INSO

17748

1st Edition

2014

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

استاندارد ملی ایران

۱۷۷۴۸

چاپ اول

۱۳۹۲

فناوری اطلاعات - فنون امنیتی - الزامات برای اصالت‌سنجی تا حدودی گمنام، تا حدودی غیرپیوندپذیر

Information technology — Security techniques — Requirements for partially anonymous, partially unlinkable authentication

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 حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، 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، سازمان‌های دولتی و غیر دولتی حاصل می‌شود . پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون‌های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش نویس استانداردهایی که مؤسسات و سازمان‌های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. 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 می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی 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 می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه-بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی 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 – الزامات برای اصالت‌سنجی تا حدودی گمنام، تا حدودی غیرپیوندپذیر»

رئیس :	**سمت و/ یا نمایندگی**
کمرخانی، حبیب (فوق لیسانس IT- امنیت)	رئیس قسمت تحقیقات و پژوهش بنادر و کشتی‌رانی ایران
دبیر:	
بی‌مانند، هدی (لیسانس مهندسی کامپیوتر)	کارشناس رایانه و آمار اداره کل استاندارد ایلام
اعضاء : (اسامی به ترتیب حروف الفبا)	
اکبری، علی (لیسانس مهندسی برق،الکترونیک)	کارشناس مسؤول فناوری اطلاعات هلال احمر ایلام
بشارتی، یاسر (لیسانس مهندسی کامپیوتر)	کارشناس رایانه جهاد دانشگاهی ایلام
جستجو، صفورا (لیسانس مهندسی کامپیوتر)	کارشناس فنی سامانه الکترونیک ارتباط مردمی(سامد) استانداری ایلام
حیدری، نرگس (فوق لیسانس مهندسی کامپیوتر)	عضو هیأت علمی دانشگاه آزاد اسلامی ایلام
عبدی، اسرا (لیسانس مترجمی زبان اتگلیسی)	مدرس جهاد دانشگاهی ایلام
فرهاد شیخ احمد، لیلا (فوق لیسانس مهندسی کامپیوتر-نرم‌افزار)	کارشناس استاندارد تهران
مرادی، افسانه (لیسانس مهندسی کامپیوتر)	کارشناس آموزش و پرورش استان البرز

فهرست مندرجات

پیش‌گفتار

استاندارد « فناوری اطلاعات - فنون امنیتی - الزامات برای اصالت‌سنجی تا حدودی گمنام، تا حدودی غیرپیوندپذیر » که پیش نویس آن در کمیسیون‌های مربوط توسط سازمان ملی استاندارد ایران تهیه و تدوین شده است و در سیصد و سی امین اجلاس کمیته ملی استاندارد رایانه و فراوری داده مورخ ۹۳/۱۲/۲۰ 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 ماخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است :

ISO/IEC 29191:2012, Information technology — Security techniques — Requirements for partially anonymous, partially unlinkable authentication

فناوری اطلاعات - فنون امنیتی - الزامات برای اصالت‌سنجی تا حدودی گمنام، تا حدودی غیرپیوندپذیر

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ملی، تعیین الزامات و چارچوبی برای اصالت‌سنجی تا حدودی گمنام، تا حدودی غیرپیوندپذیر است.

۲ اصطلاحات وتعاریف

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

۲-۱

اصالت‌سنجی[1]

تمهیدی برای تضمین هویت یک هستار است.

[منبع: ISO/IEC 18014-2[2]]

۲-۲

مدعی[3]

مدعی، هستار یا نمایانگری از یک اصل،به منظور اصالت سنجی است.

[به استاندارد ملی ایران شماره ۱۰۸۲۵-۱: سال ۱۳۹۱ مراجعه شود]

۲-۳

اعتبارنامه[4]

هویت را بازنمایی می‌کند.

[منبع: ISO/IEC 24760-1]

---

1 - authentication

۲ – استاندارد بین‌المللی ISO/IEC 18014-2:2002، در سال ۱۳۸۷ با شماره ملی ۱۱۳۱۰-۲ منتشر شده است.

3 - claimant

4 - credential

۴-۲

بازکننده تعیین شده[1]

هستاری است که می‌تواند مدعی را از رونوشت اصالت‌سنجی، باز شناسایی کند.

یادآوری- توصیه می‌شود، انتخاب بازکننده تعیین شده، پیش از تراکنش انجام شود. هستار و یا هستارهایی که انتخاب می‌کنند ممکن است با پیاده‌سازی متفاوت باشد. همان‌طورکه باز کننده تعیین شده دارای توانایی شناسایی مدعی است، انتخاب بازکننده‌ی تعیین شده و نیز انتخاب رونوشت اصالت‌سنجی ارائه شده به بازکننده‌ی تعیین شده نیاز به دقت در انجام آن دارد.

۵-۲

هویت[2]

مجموعه‌ای از صفت‌های مربوط به هستار است.

[منبع: ISO/IEC 24760-1]

۶-۲

شناسایی مجدد[3]

مدعی را با دنبال کردن اصالت‌سنجی تا حدودی گمنام، تا حدودی غیرپیوندپذیر تعیین هویت می‌کند.

یادآوری- همچنین شناسایی مجدد، بازکردن نامیده می‌شود.

۷-۲

رونوشت اصالت‌سنجی

سابقه ای[4] از توالی‌های داده های مبادله شده ناشی از فرآیند اصالت‌سنجی است.

۳ کلیات

بسیاری از سازوکارهای رمزنگاری در دسترس هستند و امروزه برای بهبود امنیت فرآیند اصالت‌سنجی مورد استفاده قرار می‌گیرند. این امر زمانی منجر به اعتماد بیشتری می‌شود که به دنبال اصالت‌سنجی موفقیت‌آمیز، یک هستار، دسترسی مناسبی را به منابع حفاظت شده با استفاده از برخی از فرآیند صدور مجوز[5] بدهد . توجه داشته باشید که جزییات صدور مجوز خارج از محدوده‌ی این استاندارد است و بنابراین

1 - designated opener
2 - Identity
3 - re-identification
4 - Record
5 - Authorization

در پرانتز مشخص شده‌اند. اصالت‌سنجی نوعی و مدل صدور مجوز شامل مراحل زیر است(به طور معمول هر مرحله شامل تعدادی از زیرمرحله است، که بسیاری از آن‌ها در استاندارد ISO/IEC 29115 موجود است)

الف) نام نویسی[1]

ب) اصالت‌سنجی

پ) صدور مجوز

در استفاده امروزی، اکثر سازوکارهای رمزنگاشتی[2] ، نیاز به آشکارسازی از اطلاعات قابل شناسایی دارد و ردگیری هستار را در سراسر تراکنش فعال می‌کند. به عنوان مثال، استفاده از کلیدهای عمومی می‌تواند نام واقعی هستار را پنهان کند. با این حال، اگر کلید عمومی یا نام مستعار یکسانی برای اصالت‌سنجی‌های چندگانه استفاده شود، آن را می‌توان در پیوند دادن اطلاعات در مورد هستار در سراسر تراکنش مورد استفاده قرار داد و همین‌طور یک رخ‌نما[3] ایجاد کرد.

اما گمنامی و غیرپیوندپذیر بودن کامل ممکن است همیشه مطلوب نباشد. به عنوان مثال، یک هستار می‌تواند گمنامی را برای خروج از جریمه در بهره برداری از یک سامانه استفاده کند. بنابراین، در حالی که گمنامی و غیرپیوندپذیر بودن ممکن است در برخی شرایط مناسب باشد، مواردی وجود دارد که ممکن است لازم باشد تا به طرفین معینی، توانایی شناسایی مجدد هستار را ارائه شود.

برای دست‌یابی به هدف کلی اصالت‌سنجی تا حدودی گمنام، تا حدودی غیرپیوندپذیر، مراحل فرایند به شرح زیر است:

الف- ثبت[4]/نام نویسی، جهت دست‌یابی به گمنامی شامل راه‌اندازی برای رسیدن به گمنامی است.

ب- اصالت‌سنجی

پ- (صدور مجوز)

ت- شناسایی مجدد (در زمان مناسب)

۴ چارچوب

به منظور درک مرورکلی چارچوب، فرانامه‌ی[5] معمولی به عنوان مثال ارائه شده است که مدعی با نام نویسی یک خدمت آغاز می‌کند. این خدمت شامل یک صادرکننده است که اعتبارنامه‌ها را ایجاد و آن‌ها را برای مدعی صادر می‌کند. سپس مدعی ، اعتبارنامه‌ها را برای اصالت‌سنجی استفاده می‌کند. در صورتی که

1 - Enrollment
2 - Cryptographic
3 - profile
4 - Registration
5 - Scenario

اصالت‌سنجی موفقیت‌آمیز باشد، یک رونوشت از اصالت‌سنجی ایجاد می‌شود. این رونوشت باید شامل اطلاعات لازم برای فعال کردن شناسایی مجدد توسط بازکننده‌ی تعیین شده باشد، هرچند که ممکن است شامل چیزهای دیگری باشد. اگر شناسایی مجدد مورد نیاز باشد، رونوشت اصالت‌سنجی به بازکننده‌ی تعیین شده که قبل از هر تراکنشی داده می‌شود، باید ایجاد و با اجزای رمزنگاشتی لازم برای شناسایی مجدد ارائه شود. هر سامانه مجموعه شیوه‌ها و اصول خود را برای تعیین این که چه زمان شناسایی مجدد مناسب یا ضروری است، دارا است. این جزییات در دامنه این استاندارد نیست. اصول از قبیل آشکار بودن[1]، شفافیت[2] و توجه بسیار در استاندارد ISO/IEC 29100 توضیح داده شده است.

هر برنامه کاربردی الزامات خود را خواهد داشت، بنابراین هر پیاده‌سازی خاص ممکن است از جریان توصیف شده در بالا، اختلاف داشته باشد. به عنوان مثال، اعتبارنامه‌های مبتنی بر رمزنگاشتی را می‌توان به جای صادرکننده توسط مدعی ایجاد کرد؛ یا اعتبارنامه‌ها ممکن است به صورت الکترونیکی یا به نفسه صادر شود. اما این قبیل اختلافات، جنبه‌های اساسی چارچوب را تغییر نمی‌دهد.

این چارچوب مجموعه‌ای از نقش‌ها و عملیات‌هایی را تعریف می‌کند که در شکل ۱ نشان داده شده است.

این چهار نقش عبارتند از:

الف- صادرکننده - هستاری که اعتبارنامه‌ها را برای مدعی صادر می‌کند.

ب- مدعی - هستاری که توسط یک بازبینی‌کننده، اصالت‌سنجی خواهد شد.

پ- بازبینی‌کننده - هستاری که بازبینی می‌کند که آیا مدعی دارای اعتبارنامه معتبر است یا خیر.

ت- بازکننده‌ی تعیین شده - هستاری که می‌تواند مدعی را شناسایی مجدد کند.

در میان چهار نقش فوق، چهار عملیات اساسی در این چارچوب وجود دارد.

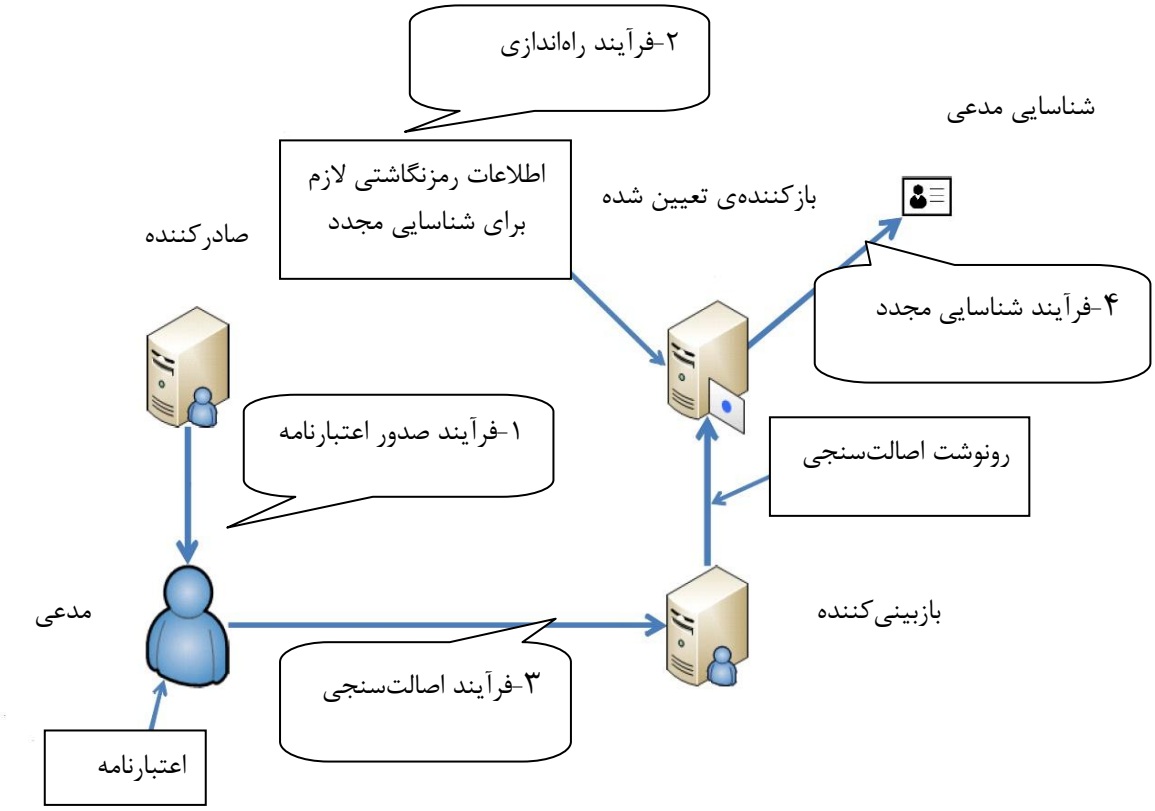
۱- فرآیندی بین صادرکننده و مدعی جهت انجام فرآیند صادرکننده اعتبارنامه است. پس از این فرآیند، مدعی یک اعتبارنامه دارد.

۲- فرآیندی برای بازکننده‌ی تعیین شده جهت راه‌اندازی رمزنگاشتی اطلاعات لازم برای شناسایی مجدد است.

۳- فرآیندی بین مدعی و بازبینی‌کننده جهت انجام اصالت‌سنجی است که رونوشت اصالت‌سنجی ایجاد می‌کند. اصالت‌سنجی در صورتی که بازبینی‌کننده بتواند تعیین کند مدعی دارای اعتبارنامه معتبر است، موفقیت‌آمیز است.

1 - Openness
2 - Transparency

۴- فرآیندی توسط بازکننده‌ی تعیین شده جهت شناسایی مدعی از رونوشت اصالت‌سنجی است، که شناسایی مجدد نامیده می‌شود. در این فرآیند، یک بازکننده‌ی تعیین شده از رونوشت اصالت‌سنجی استفاده می‌کند و ممکن است از اطلاعات دیگری که جهت فعال کردن شناسایی مجدد مناسب باشد، استفاده کند.



شکل۱- چارچوب اصالت‌سنجی تا حدودی گمنام، تا حدودی غیرپیوندپذیر

۵ الزامات

اصالت‌سنجی تا حدودی گمنام، تا حدودی غیرپیوندپذیر باید تمام الزاماتی را که در زیر توصیف شده برآورده سازد.

الف- مدعی باید توسط بازبینی‌کننده بدون این‌که توسط بازبینی‌کننده قابل شناسایی باشد، تایید اعتبار شود.

جهت گمنام باقی ماندن مدعی برای بازبینی‌کننده، تراکنش نباید زمانی که به بازبینی‌کننده اجازه‌ی تایید این را می‌دهد که مدعی دارای اعتبار نامه معتبر است، هر گونه اطلاعاتی را جهت شناسایی مدعی ارائه کند.

ب- رونوشت اصالت‌سنجی نباید به خودی خود بتواند اطلاعاتی را ارائه کند که بتواند تراکنش‌های اصالت‌سنجی چندگانه را توسط همان مدعی پیوند دهد.

جهت غیرقابل‌پیوند باقی ماندن مدعی برای بازبینی‌کننده، تراکنش جهت پیوند تراکنش‌های چندگانه توسط همان مدعی، نباید هر گونه اطلاعاتی را ارائه دهد.

پ- رونوشت اصالت‌سنجی باید شامل اطلاعات لازم برای بازکننده‌ی تعیین شده جهت شناسایی مجدد مدعی باشد.

بازکننده تعیین شده جهت داشتن توانایی شناسایی مجدد مدعی در بعد، رونوشت حاصل از یک تراکنش موفق باید اطلاعاتی را جهت شناسایی مدعی ارائه کند. توجه داشته باشید، بازکننده‌ی تعیین شده ممکن است جهت فعال کردن شناسایی مجدد، اطلاعات دیگری را استفاده کند که مناسب باشد.

ت- بازکننده‌ی تعیین شده باید بتواند مدرکی ارائه دهد که تعیین هویت مدعی درست است.

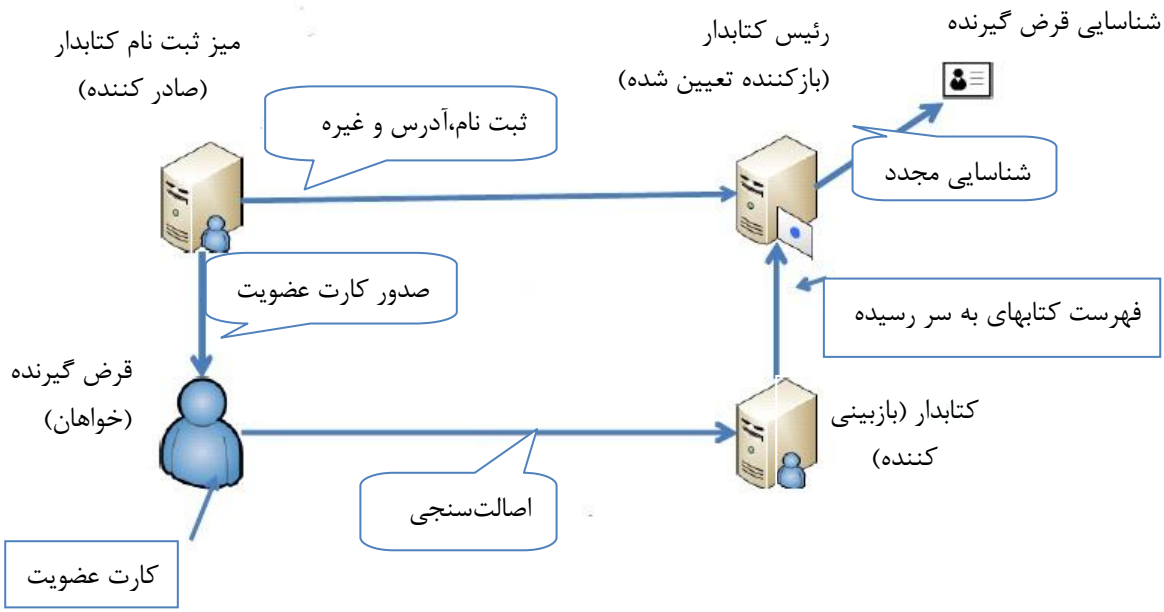
به منظور جلوگیری از ادعاهای متقلبان توسط بازکننده تعیین شده، بازکننده‌ی تعیین شده باید بتواند مدرکی ارائه کند که رویه برای شناسایی مجدد به درستی انجام می‌شود.

پیوست الف
(اطلاعاتی)
مثال کاربردی

الف-۱ مثال کاربردی در کتابخانه

در برخی از کشورها، فهرستی از کتاب‌ها که یک فرد از یک کتابخانه به امانت می‌گیرد حساس در نظر گرفته می‌شود زیرا این فهرست می‌تواند اندیشه‌های فردی، وجدان و مذهب را نشان دهد. به دلیل این حساسیت، امانت‌گیرندگان ممکن نیست بخواهند نام خود را در فهرستی از کتاب‌هایی که توسط آن‌ها به امانت گرفته، پیوند دهند. در همین زمان، کتابخانه ممکن است به ارتباط عنوان یک کتاب امانت گرفته شده با نام امانت گیرنده نیاز داشته باشد (به عنوان مثال، اگر کتاب در تاریخ مقرر بازگردانده نشود). اصالت‌سنجی تا حدودی گمنام، تا حدودی غیرپیوندپذیر می‌تواند در این فرانامه می‌توانند استفاده شود.

کتابدار (صادر کننده) میز نام نویسی در کتابخانه، یک کارت عضویت و قواعد را برای شناسایی مجدد به فرد (مدعی) که می‌خواهد کتاب به امانت بگیرد، ارائه می‌کند. هنگامی که فرد می‌خواهد کتابی را به امانت بگیرد، باید کارت عضویت را به کتابدار (بازبینی‌کننده) ارائه کند تا بررسی کند فرد عضو کتابخانه بوده و رویه وارسی کتاب را انجام دهد. یک سابقه تراکنش ایجاد شده و در دادگان ذخیره می‌شود که کتابخانه می‌تواند مدیریت و ردگیری کتاب به امانت گرفته شده را انجام دهد. همه افراد در این دادگان، گمنام باقی می‌مانند و تراکنش‌های وارسی نمی‌تواند به هم پیوند داده شود.



شکل الف-۱-مورد استفاده کتابخانه

اگر فرد یک کتاب را بیش از مدت امانت‌گیری نگه دارد، دادگان، رییس کتابخانه (بازبینی کننده) را آگاه می‌سازد که می‌تواند نام امانت‌گیرنده‌ی کتاب به تعویق افتاده را شناسایی و به فرد مربوطه اطلاع مناسبی دهد، آگاه می‌سازد.

الف-۲ مثال کاربردی در سامانه ترافیک هوشمند

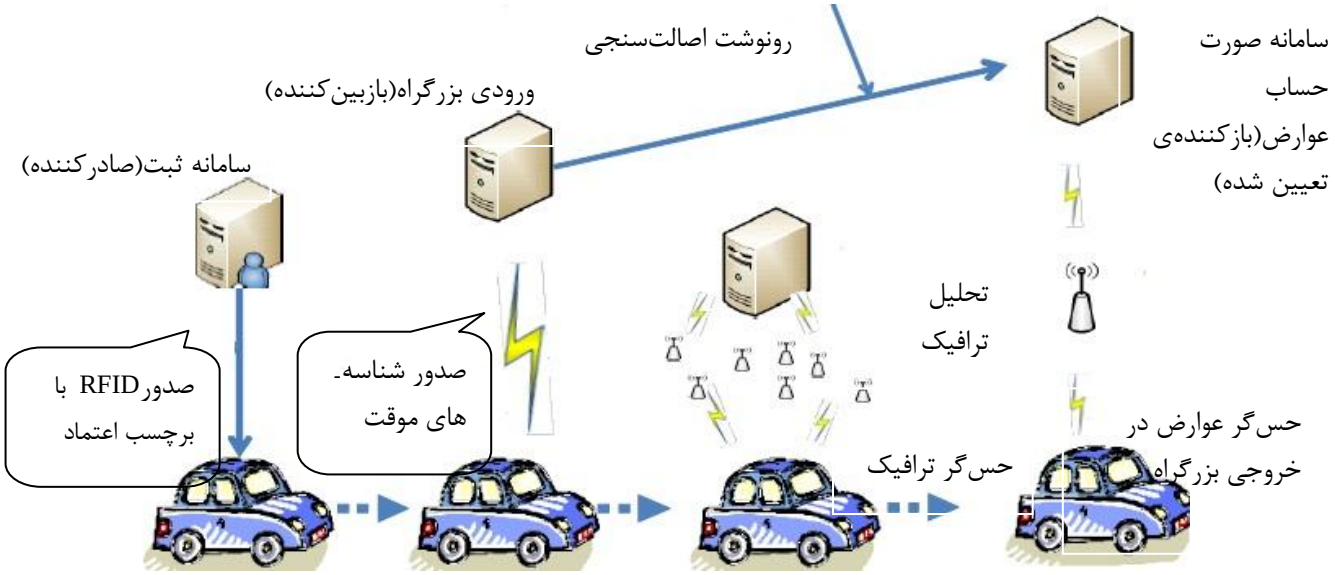
اندازه‌گیری‌های دقیق، تحلیل زمان واقعی و پیش‌بینی تراکم ترافیک و جریان خودروها در بزرگراه‌ها برای مشارکت‌کنندگان جهت بهبود جریان ترافیک، امنیت و پایداری مهم است. ردیابی دقیق از ماشین در بزرگراه‌ها بسیار مهم است. از سوی دیگر، توانایی ردیابی هر خودرو در زمان واقعی به شیوه‌ای مداوم به طور بالقوه دارای کاربرد حریم خصوصی است. اصالت‌سنجی تا حدودی گمنام، تا حدودی غیرپیوندپذیر را می‌توان در این فرانامه برای حمایت از نیازهای سامانه مدیریت ترافیک هوشمند با حفظ حریم خصوصی رانندگان استفاده کرد .

برای کاربران مسیر اغلب علامتی صادر می‌شود که می‌تواند با شیوه بدون تماس خوانده شود. در ورودی بزرگراه بین شهری، علامت خود را با استفاده از اصالت‌سنجی تا حدودی گمنام، تا حدودی غیرپیوندپذیر اصالت‌سنجی کرده و شناسانه موقتی را دریافت می‌کند که تا زمانی که ماشین از بزرگراه خارج شود، استفاده می‌شود.

با ورود این شناسانه موقت، مرکز کنترل ترافیک هوشمند می‌تواند یک فهرست از هر یک از ماشین‌ها، زمان ورود و زمان خروج به بزرگراه را بدون دانستن شناسانه‌ی دائمی از هر خودرو ایجاد کند. این فهرست را می‌توان برای انجام تحلیل زمان واقعی جریان ترافیک یا برای کنترل جریان توسط رد دسترسی ماشین‌ها در بخش متراکمی از بزرگراه مورد استفاده قرار داد. همچنین می‌توان آن را در طرح‌ریزی ظرفیت درباره الگوهای واقعی مورد استفاده قرار داد.

هنگامی که یک ماشین با یک شناسانه موقت از یک ایستگاه عوارض راهداری عبور کند، سامانه پرداخت عوارض صدور مجوز استفاده خدمات شناسایی را می‌دهد، که می‌تواند شناسانه موقت را به صورت حساب خودرو تبدیل کنید. در شرایط دیگری که ممکن است که از صدور مجوزها تقاضای شناسایی مجدد شود، توصیه می‌شود برای کاربر پیش‌رو شناخته شده باشد.

این مورد استفاده نشان می‌دهد که چگونه یک سامانه با استفاده از اصالت‌سنجی تا حدودی گمنام، تا حدودی غیرپیوندپذیر، را می‌توان با اهداف چندگانه مورد استفاده قرار داد.



شکل الف-۲- مورد استفاده ITS

پیوست ب

(اطلاعاتی)

برنامه کاربردی ساز وکار به منظور اصالت‌سنجی داده و حفاظت داده

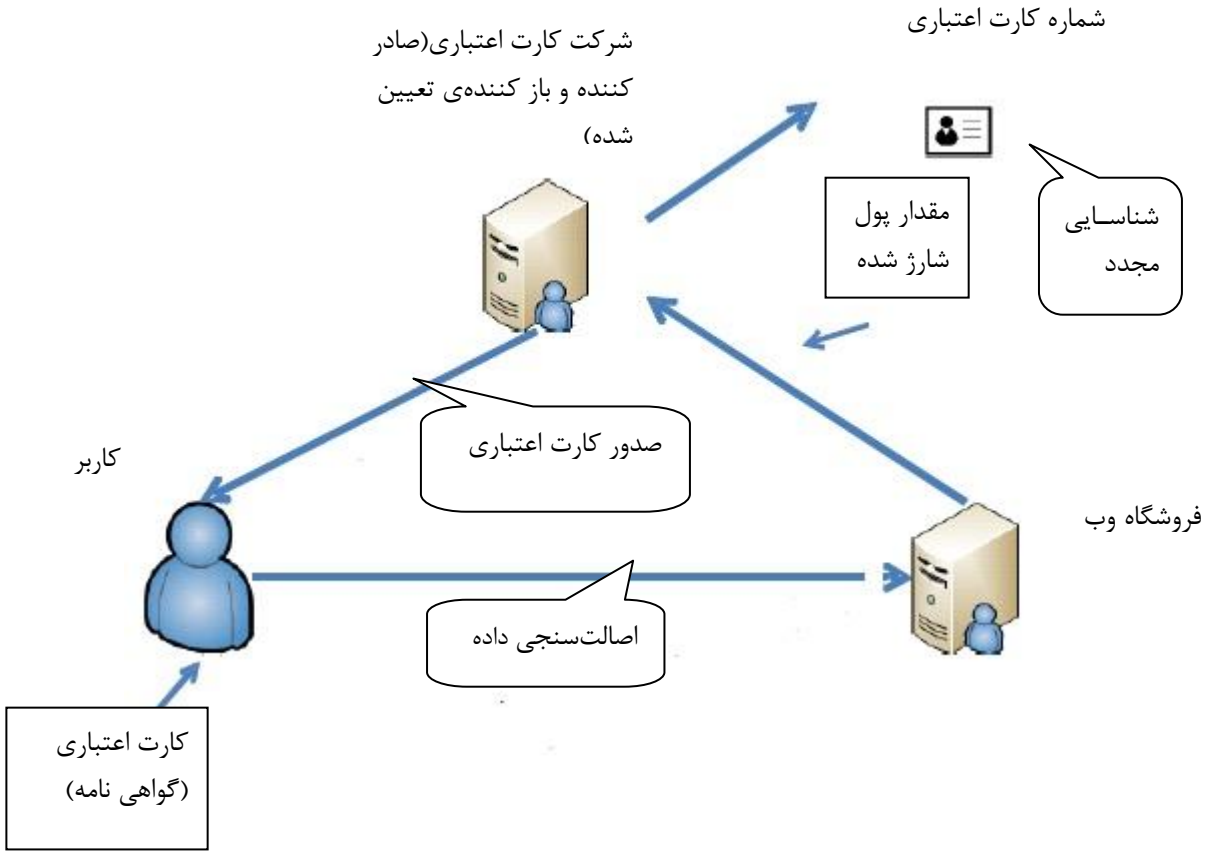
در این پیوست، ارائه یک برنامه کاربردی ارائه می‌شود که همان سازوکار را برای اصالت سنجسی داده به کار می‌رودکه در زمانی که برخی از اطلاعات را اگر چه کاربر گمنام نباشد از کاربر پنهان می‌کند، برای اصالت‌سنجی داده به خدمت می‌گیرد. در فرانامه‌ی نمونه زیر، اطلاعات پنهانی، یک شماره حساب، از قبیل شماره حساب بانکی و شماره کارت اعتباری است.

کاربران دارای حساب‌های صدور صورت حساب، از قبیل حساب‌های بانکی و حساب‌های کارت اعتباری هستند. هنگام خرید در فروشگاه وب، مهم است که کاربر یک حساب صدور صورت حساب قانونی داشته باشد. با این حال انتقال شماره حساب دقیق به فروشگاه وب مخاطره است، که ممکن است فروشگاه وب مورد سوء استفاده قرار گیرد. از سوی دیگر، این مخاطره برای فروشگاه وب در دریافت چنین شماره حساب دقیق از مشتری وجود دارد و فروشگاه‌های وب ممکن است نیاز به پرداخت هزینه اضافی برای نگه داشتن این داده‌ی امن از قانون شکنی‌ها باشد. اصالت‌سنجی تا حدودی گمنام، تا حدودی غیرپیوندپذیر، را می‌توان در این فرانامه جهت اصالت‌سنجی داده و حفاظت از داده استفاده کرد.

صدور حساب به کاربران توسط یک بانک یا کارت اعتباری شرکت انجام خواهد گرفت. کاربرانی وجود خواهند داشت که مایل به خرید برخی از محصولات از فروشگاه وب هستند.در فروشگاه وب یک بسته نرم‌افزاری موجود است که حساب قانونی کاربر را بررسی می‌کند، در صورتی که کاربر آن حساب را داشته باشد، می‌تواند فرآیند خرید و فروش کالا را انجام دهد. بازکننده‌ی تعیین شده نقش بانک یا شرکت کارت اعتباری را بازی می‌کند.

کاربر هنگام افتتاح حساب بانکی خود یا حساب کارت اعتباری درگیر در فرآیند صدور با هر یک از دو بانک یا شرکت کارت اعتباری خواهد بود. کاربر اعتبارنامه را دریافت می‌کند. زمانی که کاربر قصد خرید برخی از کالاها در فروشگاه وب را دارد، کاربر درگیر اصالت‌سنجی کاربر در فروشگاه وب است که نشان می‌دهد کاربر یک حساب قانونی در بانک یا شرکت کارت اعتبار را دارا است. با استفاده از اصالت‌سنجی تا حدودی گمنام، تا حدودی غیرپیوندپذیر، فروشگاه وب می‌تواند بدون یادگیری شماره حساب دقیق آن کاربر، کنترل کند که کاربر یک حساب قانونی را در این سازمان دارد. ورود به سامانه نام کالا، تاریخ خرید و نام بانک یا شرکت کارت اعتباری حساب کاربر، با یک رونوشت از طریق اصالت‌سنجی داده ایجاد می‌شود. رونوشت شماره حساب دقیق آن را نشان نمی‌دهد. رونوشت غیرقابل پیوند، غیر ممکن است که داده ثبت شده کالاهای دیگر را که با استفاده از همان شماره حساب خریداری شده است را پیدا کند. فروشگاه وب از این رونوشت به سازمان مدعی می‌گذرد. سازمان، بانک یا کارت اعتباری شرکت، فرآیند شناسایی مجد را بر روی رونوشت انجام می‌دهد و با موفقیت حساب دقیق صورت حساب را به دست می‌آورد.

کاربر آسوده است که فروشگاه وب شماره حساب او را یاد نمی‌گیرد و فروشگاه وب آسوده است که نیازی به یادگیری این چنین اطلاعات حریم خصوصی ندارد.



شکل ب-۱- پنهان کردن صورت حساب

کتاب‌نامه

[1]Advances in Cryptology -- EUROCRYPT ’91 Lecture Notes in Computer Science 547 Springer 1991, pp. 257-265, Chaum and van Heyst: “Group Signatures.”

[2]Advances in Cryptology -- CRYPTO '98, Lecture Notes in Computer Science 1462 Springer 1998, pp. 169-185, Kilian and Erez Petrank: “Identity Escrow.”

[3]Security in Communication Networks (SCN 2004) Lecture Notes in , Camenisch and Groth: “Group Signatures: Better Efficiency and New Theoretical Aspects.”

[4]Information Security and Privacy, 10th Australasian Conference(ACISP 2005) Lecture Notes in Computer Science 3574 Springer 2005, pp. 455-467, Furukawa and Imai: “An Efficient Group Signature Scheme from Bilinear Maps.”

[5]Proceedings of the 2006 Workshop on Digital Identity Management (IDM 2006) ACM, Isshiki, Mori, Sako, Teranishi and Yonezawa: “Using group signatures for identity management and its implementation.”.