INSO
17253-1
1st.Edition
Mar.2014

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

استاندارد ملی ایران
۱۷۲۵۳-۱
چاپ اول
اسفند ۱۳۹۲

فن آوری اطلاعات - فنون امنیتی- اصالت سنجی هستار ناشناس: قسمت ۱: عمومی

Information technology-security techniques- Anonymous entity authentication - Part1 : 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 کشورازآخرین 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 صدور گواهی 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 اصالت 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- اصالت سنجی هستار ناشناس: قسمت ۱: عمومی"

رئیس:	**سمت و/ یا نمایندگی**
رودکی، مصطفی (فوق لیسانس مهندسی برق)	مدیر تولید صنایع قطعات الکترونیک
دبیر:	
ظل‌انوار، محمد علی (لیسانس مهندسی برق)	کارشناس اداره کل استاندارد فارس
اعضاء: (اسامی به ترتیب حروف الفبا)	
ابراهیمی، علی اکبر (فوق لیسانس مخابرات)	کارشناس صنایع قطعات الکترونیک
پروا، بهروز (لیسانس مهندسی صنایع)	کارشناس اداره کل استاندارد فارس
جاویدی، محمد جواد (لیسانس شیمی)	کارشناس سازمان صنعت معدن تجارت
حکم طلعت، هادی (فوق لیسانس الکترونیک)	کارشناس صنایع قطعات الکترونیک
صداقت، عزیز (لیسانس کامپیوتر)	کارشناس صنایع قطعات الکترونیک
عطروش، حسینعلی (لیسانس مهندسی برق الکترونیک)	کارشناس اداره کل استاندارد فارس

کاووسی، زهرا (فوق لیسانس مهندسی فناوری اطلاعات)	کارشناس سازمان صنعت معدن تجارت
کشتگری، منیژه (دکتری مهندسی کامپیوتر)	استادیار دانشگاه صنعتی شیراز
مغانی، مهدی (کارشناس ارشد ریاضی کاربردی)	کارشناس سازمان فناوری اطلاعات

فهرست مندرجات

پیش گفتار

استاندارد " فناوری اطلاعات- فنون امنیتی- اصالت سنجی هستار ناشناس قسمت ۱: عمومی"که پیش نویس آن درکمیسیون های مربوط توسط سازمان ملی استاندارد ایران تهیه و تدوین شده و در سیصد و بیست و دومین اجلاس کمیتهٔ ملی استاندارد رایانه و فرآوری داده ها مورخ ۱۳۹۲/۱۱/۲۸مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ ، به عنوان استاندارد ملی ایران منتشر می‌شود .

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

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

ISO/IEC 20009-1:2013, Information technology- security techniques - Anonymous entity authenticaton- part 1: general

فناوری اطلاعات - فنون امنیتی- اصالت سنجی هستار ناشناس: قسمت ۱: عمومی

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد تعیین یک مدل، الزامات و محدودیت ها برای مکانیزم های اصالت سنجی هستار ناشناس که قانونی بودن یک هستار را تایید می‌کند، می باشد.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد به آن ها ارجاع شده است. بدین ترتیب آن مقررات جزئی از این استاندارد زیر محسوب میشود. در مورد مراجع دارای تاریخ چاپ و / یا تجدید نظر، اصلاحیه ها و تجدید نظرهای بعدی این مدرک مورد نظر نیست. معهذا بهتر است کاربران ذینفع این استاندارد، امکان کاربرد آخرین اصلاحیه ها و تجدید نظرهای مدرک را مورد بررسی قرار دهند. در مورد مراجع بدون تاریخ چاپ و / یا تجدید نظر، آخرین چاپ و / یا تجدید نظر آن مدارک الزامی ارجاع داده شده مورد نظر است.
استفاده از مراجع زیر برای کاربرد این استاندارد الزامی است:

- هیچ

۳ اصطلاحات و تعاریف

۱-۳

قدرت تشخیص [1]

عدد مشتق شده از احتمال تعیین صحیح امضا کننده واقعی از امضا ارائه شده توسط یک هستار غیرمجاز

یادآوری- قدرت تشخیص n به این معنا است که احتمال اینکه یک هستار غیرمجاز بتواند امضا کننده واقعی را از یک امضا حدس بزند برابر است با $\frac{1}{n}$

(منبع: ISO/IEC 20008-1)

۲-۳

اصالت سنجی هستار ناشناس

تایید یک هستار با صفات معین بدون تمایز قائل شدن با دیگر هستارهای همسان

1- Anonymity strength

۳-۳

امضا دیجیتال ناشناس

امضایی که بتواند با استفاده از یک راهنمای عمومی گروهی یا راهنماهای عمومی چندگانه تایید شود ونتواند با شناسه متمایز امضا کننده خود توسط هر هستار غیرمجاز از جمله تایید کننده امضا،ردیابی شود.

(منبع: ISO/IEC 20008-1)

۴-۳

چالش[1]

اقلام داده تصادفی انتخاب شده و ارسالی توسط تایید کننده به متقاضی که توسط متقاضی مورد استفاده قرار گرفته و در ارتباط با اطلاعات محرمانه ی نگهداری شده توسط متقاضی جهت ارائه یک پاسخ برای تایید کننده ارسال می شود.

(منبع : ISO/IEC 9798-1: 2010)

۵-۳

متقاضی

هستاری که یک اصل را برای اهداف اصالت سنجی بیان می کند.

(منبع : ISO/IEC 9798-1: 2010)

۶-۳

کلید

دنباله ای از نمادها که عملکرد یک تغییر شکل پنهانی را کنترل می‌کند.

(منبع : ISO/IEC 9798-1: 2010)

۷-۳

پیوند دهنده

هستاری که عمل پیوند دادن را انجام می دهد.مثال: پیوند دو یا تعداد بیشتری از نمونه های اصالت سنجی هستار ناشناس

۸-۳

پیوند دادن

فرایندی که در آن انجام دو یا تعداد بیشتری از نمونه‌های اصالت سنجی هستار ناشناس توسط یک هستاریکسان نشان داده شده است.

1- challenge

۹-۳

باز کننده[1]

هستار مجاز که عمل افتتاح را انجام می دهد. **مثال**: یادگیری هویت قسمتی که در یک نمونه ویژه از یک مکانیزم اصالت سنجی هستار ناشناس به کار گرفته شده است.

یادآوری- یک افتتاح کننده، به یک افتتاح کننده تعیین شده در استاندارد ISO/IEC 29191 ارجاع داده می شود.

۱۰-۳

باز کردن

فرایندی که یک هستار مجاز، هویت قسمتی را که در یک نمونه ویژه از یک مکانیزم اصالت سنجی هستار ناشناس به کار گرفته شده، فرا می گیرد.

یادآوری- عمل افتتاح، به تشخیص هویت مجدد در استاندارد ISO/IEC 29191 ارجاع داده می شود.

۱۱-۳

اصالت سنجی ناشناس متقابل

اصالت سنجی هستار ناشناس که هر دو هستار را با اطمینان از درستی هستار دیگر، تامین می‌نماید.

۱۲-۳

اصالت سنجی ناشناس بخشی

اصالت سنجی هستار ناشناس که اجازه افتتاح بوسیله هستارهای مجاز را می‌دهند.

۱۳-۳

اصل

هستاری که درستی آن می تواند احراز شود.

۱۴-۳

عدد تصادفی

پارامتر متغیر زمان که مقدار آن غیرقابل پیش بینی می باشد.

(منبع: ISO/IEC 9798-1: 2010)

۱۵-۳

عدد دنباله

پارامتر متغیر زمان که مقدار آن از یک دنباله معین در یک بازه زمانی غیرقابل تکرار به دست می آید.

(منبع: ISO/IEC 9798-1: 2010)

1-opener

۳-۱۶

مهر زمان [1]

پارامتر متغیر زمان که یک نقطه از زمان را در رابطه با یک مرجع مشترک مشخص می سازد.

(منبع: ISO/IEC 9798-1: 2010)

۳-۱۷

پارامتر متغیر زمان

اقلام داده مورد استفاده جهت تایید اینکه یک پیام بازپخش[2] نیست. **مثال**: یک عدد تصادفی، عدد دنباله یا مهر زمان

(منبع: ISO/IEC 9798-1: 2010)

۳-۱۸

نشانه[3]

پیامی شامل فیلدهای داده مرتبط با یک ارتباط ویژه و شامل اطلاعاتی که با استفاده از تکنیک‌های پنهانی تغییر شکل یافته اند.

(منبع : ISO/IEC 9798-1: 2010)

۳-۱۹

شخص ثالث مورد اعتماد

مرجع امنیتی یا نماینده آن که بوسیله دیگر هستارها و در رابطه با فعالیت های مرتبط امنیتی مورد اطمینان قرار گرفته است.

(منبع: ISO/IEC 9798-1: 2010)

۳-۲۰

اصالت سنجی ناشناس یک طرفه

اصالت سنجی هستار ناشناس که یک هستار را همراه با اطمینان از درستی هستار دیگر تامین می نماید.اما به صورت برعکس درست نیست.

۳-۲۱

اصالت سنجی متقابل ناشناس یک طرفه

نتیجه یک فرایند بین دو بخش که به طور همزمان اصالت سنجی هستار ناشناس را در یک جهت و اصالت سنجی هستار را در جهت دیگر تامین می نماید.

1- time stamp 3- token

2- replay

۲۲-۳

تایید کننده

هستاری که به اطمینان از درستی یک هستار دیگر نیاز دارد(متقاضی).

۴ نمادها واختصارات

۴-۱ نمادها

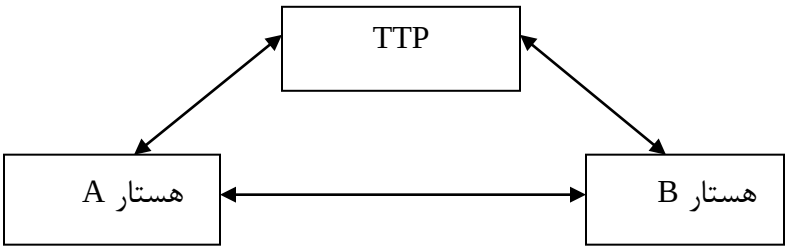
A : یک هستار شرکت کننده در یک مکانیزم اصالت سنجی هستار ناشناس

B : یک هستار شرکت کننده در یک مکانیزم اصالت سنجی هستار ناشناس

۴-۲ اختصارات

TTP : شخص ثالث مورد اعتماد

۵ مدل اصالت سنجی هستار ناشناس



شکل ۱- مدل اصالت هویت هستار ناشناس

مدل عمومی برای مکانیزم های اصالت سنجی هستار ناشناس در شکل ۱ نشان داده شده است.وجود تمام هستارها و مبادله ها در هر مکانیزم اصالت سنجی الزامی نمی باشد.

برای مکانیزم های اصالت سنجی هستار ناشناس تعیین شده در دیگر قسمت های استاندارد ISO/IEC 20009 و برای اصالت سنجی ناشناس یک طرفه، هستار A به عنوان متقاضی و هستار B به عنوان تایید کننده درنظر گرفته می شود.برای اصالت سنجی ناشناس متقابل هستار A و B هر دو نقش های مطالبه کننده و تاییدکننده را ایفا می کنند.برای اصالت سنجی متقابل ناشناس یک طرفه ، هستار A وB هردو نقش متقاضی و تایید کننده را ایفا می کنند و علاوه بر این یک جهت اصالت سنجی ناشناس بوده و جهت دیگر اینگونه نمی باشد(برای مثال: A هویت B را تایید می کند و B تایید می کند که A یک عضو از گروه هستارهای از پیش تعریف شده می باشد).

نقش دقیق و صریح TTP بستگی به مکانیزم مورد استفاده دارد.بعضی از مکانیزم ها ممکن است ازهیچ شخص ثالث مورد اعتماد استفاده نکنند.به طور متناوب یک TTP ممکن است فقط درگیر یک راه برون خطی[1] شود.
مثال: توسط تامین یک یا هر دو هستار A و B همراه با اطلاعاتی که استفاده از مکانیزم را مقدم بر کاربرد آن پشتیبانی می کند.به عنوان پیشنهاد سوم، یک TTP ممکن است به صورت فعال در مکانیزم توسط مبادله پیام ها با یک یا هر دو بخش در طول مدت زمان کاربرد مکانیزم درگیر شوند. یک TTP می تواند در فرایندهای بازکردن یا پیوند دادن درگیر شود.اگر یک TTP(درون خطی یا برون خطی) درگیر شود آنگاه TTP باید برای اهداف اصالت سنجی هستار ناشناس، مورد اطمینان بخش های درگیر باشد.
برای اهداف اصالت سنجی هستار ناشناس، هستارها پیام های همگون شده را تولید و مبادله می‌کنند که به آنها نشانه گفته می‌شود.هستارها مبادله حداقل یک نشانه برای اصالت سنجی ناشناس یک طرفه و حداقل دو نشانه برای اصالت سنجی ناشناس متقابل را انجام می دهند.اگر یک رقابت برای آغاز کردن یک مبادله اصالت سنجی هستار ناشناس ارسال شود آنگاه یک مجوز(گذر) اضافی ممکن است نیاز باشد.در صورتی که شخص ثالث مورد اعتماد درگیر باشد مجوزهای اضافی ممکن است مورد نیاز باشد.
در شکل ۱پیکان ها جریان بالقوه اطلاعات را نمایش می دهند.هستارهای A و B ممکن است به صورت مستقیم با یکدیگر اثر متقابل داشته باشند یا با شخص ثالث مورد اعتماد به ترتیب از طریق B یا A به صورت مستقیم اثر متقابل داشته باشند یا از اطلاعات به دست آمده توسط شخص ثالث مورد اعتماد استفاده نماید.
تبادل پیام که مکانیزم اصالت سنجی هستار ناشناس را بوجود می آورد، مدارکی را برای تاییدکننده دال برمعتبر بودن متقاضی تامین می نماید. **مثال**: عضویت گروه هستارهای از پیش تعریف شده.این مدارک شکل دانش اثبات شده را از طریق تکنیک های رمز نگاری اطلاعات محرمانه به خود می‌گیرند که فقط یک هستار مجاز مستحق آن می‌باشد.علاوه براین مکانیزم های معین اجازه اثبات متقاضی را به تایید کننده می دهد که این علاوه بر وجود یک هستار معتبر دارای صفات دیگر نیز می‌باشد.جزئیات مکانیزم‌های اصالت سنجی هستار ناشناس در استاندارد ISO/IEC 20009 در قسمت های بعدی از این استاندارد تعیین شده است.

۶ الزامات و محدودیت های کلی

برای اینکه یک هستار(مثال: تایید کننده) بتواند به صورت ناشناس هستار دیگررا احراز کند(مثال: متقاضی) تایید کننده و متقاضی هردو بایستی از مجموعه تکنیک های رمزنگاری و پارامترهای مشترک استفاده نمایند.
در طول عمر عملکردی یک کلید رمزنگاری، مقادیر تمام پارامترهای متغیر زمان که کلید در آن عمل می کند(مثال: مهرهای زمان، اعداد دنباله و اعداد تصادفی) نبایستی قابل تکرار باشند(حداقل با احتمال قریب به اتفاق).

1 – offline way

فرض بر این است که در طول استفاده از مکانیزم اصالت سنجی هستار ناشناس، هستار های A و B از وضعیت مورد ادعای یکدیگر آگاه می باشند برای مثال: گروهی که متقاضی ادعای عضویت در آن را دارد و وضعیت هستارها چگونه خواهد بود اگر مشخصه های اضافی مورد ادعا درست باشند.این ممکن است با گنجاندن داده (شامل رشته‌های داده تولید شده به صورت رمز نگاری)در اطلاعات مبادله شده بین دو هستار به دست آید یا ممکن است از مفهوم کاربرد مکانیزم آشکار گردد.

اصالت سنجی مطالبه کننده می تواند فقط برای لحظه مبادله اصالت سنجی هستار ناشناس معلوم گردد.

برای ضمانت صحت داده های مرتبط و متعاقب بین تایید کننده و متقاضی، مبادله اصالت سنجی هستار ناشناس بایستی در اتصال با وسایل ارتباطی ایمن مورد استفاده قرار گیرد(مثال: یک جلسه ارتباطی که مفهوم آن یکپارچگی حفاظت شده بوده و درجاییکه کلید محرمانه الزامی یا جفت کلید خصوصی/عمومی در طول مبادله اصالت سنجی هستار ناشناس برقرار شود از مکانیزم تمامیت داده مثل یک امضای دیجیتال یا رمز اصالت سنجی پیام استفاده می کند).

اگر اصالت سنجی ناشناس بخشی مورد نیاز باشد، متقاضی باید داده کافی را در طول مبادله اصالت سنجی برای توانمندسازی عمل سازی بازکردن متعاقب توسط موجودیت های مجاز تامین نماید.

۷ مدیریت ناشناس

درجه ناشناسی اختصاص داده شده به یک فرد متفاوت خواهد بود و بستگی به ویژگی های مکانیزم اصالت سنجی هستار ناشناس به کارگرفته شده و محیط مورد استفاده دارد.مثال:اگر یک هستارمالکیت یک صفت شناخته شده از مفهوم کاربرد تصرف شده توسط فقط دو فرد را ثابت کند آنگاه درجه ای که هستار، ناشناس باقی می‌ماند به طور واضح محدود خواهد بود.این درجه،مفهوم قدرت تشخیص را به عنوان اندازه مجموعه‌ای از هستارها درون یکدیگر تحریک می کند.در مثال بالا هستار با صفات یگانه دارای قدرت تشخیص ۲ می باشد.

در بعضی موارد ممکن است برای ناشناسی یک شرکت کننده در جلسه اصالت سنجی، بعد از استفاده یک مکانیزم در جاییکه این از دست دادن ناشناسی می تواند کامل یا محدود باشد ، لغو کردن ضروری باشد.دو موقعیت ویژه کاهش ناشناسی برای مثال افتتاح و پیوند دادن شناسایی شده است. پیوند دادن یک فرایند است که توسط یک هستار شناخته شده به عنوان پیوند دهنده انجام می شود که دو یا تعداد بیشتری نمونه های اصالت سنجی هستار ناشناس نمایش داده شده تا توسط هستار یکسان انجام شود و بیانگر مقداری از دست دادن ناشناسی می باشد. افتتاح یک فرایند است که یک هستار مجاز شناخته شده به عنوان یک باز کننده، هویت آن قسمت که در یک نمونه ویژه از مکانیزم اصالت سنجی هستار ناشناس به کار گرفته شده را فرا می گیرد و از دست دادن کامل ناشناسی را حداقل با در نظر گرفتن بازکننده بیان می کند. مهم است که ذکر گردد تمامی مکانیزم ها الزاما افتتاح یا پیوند دادن را حمایت نمی‌کنند.یک مکانیزم اصالت سنجی هستار ناشناس که بازکردن را توسط هستارهای مجاز ممکن می‌سازد به عنوان یک مکانیزم اصالت سنجی ناشناس بخشی شناخته می-

شود.یک مکانیزم اصالت سنجی هستارناشناس که افتتاح را توسط هستارهای مجاز ممکن می سازد و توانایی پیوند دادن را ندارد به عنوان یک مکانیزم بخشی، مکانیزم اصالت سنجی غیرقابل پیوند دادن بخشی شناخته می شود.