازوکارهای ابطال محلی در ISO/IEC 20008-2 مشخص شده‌اند.

یادآوری ۱- این نوع ابطال، به ابطال محلی تصدیق‌کننده نیز شناخته می‌شود.

یادآوری ۲- در این نوع ابطال اگرچه تصدیق‌کننده، سازوکار ابطال را اجرا می‌کند اما مجاز است نداند که امضاء کننده‌ی باطل‌شده چه کسی است.

۶-۸-۵ فهرست‌های ابطال

در کل، فهرست ابطال توسط فردی ایجاد می‌شود که مورد اعتماد کاربران فهرست است و یا توسط خود کاربر ایجاد می‌شود. فهرست ابطال برای مشخص کردن اختیار خاصی برای ایجاد امضای دیجیتالی که ابطال شده است استفاده می‌شود. معمولاً استفاده از فهرست ابطال برای وارسی اعتبار امضاء، بخشی از فرآیند درستی‌سنجی امضاء را تشکیل می‌دهد. بسته به محتوای فهرست ابطال، برخی از سازوکارهای ابطال به امضاء کننده‌ای نیاز دارند که ثابت کند امضاء کننده، اختیار ایجاد امضاء را بر اساس فهرست ابطال در زمان امضاء دارد؛ سازوکارهای ابطال دیگر فقط نیاز دارند که تصدیق‌کننده، فهرست ابطال را در طول فرآیند بررسی امضاء وارسی کند. بسته به سازوکار، فهرست ابطال مجاز است به یک پارامتر منفرد، برای وارسی و اثبات کارآمد، فشرده‌سازی شود. اثبات کردن نباید اطلاعات حساسی را راجع به حریم خصوصی امضاء کننده نشان دهد.

یادآوری- سازوکاری که فهرست ابطال را به یک پارامتر منفرد فشرده می‌کند به انباشتگر[1] معروف است.

سه نوع فهرست ابطال متناظر با سه سطح ابطال وجود دارد.

الف- فهرست ابطال کلید عمومی گروه. چنین فهرستی باید توسط مرجع مورد اعتمادی ایجاد شود و شامل کلیدهای عمومی ابطال‌شده گروه است. بسته به سازوکار، این فهرست مجاز است به‌عنوان بخشی از هر فرآیندی وارسی شود که در آن کلید عمومی گروه استفاده می‌شود.

ب-فهرست ابطال سراسری گروه. چنین فهرستی باید توسط صادرکننده گروه یا مرجع مورد اعتماد در سطح گروه دیگری ایجاد شود و توسط تصدیق‌کننده‌ی امضای گروه استفاده شود. محتوای چنین فهرست ابطالی به سازوکار تعداد موارد خاصی شامل فهرست ابطال کلید خصوصی و فهرست ابطال گواهی عضویت و فهرست ابطال امضای گروه بستگی دارد.

پ- فهرست ابطال محلی تصدیق‌کننده. چنین فهرستی می‌تواند توسط خود تصدیق‌کننده یا توسط هستار دیگری ایجاد شود و توسط تصدیق‌کننده پذیرفته شود و فقط توسط آن استفاده شود. محتوای چنین فهرست ابطالی به سازوکار و تعداد موارد کلی شامل فهرست ابطال فهرست سیاه متعلق به تصدیق‌کننده و فهرست ابطال امضای گروه بستگی دارد. بسته به سازوکار تصدیق‌کننده مجاز است فهرست ابطال سراسری را به‌عنوان بخش یا کل فهرست ابطال محلی تصدیق‌کننده بپذیرد.

محتوای لیست ابطال می‌تواند متفاوت باشد که در مثال‌های زیر بیان شده است.

الف- در «ابطال کلید خصوصی»، کلید امضای خصوصی امضاء کننده‌ی ابطال‌شده در فهرست ابطال مشخص شده است و تصدیق‌کننده می‌تواند وارسی کند که آیا امضای ارائه‌شده با استفاده از چنین کلیدی ایجاد شده است یا خیر. چنین فهرستی می‌تواند در ابطال سراسری و هم‌چنین ابطال محلی استفاده شود.

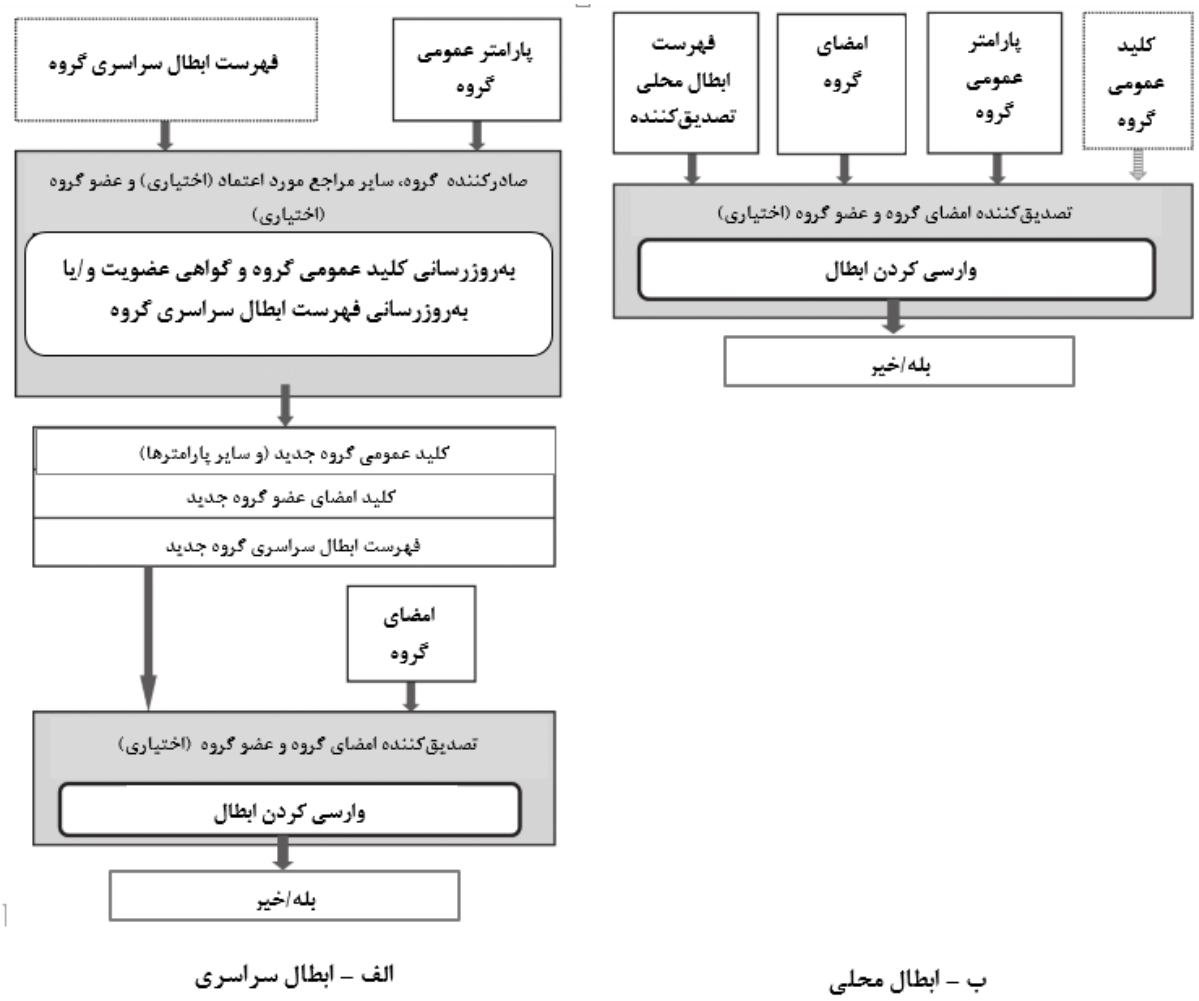
ب- در «ابطال گواهی عضویت»، گواهی عضویت گروه امضاء کننده‌ی ابطال‌شده در فهرست ابطال قرار می-گیرد و ممکن است نیاز باشد تا امضاء کننده اثبات کند گواهی عضویت امضاکننده در فهرست نیست. بسته به سازوکار چنین فهرستی می‌تواند در ابطال سراسری استفاده شود.

پ- در «ابطال فهرست سیاه تصدیق‌کننده»، امضاء (امضایی ناقص) متناسب با پایه پیوند امضا در فهرست ابطال می‌گنجد و تصدیق‌کننده می‌تواند وارسی کند که آیا امضای ارائه‌شده توسط امضاءکننده‌ای ایجاد شده است که امضای فهرست شده را ایجاد کرده است یا خیر. چنین فهرستی می‌تواند در ابطال محلی استفاده شود.

ت- در «ابطال امضاء»، امضاء (امضایی ناقص) در فهرست ابطال گنجانده می‌شود و تصدیق‌کننده می‌تواند وارسی کند که آیا امضای ارائه‌شده به همراه جزئی از شواهد ارائه‌شده توسط امضاء کننده توسط همان

1 - Accumulator

امضاءکننده‌ای ایجاد شده است که امضای فهرست شده را ایجاد کرده است یا خیر. بسته به سازوکار چنین فهرستی می‌تواند در ابطال محلی یا سراسری استفاده شود.



شکل ۸- فرآیندهای ابطال امضای گروه

۷ سازوکارهایی که از کلیدهای عمومی چندگانه استفاده می‌کنند

۷-۱ مدل کلی

سازوکار امضای دیجیتال ناشناسی که از کلید عمومی چندگانه استفاده می‌کند به سازوکار امضای حلقه نیز معروف است. سازوکار امضای حلقه مجموعه‌ای از امضاءکنندگان احتمالی را در برمی‌گیرد. هر امضاءکننده احتمالی یک جفت کلید امضاء به همان شکل سازوکار امضای متداول را دارد. این امضاءکننده‌های احتمالی مستقل از یکدیگر هستند، یعنی نیازی نیست که بر سر فرآیند امضای یکسانی، توافق داشته باشند. یکی از آن‌ها امضاءکننده‌ی واقعی است و دیگری (دیگران) امضاءکننده (گان) بالقوه است. امضاءکننده‌ی واقعی امضاءکننده‌ی بالقوه را انتخاب می‌کند و گروه را تشکیل می‌دهد.

سازوکار امضای حلقه با مشخصات فرآیندهای زیر تعریف می‌شود:

- فرآیند تولید کلید،

- فرآیند امضای حلقه،
- فرآیند درستی‌سنجی امضای حلقه

۷-۲ هستارها

سه نوع هستار درگیر سازوکار امضای دیجیتال ناشناسی هستند که از کلید عمومی چندگانه استفاده می‌کند و در ادامه ارائه‌شده‌اند:

- امضاءکننده‌ی واقعی: امضاءکننده‌ی واقعی هستاری است که امضای دیجیتال را ایجاد می‌کند.
- امضاءکننده‌ی بالقوه: امضاءکننده‌ی بالقوه هستاری است که کلید عمومی آن در ایجاد امضای دیجیتال استفاده‌شده است، به این معنا که کلید عمومی هم در فرآیند امضاء و هم در فرآیند درستی‌سنجی امضاء استفاده‌شده است، اگرچه امضاءکننده‌ی بالقوه در این دو فرآیند هیچ اقدامی نمی‌کند.
- تصدیق‌کننده: تصدیق‌کننده هستاری است که امضای دیجیتالی را بررسی می‌کند.

۷-۳ فرآیند تولید کلید

فرآیند ایجاد کلید مجموعه‌ای از فرآیندهای درستی‌سنجی تولید کلید و امضاء را در برمی‌گیرد. جفت‌های کلید امضاء به‌طور مستقل از یکدیگر تولید می‌شوند.

۷-۴ فرآیند امضای حلقه

در فرآیند امضاء، امضاءکننده‌ی واقعی، امضاءکننده‌ی بالقوه (مجموعه‌ای از امضاءکنندگان بالقوه) را انتخاب می‌کند و پیامی را با استفاده از کلید امضای خصوصی خودش و کلید (های) درستی‌سنجی عمومی امضاءکنندگان بالقوه، بدون نیاز به تأیید یا کمک آن‌ها امضاء می‌کند.

۷-۵ فرآیند درستی‌سنجی امضای حلقه

در فرآیند درستی‌سنجی، تصدیق‌کننده از کلیدهای عمومی امضاءکننده‌ی واقعی و امضاءکننده (گان) بالقوه درگیر در فرآیند امضاء استفاده می‌کند تا امضاء را بررسی کند. تصدیق‌کننده وارسی می‌کند که آیا امضاء توسط یکی از امضاءکنندگان مجموعه بدون دانستن اینکه کدام‌یک امضاءکننده‌ی واقعی است امضاء شده است یا خیر.

کتاب‌نامه

[1] ISO/IEC 9594-8:2008, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks — Part 8*

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

[3] ISO/IEC 9798 (all parts), *Information technology — Security techniques — Entity authentication*

[4] ISO/IEC 10118 (all parts), *Information technology — Security techniques — Hash-functions*

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

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

[7] ISO/IEC 11889 (all parts):2009, *Information technology — Trusted Platform Module*

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

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

[10] ISO/IEC 15945:2002, *Information technology — Security techniques — Specification of TTP services to support the application of digital signatures*

[11] ISO/IEC 18033-2:2006, *Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers*

[12] ISO/IEC 20008-2, *Information technology — Security techniques — Anonymous digital signatures — Part 2: Mechanisms using a group public key*

[13] ISO/IEC 20009 (all parts), *Information technology — Security techniques — Anonymous entity authentication*

[14] Brickell E., Chen L., Li J. Simplified security notions of direct anonymous attestation and a concrete scheme from pairings. *Int. J. Inf. Secur.* 2009, **8** (5) pp. 315–330