INSO

17642-1

1st. Edition

2014

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standardization Organization

استاندارد ملی ایران

۱۷۶۴۲-۱

چاپ اول

۱۳۹۲

فناوری اطلاعات- فنون امنیتی- چارچوب کاری برای مدیریت هویت-

قسمت ۱: واژگان و مفاهیم

Information technology - Security techniques - A framework for identity management - Part 1: Terminology and concepts

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- چارچوب کاری برای مدیریت هویت-

قسمت ۱: واژگان و مفاهیم »

رئیس:	**سمت و/ یا نمایندگی**
صفایی، سپیده (کارشناس کامپیوتر)	کارشناس نرم‌افزار شرکت داده‌کاوان امن‌پرداز
دبیر: منافی، علیرضا (کارشناس ارشد کامپیوتر)	مدیر عامل شرکت امن‌افزار گستر شریف
اعضاء: (اسامی به ترتیب حروف الفبا)	
اخوان نیاکی، سید انوشیروان (کارشناس ارشد مدیریت فناوری اطلاعات)	مشاور مدیر عامل و مدیر مرکز مدیریت دانش و داده کاوی شرکت ایزایران
مروجی، سجاد (کارشناس ارشد کامپیوتر)	مدرس دانشگاه
مهدوی، سید علیرضا (کارشناس ارشد مدیریت فناوری اطلاعات)	مشاور شرکت داده‌پردازان آبشار
عصمت علی محمد ملایری (کارشناس ارشد نرم‌افزار)	مدرس دانشگاه آزاد ملایر

فهرست مندرجات

پیش‌گفتار

استاندارد« فناوری اطلاعات- فنون امنیتی- چارچوب کاری برای مدیریت هویت-قسمت ۱: واژگان و مفاهیم» که پیش‌نویس آن درکمیسیون‌های مربوط توسط تهیه و تدوین شده و در دویست و شصت و هفتمین اجلاسیه کمیتهٔ ملی استاندارد. رایانه و فرآوری داده مورخ۱۳۹۲/۱۲/۸ مورد تصویب قرار گرفته است ، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ ، به‌عنوان استاندارد ملی ایران منتشر می‌شود .

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های 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 ارائهٔ شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت . بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

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

ISO/IEC 24760-1:2011 -Information technology - Security techniques –Aframework for identity management -Part 1: Terminology and concepts

مقدمه

سامانه‌های پردازش داده، به طور معمول، دامنهٔای از اطلاعات را در مورد کاربرانشان، که می‌تواند یک فرد، قطعه‌ای از تجهیزات یا نرم‌افزارهایی که در اتصال به آنها است، جمع‌آوری می‌کنند و تصمیمات را براساس اطلاعات جمع‌آوری شده اتخاذ می‌کنند. چنین تصمیماتی که مبتنی بر هویت هستند می‌توانند به دسترسی به برنامه‌های کاربردی یا دیگر منابع ارتباط داشته باشند.

در راستای توجه به نیاز به وجود سامانه‌هایی که به‌صورت کارآمد و موثر به‌کار گرفته می‌شوند تا تصمیمات مبتنی بر هویت را اتخاذ کنند، ISO/IEC 24760 چارچوب کاری را برای صدور، اجرا و استفاده از داده‌هایی که جهت مشخص کردن افراد، سازمان‌ها یا مولفه‌های فناوری اطلاعات که از طرف افراد یا سازمان‌ها به‌کار گرفته می‌شوند، تعیین می‌کند.

برای بسیاری از سازمان‌ها مدیریت مناسب اطلاعات هویتی جهت حفظ امنیت فرآیندهای سازمانی حیاتی است. برای افراد، مدیریت صحیح هویت جهت حفاظت از حریم شخصی از اهمیت برخوردار است.

ISO/IEC 24760 مفاهیم بنیادی و ساختارهای عملیاتی مدیریت هویت را با هدف درک مدیریت سامانه اطلاعاتی تعیین می‌کند، از این رو سامانه‌های اطلاعاتی می‌توانند التزام‌های تجاری، قراردادی، تنظیمی[1] و قانونی را برآورده کنند.

این استاندارد اصطلاحات و مفاهیم برای مدیریت هویت را جهت افزایش ادراک عمومی در حوزه مدیریت هویت تعیین می‌کند. این قسمت همچنین کتاب‌شناسی[2] اسناد مرتبط با استانداردسازی جنبه‌های گوناگون مدیریت هویت را نیز ارائهٔ می‌دهد.

1 - Regulatory
2 - bibliography

فناوری اطلاعات- فنون امنیتی- چارچوب کاری برای مدیریت هویت-قسمت ۱: واژگان و مفاهیم

۱ هدف و دامنهٔ کاربرد

هدف از تدوین این استاندارد تعیین

- اصطلاحات مدیریت هویت را تعریف می‌کند، و
- مفاهیم اصلی هویت و مدیریت هویت و ارتباط آنها را تعیین می‌کند.

این استاندارد برای هر سامانه اطلاعاتی که اطلاعات هویت را پردازش می‌کند کاربرد دارد.

کتاب‌شناسی اسناد که توصیف کننده جنبه‌های گوناگون مدیریت اطلاعات هویت است، ارائه می‌شود.

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

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به‌کار می‌رود:

یادآوری- اصطلاحات و تعاریف در این استاندارد مطابق با ISO/IEC 10241، استانداردهای واژگان بین‌المللی- آماده‌سازی و طرح‌بندی، پیش‌نویس شده است، که مشخص می‌کند اصطلاحات جایگزین که اغلب برای اصطلاحی که به‌صورت حروف سیاه برجسته بیان می‌شود، مورد استفاده قرار می‌گیرد، می‌تواند در یک خط جداگانه پیش از متن که اصطلاح را تعریف می‌کند، قرار گیرد. این استاندارد اصطلاح را تنها به‌صورت حروف سیاه برجسته استفاده می‌کند.

۳-۱ اصطلاحات عمومی

۳-۱-۱ هستار[1]

قسمتیء داخل یا خارج از سامانه فن‌آوری اطلاعات و ارتباطات، مانند یک فرد، سازمان، دستگاه یا زیرسامانه یا یک گروه از چنین قسمت‌هایی که به‌صورت قابل شناسایی متمایزند.

مثال- یک مشترک انسانی در یک سرویس مخابراتی، بنگاه دولتی، سیم کارت، گذرنامه، کارت واسط مشترک شبکه، وبگاه.

۳-۱-۲

هویت

هویت جزئی[2]

مجموعه‌ای از **صفت‌ها (۳-۱-۳)** مرتبط با یک **هستار (۳-۱-۱)**

1- Entity

2 -partial identity

یادآوری ۱- یک هستار می‌تواند بیش از یک هویت داشته باشد.

یادآوری ۲- چندین هستار می‌توانند دارای یک هویت مشابه باشند.

یادآوری۳- در یک دامنهٔ خاص کاربردپذیری، یک هستار می‌تواند به یک هویت متمایزکننده و یا یک شناسانه تبدیل شود تا این امکان را فراهم کند که هستارها متمایز شوند یا در آن دامنهٔ به طور منحصر به فرد شناسایی شوند..

یادآوری ٤ ITU-T $X1252$[13] استفاده متفاوت از هویت را تعیین می‌کند. در این بخس از ISO/IEC 24760 اصطلاح شناسه بر این وجه دلالت دارد.

۳-۱-۳

صفت

مشخصه یا صفت یک **هستار (۳-۱-۱)** که می‌تواند برای توصیف وضعیت، ظاهر یا دیگر جنبه‌های آن به‌کار رود.

یادآوری-کارکرد اصلی مفهوم یک صفت در این استاندارد باید یک جنبه خاص، به خوبی تعریف شده یک هستار در سامانه مدیریت هویت باشد. ارزش‌های صفت‌ها در یک هویت با هم، یک هستار را در یک دامنهٔ توصیف می‌کنند.

مثال-نوع هستار، اطلاعات نشانی، شمارهٔ تلفن، مزیت، نشانی MAC [1]، نام دامنهٔ صفت‌های امکان پذیر هستند.

۳-۱-۴

شناسانه[2]

هویت منحصر به فرد

هویت اختصاصی

اطلاعات هویتی (۳-۲-۴) که بدون ابهام یک **هستار (۳-۱-۳)** را از هستار دیگر در یک **دامنهٔ (۳-۲-۲)** معین متمایز می‌کنند.

یادآوری۱- یک شناسانه می‌تواند برای استفاده در خارج از دامنهٔ مفید باشد.

یادآوری۲- یک شناسانه می‌تواند یک صفت با یک ارزش اختصاص داده شده باشد.

یادآوری۳- یک شناسانه می‌تواند یک یا چند صفت باشد که تعیین می‌کند که آیا هویت با معیارهای تعیین شده مطابقت می‌کند و یا مطابقت نمی‌کند.

مثال- نامی از یک باشگاه با شمارهٔ عضویت باشگاه، شمارهٔ کارت بیمه سلامت همراه با نام شرکت بیمه، نشانی ایمیل، یا یک شناسانه منحصر به فرد کلی (UUID) می‌توانند همه به‌عنوان شناسانه مورد استفاده قرار گیرند. در یک ثبت کننده رأی، ترکیبی از صفت‌های نام، نشانی و تاریخ تولد برای تشخیص آشکار رأی‌دهنده کفایت می‌کند.

1- Media Access Control

2- identifier

۳-۱-۵

دامنهٔ منشاء

خصیصه یک **صفت (۳-۱-۳)** که **دامنهٔای (۳-۲-۳)** را که در آن صفت شکل گرفته است یا ارزش آن اختصاص یافته است تعیین می‌کند

یادآوری ۱- دامنهٔ منشاء نوعاً معنا و قالب ارزش صفت را تعیین می‌کند. چنین مشخصاتی می‌تواند مبتنی بر استانداردهای بین‌المللی باشد.

یادآوری ۲- یک صفت ممکن است دربرگیرنده یک ارزش آشکار باشد که مرجع آن دامنهٔ منشاء است، برای مثال کد ISO یک کشور برای شمارهٔ گذرنامه که مرجع آن کشور صادرکننده‌ای است که دامنهٔ منشاء اطلاعات هویتی در گذرنامه است.

یادآوری ۳- به‌صورت عملیاتی، دامنهٔ منشاء می‌تواند به‌عنوان یک منبع معتبر برای یک صفت (برخی مواقع به‌عنوان مرجع صفت شناخته می‌شود) در دسترس باشد. یک منبع معتبر می‌تواند خارج ار منشاء دامنهٔ واقعی عمل کند. منابع چندگانه معتبر می‌توانند برای دامنهٔ مشابه منبع وجود داشته باشند.

مثال- دامنهٔ منشاء یک شمارهٔ عضویت باشگاه یک باشگاه خاص است که شماره را اختصاص داده است.

۳-۱-۶

شناسه مرجع

RI

شناسه (۳-۱-۴) در یک **دامنهٔ (۳-۲-۳)** برای مدت زمانی که یک **هستار (۳-۱-۱)** در دامنهٔ شناخته می‌شود به‌صورتی در نظر گرفته می‌شود که یکسان باقی بماند و به دیگر هستارها برای دوره تعیین شده در یک خط مشیء پس از آن که شناخته شدن هستار در آن دامنهٔ متوقف شده است وابسته نباشد.

یادآوری ۱- یک شناسانه مرجع حداقل برای حضور هستار در یک دامنهٔ اصرار می‌کند و ممکن است به مدت طولانی تری نسبت به هستار باقی بماند، برای مثال برای اهداف بایگانی.

یادآوری ۲- یک شناسانه مرجع برای یک هستار می‌تواند طی دوره حیات یک هستار، در نقطه‌ای که شناسانه قدیمی دیگر برای آن هستار کاربرد ندارد، تغییر کند.

مثال - یک شمارهٔ گواهی نامه رانندگی که برای طول دوره رانندگی یک راننده یکسان باقی می‌ماند یک شناسانه ماندگار است، که مرجع اطلاعات هویتی افزوده است و این شماره یک شناسانه مرجع به شمار می‌آید. یک نشانی IP شناسانه مرجع نیست چراکه می‌تواند به دیگر هستارها اختصاص داده شود.

۳-۲ شناسایی

۳-۲-۱

شناسایی

فرآیند تشخیص **هستار (۳-۱-۱)** در یک **دامنهٔ (۳-۲-۳)** خاص که از دیگر هستارها متمایز است.

یادآوری ۱- فرآیند شناسایی برای درستی‌سنجی صفت‌های ادعا شده یا مشاهده شده به کار می‌رود.

یادآوری ۲- شناسایی، نوعاً، قسمتیء از تعاملات میان هستار و سرویس‌ها در یک دامنهٔ و جهت دستیابی به منابع است. شناسایی می‌تواند چندین بار هنگامی‌که هستار در دامنهٔ شناخته می‌شود رخ دهد.

۳-۲-۲

درستی‌سنجی

فرآیند تعیین اینکه **اطلاعات هویتی (۳-۲-۴)** ارائه‌شدهٔ مرتبط با یک **هستار (۳-۱-۱)** خاص برای هستاری که باید در یک **دامنهٔ(۳-۲-۲)** خاص در نقطه‌ای از زمان شناسایی شود قابل اجرا است

یادآوری- درستی‌سنجی می‌تواند شامل بررسی موجود بودن صفت‌های لازم، برخوردادری از نحو صحیح و هستار در یک دورهٔاعتبار تعریف شده، باشد.

۳-۲-۳

دامنهٔ

دامنهٔ کاربردپذیری

متن

DA

محیطی که در آن یک هستار (۳-۱-۱) می‌تواند مجموعه‌ای از صفت‌ها (۳-۱-۳) برای شناسایی (۳-۲-۱) و دیگر اهداف را به‌کار برد.

یادآوری ۱- به طور کلی دامنهٔ یک هویت در ارتباط با مجموعه‌ای خاص از صفت‌ها به خوبی تعریف می‌شود.

یادآوری ۲ ITU-T $X1252$[13] از متن اصطلاح استفاده می‌کند؛ این استاندارد دامنهٔ اصطلاح را ترجیح می‌دهد.

مثال- یک سامانه فناوری اطلاعات که به‌وسیلهٔ یک سازمان به‌کار گرفته می‌شود و به کاربران اجازهٔ ورود به سامانه را می‌دهد دامنه‌ای برای نام ورود به سامانه کاربر است.

۴-۲-۳

اطلاعات هویتی

مجموعه‌ای از ارزش‌های **صفت‌ها (۳-۱-۳)** به‌صورت اختیاری با هر فرادادهٔ مرتبط در یک **هویت (۳-۱-۲)**

یادآوری- در یک سامانه فناوری اطلاعات و ارتباطات یک هویت به‌عنوان اطلاعات هویتی وجود دارد.

۳-۳ اصالت‌سنجی یک هویت

۱-۳-۳

اصالت‌سنجی[1]

فرآیند رسمی درستی‌سنجی (۳-۲-۲) که در صورت موفقیت، به هویت اصالت‌سنجی شده (۳-۳-۲) برای یک هستار (۳-۱-۱) منجر می‌شود.

یادآوری ۱- فرآیند اصالت‌سنجی شامل آزمایش‌هایی به وسیلهٔ یک درستی‌سنج با یک یا چند صفت هویتی ارائهٔ شده به وسیلهٔ یک هستار جهت تعیین، با سطح مورد نیاز تضمین، صحت آنها است.

یادآوری ۲- اصالت‌سنجی نوعاً شامل استفاده از یک خط مشیء جهت تعیین سطح مورد نیاز تضمین برای نتیجهٔ یک اجرای موفق است.

1- authentication

یادآوری ۳- شناسایی به طور معمول به‌صورت اصالت‌سنجی صورت می‌گیرد تا نتیجه به‌صورت سطح معینی از تضمین به‌دست آید.

۲-۳-۳

هویت اصالت‌سنجی شده

اطلاعات هویتی (۳-۲-۴) برای یک **هستار (۳-۱-۱)** که جهت ثبت نتیجهٔ **اصالت‌سنجی (۳-۳-۱)** ایجاد شده است.

یادآوری ۱- یک هویت اصالت‌سنجی شده نوعاً شامل اطلاعات به‌دست آمده در فرآیند اصالت‌سنجی است، برای مثال سطح تضمین احراز شده.

یادآوری ۲- وجود یک هویت اصالت‌سنجی شده در یک دامنهٔ خاص مشخص می‌کند که یک هستار در آن دامنهٔ شناسایی شده است.

یادآوری ۳- هویت اصالت‌سنجی شده نوعاً طول عمری دارد که به وسیلهٔ یک خط مشیء اصالت‌سنجی شده است.

۳-۳-۳

مرجع اطلاعات هویتی

IIA

هستار (۳-۱-۱) مرتبط با یک **دامنهٔ** خاص**(۳-۲-۳)** که می‌تواند توضیحات قابل اثباتی را درمورد اعتبار و یا صحت یک یا چند ارزش **صفت (۳-۱-۳)** در یک **هستار (۳-۱-۲)** بیان کند.

یادآوری ۱-یک مرجع اطلاعات هویتی نوعاً به دامنهٔ مرتبط است، برای مثال دامنهٔ منشاء، که در آن صفت‌هایی که IIA می‌تواند برآن تاکید کند، دارای یک اهمیت خاص است.

یادآوری ۲-فعالیت یک مرجع اطلاعات هویت می‌تواند مشروط به خط مشیء حفاظت حریم شخصی باشد.

یادآوری ۳-یک هستار می‌تواند عملکردهای ارائهٔ دهندهٔ اطلاعات هویتی و مرجع اطلاعات هویتی را ترکیب کند.

۴-۳-۳

ارائهٔ دهندهٔ اطلاعات هویتی

ارائهٔ دهنده هویت

IIP

هستاری (۳-۱-۱) که اطلاعات هویتی (۳-۲-۴) در دسترس را ایجاد می‌کند

یادآوری- نمونه عملیات‌های اجرا شده به وسیلهٔ یک ارائهٔ دهنده اطلاعات هویتی، ایجاد و حفظ اطلاعات هویتی برای هستارهای شناخته شده در یک دامنهٔ خاص هستند. یک ارائهٔ دهنده اطلاعات هویتی و یک مرجع اطلاعات هویتی می‌توانند یک هستار مشابه باشند.

۵-۳-۳

اعتبارنامه

ارائهٔ یک هویت (۳-۱-۲)

یادآوری ۱-یک اعتبارنامه نوعاً، جهت تسهیل اصالت‌سنجی داده‌های اطلاعات هویتی در هویتی که ارائهٔ می‌دهد شکل می‌گیرد.

یادآوری۲- اطلاعات هویتی ارائهٔ شده به وسیلهٔ یک اعتبارنامه می‌تواند برروی کاغذ چاپ شود یا در یک نشانه [1] فیزیکی که به‌صورتی آماده شده اند تا اطلاعات را به‌صورت معتبر اثبات کنند، ذخیره شود.

مثال - یک اعتبارنامه می‌تواند یک نام کاربری، نام کاربری همراه با رمزعبور، PIN، کارت هوشمند، نشانه، اثرانگشت، گذرنامه و غیره باشد.

۶-۳-۳

درستی‌سنج

هستاری (۳-۱-۱) که عمل **درستی‌سنجی (۳-۲-۲)** را انجام می‌دهد

یادآوری-یک درستی‌سنج کننده می‌تواند مشابه با یا به جای هستاری که شناسایی هستارها را برای یک دامنهٔ خاص انجام می‌دهد عمل کند.

۷-۳-۳

قسمت مورد اطمینان

RP

هستاری (۳-۱-۱) که به **درستی‌سنجی (۳-۲-۲)** **اطلاعات هویتی (۳-۲-۴)** برای یک هستار خاص اطمینان دارد.

یادآوری- قسمت مورد اطمینان، در معرض خطری است که به‌وسیلهٔ اطلاعات هویتی نادرست ایجاد می‌شود. نوعاً، این قسمت دارای ارتباط مطمئن با یک یا چند مرجع اطلاعات هویتی است.

۸-۳-۳

اثبات هویت

شرح بیان شده از سوی یک **مرجع اطلاعات هویتی (۳-۳-۳)** مورد استفاده به وسیلهٔ **قسمت مورد اطمینان (۳-۳-۷)** جهت **اصالت‌سنجی (۳-۳-۱)**

یادرآوری-اثبات هویت می‌تواند اثبات رمزنگاشتی اصالت‌سنجی موفق باشد که با الگوریتم‌ها و کلیدهای مورد توافق میان قسمت‌ها ایجاد شود، برای مثال در یک اتحادیهٔ [2] هویت.

۹-۳-۳

تضمین هویت

سطح تضمین در نتیجهٔ **شناسایی (۳-۲-۱)**

یادآوری- تضمین هویت، سطح اطمینان در منشاء، یکپارچگی و کاربردپذیری اطلاعات هویتی شامل اطمینان در حفاظت اطلاعات هویتی را بیان می‌کند.

۳-۴ مدیریت هویت

۱-۴-۳

مدیریت هویت

IDM

1 -token
2 - federation

فرآیندها و خط مشیءهای دخیل در مدیریت چرخهٔ حیات و ارزش، نوع و فراداده‌های اختیاری **صفت‌ها (۳-۱-۳)** در **هویت‌های (۳-۱-۲)** شناخته شده در یک دامنهٔ خاص

یادآوری۱- به‌صورت کلی مدیریت هویت در تعامل میان قسمت‌هایی که اطلاعات هویتی پردازش می‌شوند دخیل است.

یادآوری۲- فرآیندها و خط مشیءها در مدیریت هویت از عملکردهای یک مرجع اطلاعات هویتی درجایی که قابل اجرا باشد پشتیبانی می‌کند، به طور خاص جهت اعمال تعامل میان یک هستار که هویت برای آن مدیریت می‌شود و مرجع اطلاعات هویتی.

۳-۴-۲

اثبات هویت

اصالت‌سنجی اولیه هستار

شکل خاص **اصالت‌سنجی (۳-۳-۱)** مبتنی بر شواهد **هویت (۳-۴-۴)** که به‌صورت شرط برای **ثبت**[1] **(۳-۴-۳)** اجرا می‌شود.

یادآوری ۱- نوعاً اثبات هویت شامل اصالت‌سنجی گسترده اطلاعات هویتی ارائهٔ شده می‌شود و می‌تواند غربالگری، بررسی و تطبیق منحصربه فرد بودن، احتمالا مبتنی بر فنون بیومتریک را شامل شود.

یادآوری ۲- اصالت‌سنجی در قلب محک هویت، نوعاً مبتنی بر یک خط مشیء ثبت است که شامل مشخصات معیارهای درستی‌سنجی شواهد هویتی ارائهٔ شده به وسیلهٔ هستار می‌شود.

یادآوری ۳- هویت اصالت‌سنجی شده که نتیجه اصالت‌سنجی در محک هویت است ممکن است طی ثبت متعاقب در ثبت نام وجود داشته باشد و می‌تواند جهت تسهیل شناسایی آتی هستار به‌کار رود.

۳-۴-۳

ثبت

فرآیند ایجاد یک **هستار (۳-۱-۱)** در یک **دامنهٔ (۳-۲-۳)** خاص

یادآوری۱- ثبت به ثبت نام هویت منجر می‌شود. اثبات هویت نوعاً جهت ایجاد اطلاعات هویتی جهت ثبت نام شدن برای یک هستار خاص اجرا می‌شود.

یادآوری۲- به طور کلی، ثبت‌نام اطلاعات هویتی را برای ذخیره‌سازی در یک ثبت هویت، تلفیق و ایجاد می‌کند تا در شناسایی بعدی هستار، در دامنه به کار رود.

۴-۴-۳

شواهد هویت

شواهدی برای هویت

اطلاعات هویتی (۳-۲-۴) برای یک **هستار (۳-۱-۱)** مورد نیاز برای **اصالت‌سنجی (۳-۳-۱)** آن **هستار (۳-۱-۱)**

یادآوری- شواهد هویت شامل اطلاعات ارائهٔ شده و جمع‌آوری‌شده شده مرتبط به یک خواهان است که برای یک اصالت‌سنجی موفق مورد نیاز است. هریک از چنین اطلاعاتی می‌تواند قسمتیء از هویت اصالت‌سنجی شده برای مدعی باشد.

۵-۴-۳

ثبت نام هویت

1 - enrolment

ثبت نام IMS

مخزن **هویت‌ها (۳-۱-۲)** برای **هستارهای (۳-۱-۱)** مختلف

یادآوری۱- یک نمونه از ثبت نام هویت به وسیلهٔ یک شناسانه مرجع فهرست (indexed) می‌شود.

یادآوری ۲- مرجع اطلاعات هویتی در یک دامنهٔ خاص نوعاً از ثبت نام هویتی خود استفاده می‌کند. اگرچه، یک ثبت نام هویت می‌تواند میان دامنه‌های مرتبط تقسیم شود، برای مثال میان هستار تجاری مشابه.

یادآوری ۳- قابلیت اطمینان اطلاعات هویتی در ثبت نام هویت به وسیلهٔ خط مشیءهای اصالت‌سنجی مورد استفاده طی ثبت، تعیین می‌شود.

۶-۴-۳

ثبت نام هویت

فرآیند ضبط اطلاعات **هویتی (۳-۲-۴) هستار (۳-۱-۱)** در یک **ثبت نام هویتی (۳-۴-۵)**

۷-۴-۳

مولد شناسانه مرجع

ابزار مورد استفاده طی **ثبت (۳-۴-۳)** جهت فراهم کردن یک ارزش منحصر به فرد جدید برای یک شناسانه **مرجع (۳-۱-۶)**

مثال-یک سامانه مدیریت پایگاه داده می‌تواند زمانی که شمارهٔ منحصر به فرد پرونده (رکورد) را به پروندهٔ جدید افزوده شده به جدول اختصاص می‌دهد و شمارهٔ پرونده به‌عنوان شناسانه مرجع مورد استفاده قرار می‌گیرد، مولّد شناسانه مرجع باشد.

۳-۵ اتحادیهٔ

۱-۵-۳

هویت متحد

هویت (۳-۱-۲) برای استفاده در چندین **دامنهٔ (۳-۲-۳)**، که با یکدیگر یک **اتحادیهٔ هویت (۳-۵-۲)** را شکل می‌دهند

یادآوری ۱-یک هویت متحد می‌تواند به‌صورت مشترک به وسیلهٔ فراهم‌کنندگان اطلاعات هویتی دامنه‌های متحد مدیریت شود.

یادآوری ۲- صفت‌های مشترک مورد استفاده در دامنه‌های متحد، می‌تواند به طور خاص جهت شناسایی مورد استفاده قرار گیرند، برای مثال جهت پشتیبانی از تک ثبت نام (SSO).

یادآوری ۳- هویت متحد می‌تواند ثابت یا موقتی باشد، برای مثال به‌صورت هویت تک ثبت نام.

۲-۵-۳

اتحادیهٔ هویت

توافق میان دو یا چند **دامنهٔ (۳-۲-۳)** مشخص کنندهٔ اینکه چگونه **اطلاعات هویتی (۳-۲-۴)** برای اهداف **شناسایی (۳-۲-۱)** میان دامنه‌ای مبادله و مدیریت خواهند شد.

یادآوری ۱- برقراری یک اتحادیهٔ هویت، نوعاً شامل توافق درمورد استفاده از پروتکل‌ها و رویه‌های متداول برای کنترل حریم شخصی، حفاظت داده‌ها و ممیزی می‌شود. توافق اتحادیهٔ می‌تواند استفاده از قالب‌های داده و فنون رمزنگاشتی استاندارد شده را معین کند.

یادآوری ۲- توافق اتحادیهٔ می‌تواند مبنایی برای مراجع هویت در هریک از دامنه‌های کاربردپذیری جهت شناسایی متقابل اعتبارنامه‌ها برای مجوز باشد.

۳-۵-۳

هویت تک ثبت نام

هویت SSO

هویتی (۳-۱-۲) که شامل درستی‌سنجی **هویت (۳-۳-۸)** منفرد است که می‌تواند به وسیلهٔ قسمت قابل **اطمینان (۳-۳-۷)** در **دامنه‌های (۳-۲-۳)** چندگانه **درستی‌سنجی (۳-۲-۲)** شود

یادآوری- درستی‌سنجی هویت در یک هویت تک ثبت نام، طی اصالت‌سنجی یک هستار در یک دامنهٔ ایجاد می‌شود و می‌تواند در اصالت‌سنجی هستار در هر دامنهٔ دیگر در اتحاد هویت مشابه مورد استفاده قرار گیرد.

۳-۶ حفاظت حریم شخصی

در حوزه‌هایی که انواع مشخصی از هستارهای قانونی، حق حفاظت حریم شخصی را اعطا کنند، اصطلاح 'فرد' در تعاریف پیش رو باید برای دربرگرفتن چنین هستارهایی تفسیر شود؛ در غیر این صورت، اصطلاح 'فرد' در ارتباط با یک انسان منفرد مورد استفاده قرار می‌گیرد.

۳-۶-۱

افشاء گزینشی

اصل مدیریت **هویت (۳-۴-۱)** که به یک فرد امکان سنجش کنترل بر اطلاعات **هویتی (۳-۲-۴)** را می‌دهد که می‌تواند به شخص ثالث انتقال یابد، برای مثال طی **اصالت‌سنجی (۳-۳-۱)**

۳-۶-۲

حداقل افشاء

اصول مدیریت هویت (۳-۴-۱) جهت محدود کردن درخواست یا انتقال اطلاعات هویتی (۳-۲-۴) به شخص ثالث به حداقل اطلاعات اکیداً مورد نیاز برای یک هدف خاص.

یادآوری- اصول تناسب به حداقل افشاء مرتبط است تا آنجا که تلاش برای مداخله کنترل در ارتباط با این فعالیت معقول است.

۳-۶-۳

نام مستعار

شناسانه‌ای (۳-۱-۴) که حاوی حداقل اطلاعات هویتی (۳-۲-۴) کافی جهت امکان پذیر کردن برقراری آن برای درستی‌سنجی کننده (۳-۳-۶) به‌صورت یک پیوند به یک هویت (۳-۱-۲) شناخته شده است.

یادآوری۱- نام مستعار می‌تواند جهت کاهش خطرات حریم شخصی که به استفاده از شناسانه‌های دارای ارزش‌های ثابت یا شناخته شده مرتبط است، مورد استفاده قرار گیرد.

یادآوری۲- نام مستعار می‌تواند یک شناسانه با یک ارزش انتخابی توسط فرد باشد، یا به‌صورت تصادفی اختصاص یابد.

۳-۶-۴

ناشناختگی[1]

حالتی در **شناسایی (۳-۲-۱)** که طبق آن یک **هستار (۳-۱-۱)** می‌تواند، بدون **اطلاعات هویتی (۳-۲-۴)** کافی جهت برقراری یک پیوند به **هویت (۳-۱-۲)** شناخته شده به‌صورت مجزا شناسایی شود.

یادآوری- شناسایی بدون نام، نوعاً، شامل استفاده از اعتبارنامه‌های خاص می‌شود که می‌تواند به‌صورت رمزنگاشتی معتبر شود. پروتکل‌های رمزنگاشتی برای معتبرسازی یک اعتبارنامه بدون نام موجود است که می‌تواند جهت ارائهٔ اطلاعات هویتی مورد نیاز برای شناسانه پیکربندی شود. هویت به‌دست آمده به این روش ممکن است دارای چندین صفت باشد.

۴ نمادها و کوته‌نوشت‌ها

دامنهٔ (کاربردپذیری)	DA
فناوری اطلاعات و ارتباطات	ICT
مدیریت هویت	IDM
سامانه مدیریت هویت	IMS
فراهم‌کننده اطلاعات هویتی	IIP
مرجع اطلاعات هویتی	IIA
شناسانه مرجع	RI

1- anonymity

طرف مورد اطمینان	RP
تک ثبت نام	SSO
شناسانه منبع یکنواخت	URI
شناسانه منحصر به فرد جامع	UUID

۵ هویت

۵-۱ کلیات

یک هویت، عبارت است از اطلاعاتی که برای بازنمود هویت در یک سامانه ICT به کار می‌رود. هدف این سامانه ICT، تعیین می‌کند که کدام یک از صفت‌های توصیف‌کننده یک هستار برای یک هویت مورد استفاده قرار می‌گیرند. در یک سامانه ICT یک هویت باید مجموعه‌ای از آن صفت‌های مرتبط با یک هستار باشد که وابسته به دامنهٔ خاص برنامه کاربردی است که سامانه ICT به آن خدمات رسانی می‌کند. بسته به الزامات ویژه این دامنهٔ، این مجموعهٔ از صفت‌های مرتبط به هستار (هویت) می‌تواند، اما الزامی وجود ندارد، که به‌صورت منحصر به فرد از دیگر هویت‌ها در سامانه ICT قابل تمایز باشد.

این استاندارد هر مجموعه‌ای از صفت‌هایی که یک هستار خاص را به‌صورت هویت برای آن هستار تعریف می‌کند،در نظر می‌گیرد. در برخی از دامنهٔها، اطلاعات هویتی برای هستارهای مختلف ممکن است مشابه باشد. در دیگر استانداردها، برای مثال فناوری اطلاعات[13]U-T X1252، هدف روشن یک هویت، قابلیت اطلاعات هویتی جهت تشخیص هستار به‌صورت کافی از یکدیگر تا حدی مرتبط با برنامه‌های کاربردی در دامنهٔ (در زمینه) است.

یادآوری ۱- درصورتی که هدف مدیریت هویت در یک دامنهٔ خاص، مسئول قرار دادن هستارها یا ارائهٔ یک امتیاز ویژه به‌صورت انحصاری برای یک هستار خاص باشد، منحصر به فرد بودن هویت ضروری است. یک هستار ممکن است دارای چندین هویت باشد، که هر هویت مرتبط با حداقل یک دامنهٔ است. یک هستار می‌تواند دارای چندین هویت مرتبط با یک دامنهٔ مشابه باشد. برخی هویت‌های یک هستار ممکن است در هیچ دامنهٔای منحصر به فرد نباشد.

یادآوری ۲- اصطلاح هستار باید با مفهومی گسترده در نظر گرفته شود. این اصطلاح یک فرد حقیقی، یک فرد معنوی یا حقوقی (موسسه، شرکت)، یک شیءء (اطلاعات، یک سامانه،یک دستگاه) یا گروهی از این هستارهای منفرد باشد.

یادآوری ۳- انسان در این استاندارد یک هستار است و دارای یک وجود منفرد، کل است. این هستار می‌تواند با بسیاری از صفت‌های مختلف تعریف شود. مجموعهٔای مختلفی از این صفت‌ها هویت‌های مختلفی را برای یک هستار انسانی مشابه شکل می‌دهد.در صورتی که یک هستار در یک دامنهٔ خاص، منحصر به فرد نباشد، می‌تواند جهت تشخیص گروهی از هستارها در آن دامنهٔ که یک یا چند مشخصه را از دیگر هستارهایی که دارای چنین مشخصه‌ای نیستند، به اشتراک می‌گذارد، به‌کار رود. هویت یک هستار جهت ایجاد اطلاعات مرتبط شناخته شده هستار در تعامل آن با سرویس‌ها و دسترسی منابع ارائهٔ شده به وسیلهٔ دامنه به‌کار می‌رود. دامنهٔ نوع و حدود ارزش‌های مجاز صفت‌ها را جهت استفاده برای شناسایی یا دیگر اهداف معین می‌کند.

یادآوری ٤- دربرخی موارد، اصطلاح ‹هویت جزئی› می‌تواند برای اشاره به یک مجموعهٔ خاص از صفت‌های گرفته از مجموعهٔ بزرگتری از صفت‌ها مورد استفاده قرار گیرد، که درمقابل می‌تواند به‌صورت هویت کامل - تمام صفت‌های موجود- یک هستار در یک دامنهٔ بیان شود. اصطلاح ترجیح داده شده در این استاندارد هویت است.

یک دامنهٔ باید یک سامانه مدیریت هویت مطابق با ISO/IEC 24760 را جهت مدیریت اطلاعات هویتی هستارهایی که قصد شناسایی آنها را دارد گسترش دهد.

۵-۲ اطلاعات هویتی

اطلاعات وابسته به یک هستار خاص در یک دامنه، اطلاعات هویتی نامیده می‌شود.

درصورتی که اطلاعات هویتی معین یک هستار را از دیگر هستارها در زمینه حالت استفاده معین به طور مناسب تشخیص دهد، این اطلاعات هویتی یک *هویت قابل تشخیص* است.

اگر ترکیب ارزش‌های موجود در اطلاعات هویتی در دامنهٔ منحصر به فرد باشد، در این صورت این اطلاعات هویتی یک *شناسانه* هستار است.

زمانی که یک هویت جدید برای یک هستار در یک دامنهٔ ایجاد می‌شود، ارائهٔ دهنده اطلاعات هویتی برای دامنهٔ می‌تواند ارزش‌هایی را برای صفت‌های مورد نیاز هویت جدید ایجاد کند. صفت‌های جدید می‌تواند شامل موارد زیر باشد

- هر اطلاعات مورد نیاز جهت تسهیل تعامل میان دامنهٔ و هستار که هویت برای آن ایجاد شده است،
- هرنوع اطلاعات مورد نیاز برای شناسایی آینده هستار، شامل تعریف جنبه‌های حضور فیزیکی هستار،
- هرنوع اطلاعات مورد نیاز برای اصالت‌سنجی هویت هستار، یا
- یک یا چند شناسانه مرجع

اطلاعات جدید هویتی می‌تواند از اطلاعات هویتی برای هستار ایجاد شده در دامنهٔ جاری یا دامنهٔ دیگر استخراج شود. استخراج اطلاعات می‌تواند شامل نسخه‌برداری، تلفیق یا ایجاد یک نام مستعار باشد.

دامنهٔ باید ثابت کند که اطلاعات هویتی ایجاد شده بدرستی مربوط به هستار است.

اطلاعات هویتی می‌تواند با فراداده تعیین کننده، برای مثال منبع آن، حوزه استفاده و دوره اعتبار مرتبط باشد. فراداده اطلاعات هویتی خود می‌تواند اطلاعات هویتی باشد و هویتی که به آن مرتبط می‌شود می‌تواند شامل آن شود.

اطلاعات هویتی و فراداده مرتبط به آن می‌تواند تغییر کند. رویه‌ها و شرایط تغییر، به روزرسانی و ایجاد اطلاعات هویتی باید براساس خط مشیءهای مناسب معین شود. این خط مشیءها می‌تواند شامل نگهداری پرونده‌ها برای بازبینی باشد. این خط مشیءها ممکن است میان وظایف و فعالیت‌های مرتبط با چرخهٔ حیات هویت متمایز باشد (به ۷-۲ مراجعه شود)، که شامل موارد زیر می‌شود.

- درخواست و دریافت اطلاعات از منابع بیرونی
- درستی‌سنجی و اعتبارسنجی
- تعیین واجد شرایط بودن و رده‌بندی کردن
- پرونده سازی
- پیش‌بینی
- بایگانی، و
- حذف کردن.

۵-۳ شناسانه

صفت یا صفت‌های منحصر به فرد در هویتی که به‌عنوان شناسانه مورد استفاده قرار می‌گیرد می‌تواند:

- قابل استفاده برای هستار جهت استفادهٔ انحصاری در دامنهٔ منشاء، یا
- مناسب برای استفاده در این دامنه‌ها به استثنای دامنهٔ منشاء باشد.

یک شناسانه می‌تواند در دامنهٔ منشاء از خطا ساخته شود، می‌تواند نتیجه مشاهده باشد یا می‌تواند مبتنی بر شناسانه‌های ارائهٔ شده باشد.

یادآوری ۱- در برخی موارد، برای مثال تک ثبت نام، یک شناسانه می‌تواند با هدف به‌کارگیری خارج از دامنهٔ منشاء نیز ایجاد شود.

یک شناسانه می‌تواند در یک شیء فیزیکی ضبط شود. این شیء فیزیکی می‌تواند با صفت‌های امنیتی تجهیز شود تا

- یکپارچگی ارزش‌های صفت‌ها را در شناسانه درستی‌سنجی کند،
- به یک درستی‌سنج اجازه دستیابی به تضمین اینکه شناسانه به طور صحیح به یک هستار مرتبط است را بدهد،
- از قابلیت اطمینان ارزش‌های صفت حفاظت کند، یا
- درستی‌سنجی اطلاعات هویتی شامل شده را برای مثال، با فراهم کردن سازوکار اصالت‌سنجی داده رمزنگاشتی شده یا مشخصات امنیتی فیزیکی درنظر گرفته شده، تسهیل می‌کند.

یادآوری ۲- در برخی موارد، شناسانه به تنهایی برای تشخیص هستار از هستار دیگر در یک دامنهٔ متفاوت با دامنهٔ منشاء کافی نیست. در این موارد، دامنهٔ دیگر ممکن است بسته به استفاده از شناسانه، به اطلاعات هویتی بیشتری نیاز داشته باشد. مثالی در این مورد می‌تواند کارت عضویت کتابخانه باشد که حاوی شمارهٔ عضویت به‌عنوان شناسانه است که دستیابی عادی به موزه را نیز فراهم می‌آورد که اگر موزه دارای دستیابی نمایشی برای سن خاصی باشد، این اطلاعات افزوده مورد سوال قرار می‌گیرد.

یادآوری ۳-یک شیء فیزیکی می‌تواند نشانگر یک شناسانه باشد. شیء فیزیکی شکلی از یک اعتبارنامه است و خود می‌تواند یک هویت (همانطور که در این استاندارد مورد استفاده قرار گرفته است) یا صفت خود جهت تشخیص منحصر به فرد بودن آن نسبت به شیء دیگر شناسانه که از دامنهٔ مشابه به‌دست می‌آید. برای مثال، یک گذرنامه حاوی شناسانه یک فرد (هستار) به‌عنوان شهروند یک کشور (دامنهٔ) ممکن است هستاری که دارای هویتی مرکب از یک شمارهٔ گذرنامه منحصر به فرد است درنظر گرفته شود.

۶ صفت‌ها

۶-۱ کلیات

صفت یک هویت، وضعیت، ظاهر و دیگر کیفیت‌های یک هستار مرتبط در یک دامنهٔ را توصیف می‌کند. هر صفت دارای معانی خود جهت کنترل تفسیر ارزش‌هایی است که صفت می‌تواند بپذیرد. معانی یک صفت می‌تواند به طور روشن تعریف شود، برای مثال، با مرجع قرار دادن یک استاندارد بین‌المللی برای تجهیزات جهت برقراری ارزش آن.

یک صفت دارای نوع، ارزش و یک زمینه عملیاتی است. صفت می‌تواند دارای نامی باشد که می‌تواند برای مراجعه به آن صفت مورد استفاده قرار گیرد. بسته به استفاده از ارزش یک صفت، زمینهٔ عملیاتی دامنهٔ منشاء آن یا دامنهٔ کاربردپذیری آن است.

معانی و نحو به روشنی تعریف و مستند شده، باید برای صفت‌ها مشخص شوند.

یادآوری- برای یک سامانه فناوری اطلاعات که مدیریت هویت را به‌کار می‌گیرد، برای هر عنصر داده‌ای، که یک صفت، نمایش داخلی و خارجی (نحو) آن و روش‌هایی که می‌تواند پردازش شود(معانی) تعریف روشن در اسناد طراحی سامانه الزامی است.

۶-۲ انواع صفت

صفت‌ها می‌توانند به یک یا چند نوع رده‌بندی شود، که شامل موارد زیر می‌شود، اما به آنها محدودد نمی‌شود.

یادآوری - رده‌بندی صفت‌ها در اینجا به‌صورت مثال بیان شده اند. برخی از صفت‌ها می‌توانند به چند نوع رده‌بندی شوند.

- اطلاعات درمورد وجود فیزیکی، مانند
  - جزئیات بیوگرافی،
  - نشانی محل زندگی یا کار،
  - کارفرما،
  - تاریخچهٔ اشتغال،
  - محل دستگاه
- اطلاعات شرح دهندهٔ تکامل هستار طی زمان، مانند
  - مدرک تحصیلی،
  - مدارک صلاحیت،
  - پاداش‌ها،
  - برنامه‌های کاربردی نصب شده،
  - پیکربندی دستگاه؛
- اطلاعات اصلی درمورد وجود فیزیکی یک هستار، مانند
  - زیست‌سنجی؛
- اطلاعات اختصاص داده شده به هستار، مانند
  - عنوان،
  - نقش،
  - امضای دیجیتال،
  - شمارهٔ امنیت اجتماعی،
  - شمارهٔ شهروندی،
  - شمارهٔ گذرنامه،

- شمارهٔ سریال تولیدکننده،
- نشانی شبکه (MAC)
- کلید رمزنگاشتی؛
- ارجاع به شیء نشان دهندهٔ اطلاعات هویتی هستار باشد، مانند
- گذرنامه،
- دیپلم تحصیلی،
- کارت کسب و کار،
- اساسنامه‌ها،
- ثبت ابزار.

۶-۳ دامنهٔ منشاء

دامنهٔ منشاء یک صفت می‌تواند برای صفت فراداده ارائهٔ دهد که نشان دهندهٔ موارد زیر است:

- دامنهٔ ارزش‌های یک صفت،
- منحصر به فرد بودن ارزش‌های صفت،
- کدبندی مقدار صفت،
- زمان ایجاد یا درستی‌سنجی صفت‌ها یا هویت‌ها،
- زمان منقضی شدن صفت‌ها یا هویت‌ها،
- روش برقراری مقدار صفت‌ها یا هویت‌ها،
- روش درستی‌سنجی مقدار صفت‌ها،
- سازوکار دستیابی به نمایش قابل فهم یک ارزش صفت انسانی.

دامنهٔ منشاء یک صفت یا هر اطلاعات تعیین شده به وسیلهٔ دامنهٔ منشاء، می‌تواند به روشنی به‌عنوان قسمتیء از ارزش صفت تعیین شود، برای مثال با ارجاع به یک سند مشخصات سامانه یا استانداردهای قابل اجرا.

یادآوری ۱-یک دامنهٔ منشاء روشن می‌تواند به‌عنوان قسمتیء از ارزش صفت تعیین شود یا زمانی که مورد نیاز است اتخاذ شود، برای مثال در فرآیند کشف.

یادآوری ۲-مشخصات صفت نشان داده شده به وسیلهٔ دامنهٔ منشاء می‌تواند با یک مرجع منحصر به فرد نشان داده شود، برای مثال URI به سند صفت‌های سامانه که در تعریف نوع صفت وجود دارد.

یادآوری ۳-ارزش یک صفت که شامل فراداده می‌شود می‌تواند یک ارزش مرکب باشد.

۷ مدیریت کردن اطلاعات هویتی

۷-۱ کلیات

یک دامنهٔ می‌تواند از یک سامانه مدیریت هویت جهت پشتیبانی از تعامل آن با هستارها بهره ببرد، برای مثال، اصالت‌سنجی.

مدیریت هویت چرخهٔ حیات اطلاعات هویتی از ثبت ابتدایی جهت بایگانی یا حذف را تحت پوشش قرار می‌دهد.

مدیریت هویت شامل نظارت، خط مشی‌ءها، فرآیندها، داده‌ها، فناوری و استانداردها می‌شود که می‌تواند شامل موارد زیر باشد:

- برنامه‌های کاربردی اجرا کننده یک ثبت نام هویت؛
- اصالت‌سنجی هویت؛
- برقراری اصل اطلاعات هویتی؛
- برقراری پیوند میان اطلاعات هویتی و یک هستار؛
- حفظ اطلاعات هویتی؛
- تضمین یکپارچگی اطلاعات هویتی؛
- فراهم آوردن اعتبارنامه‌ها و سرویس‌ها جهت تسهیل اصالت‌سنجی هستاری که به‌عنوان هویت شناخته می‌شود؛
- کاهش خطر سرقت یا سوءاستفاده از اطلاعات هویتی.

۷-۲چرخهٔ حیات هویت

شکل ۱ چرخهٔ حیات یک هویت را در یک سامانه مدیریت هویت نشان می‌دهد. در ابتدا، هیچ اطلاعاتی ارائهٔ نشده است و هستار ناشناخته است. پس از حذف تمام اطلاعات هویتی برای هستار، همچنان ناشناخته است.

یادآوری- از نقطه نظر یک سامانه مدیریت هویت، یک هستار ناشناخته وجود ندارد.

مراحل پیش رو در چرخهٔ حیات هویت شناسایی شده است:

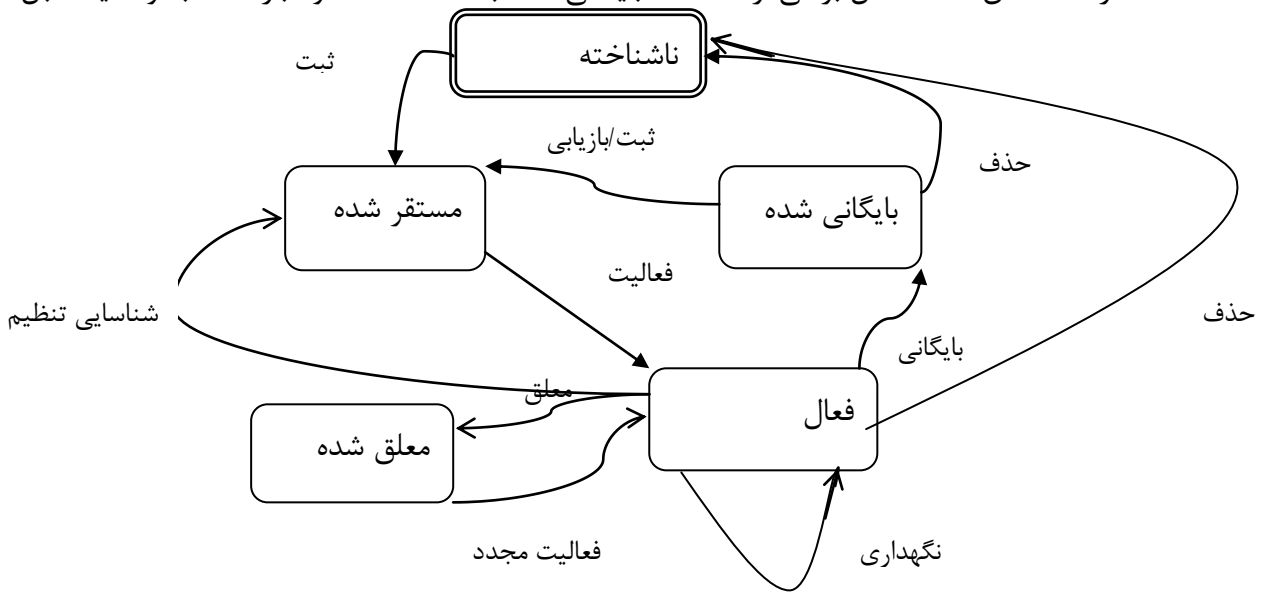
ناشناخته: هیچ اطلاعاتی در ثبت هویت که می‌تواند جهت شناسایی یک هستار مورد استفاده قرار گیرد ارائهٔ نشده که از این رو *ناشناخته* است.

برقرار: اطلاعات هویتی مورد نیاز طی فرآیند ثبت درستی‌سنجی شده است (به ۸-۳ مراجعه شود)، اطلاعات بیشتر، برای مثال شناسانه مرجع، تولید شده و اطلاعات ثبت نام شده است (به ۸-۴ مراجعه شود).

فعال: اطلاعات هویتی در سامانه مدیریت هویت که برای هستار امکان تعامل با سرویس‌ها و به‌کارگرفتن منابع قابل دسترس در دامنهٔ کاربردپذیری را ایجاد می‌کند، فراهم می‌شود، برای مثال به هستار این امکان داده می‌شود که یک دوره فعال را در یک سامانه فناوری اطلاعات آغاز کند.

معوق: اطلاعات هویتی در سامانه مدیریت هویت به طور خاص جهت نشان دادن اینکه هستار نمی‌تواند از منابع دامنهٔ بهره برداری کند ارائهٔ می‌شود.

بایگانی شده: اطلاعات هویتی برای یک هستار همچنان در ثبت هویتی باقی می‌ماند، حتی اگر هستار دیگر در دامنهٔ وجود نداشته باشد. اطلاعات بایگانی شده برای تشخیص هستار قابل دسترس نیست مگر طی ثبت مجدد احتمالی. زمانی که هستار مجددا ثبت شود، اطلاعات بایگانی شده می‌تواند جهت برقراری یک هویت جدید برای هستار که ممکن است شامل برخی از اطلاعات بایگانی شده باشد استفاده شود(بازگشت به وضعیت قبل).



شکل ۱- چرخهٔ حیات هویت

تراکنش‌های زیر می‌توانند در مدیریت کردن چرخهٔ حیات به‌کار گرفته شوند:

شامل اثبات و ثبت نام هویت با اطلاعات هویتی درستی‌سنجی و تولید شده می‌شود. به۸-۳ مراجعه شود.

فعال سازی افزوده شدن اطلاعات هویتی به اطلاعات ذخیره شده در ثبت نام هویت برای یک هستار است که به‌صورت خاص هستار را قادر می‌سازد تا به منابع دسترسی داشته باشد و با سرویس‌های ارائهٔ شده از سوی دامنهٔ تعامل داشته باشد.

نگهداری به روزرسانی اطلاعات هویتی ذخیره شده در ثبت نام هویت برای هستار است. به ۱۰ مراجعه شود.

تطبیق هویت به روزرسانی اطلاعات در ثبت نام هویت برای یک هستار است که اطلاعات جدید موجب اصلاح اطلاعات فعال سازی می‌شود.

تعلیق برخی از اطلاعات هویتی ذخیره شده در ثبت نام هویتی را برای یک هستار که موقتا امکان استفاده از آنها وجود ندارد نشانه گذاری می‌کند. تعلیق ممکن است با حذف حقوق دسترسی که در اطلاعات هویتی ذخیره شده بیان شده اند، به‌دست آید.

فعال سازی مجدد برعکس تعلیق است.

حذف از بین بردن کامل اطلاعات هویتی در یک هویت ثبت نام شده است.

بایگانی از بین بردن جزئی اطلاعات هویتی از ثبت نام هویت برای یک هستار است، به‌صورتی که اطلاعات تنها برای پردازش آماری قابل دسترسی است و تنها می‌تواند در نتیجه وابسته بودن به یک هستار با اطلاعات افزوده ارائهٔ شده به وسیلهٔ هستار در دسترس باشند.

ثبت/بازگشت به وضعیت قبل یک فرآیند ثبت است، که برخی از اطلاعات هویتی مورد استفاده به‌عنوان اثبات هویت از ثبت نام هویت به‌دست می‌آید.

۸ شناسایی

۸-۱ کلیات

شناسایی تعیین می‌کند که یک هویت ارائهٔ شده حاوی اطلاعات مورد نیاز جهت برقرار موارد زیر است

- هستار پیش از در دامنهٔ شناخته شده است، یا
- هستار برای شناخته شدن در دامنهٔ واجد شرایط است.

شناسایی می‌تواند از اطلاعات هویتی مرتبط با یک هستار خاص جهت تعیین اینکه آیا موارد زیر برقرار است استفاده کند

- هویت پیش از این برای هستار موجود است،
- هستار با اطلاعات هویتی شناخته شده یا ارائهٔ شده یا مشاهده شده مطابقت می‌کند،
- هستار به‌صورت منحصر به فرد با هویت مرتبط است.

پس از شناسایی، دامنهٔ می‌تواند فعالانه هستار و تعاملات هستار با دامنهٔ را از دیگر هستارهایی که شناسایی کرده است را نیز تشخیص دهد.

یادآوری ۱- این استاندارد شناسایی را از نقطه نظر یک دامنهٔ ارائهٔ می‌دهد. در شناسایی متقابل هر دو قسمت، هستار و دامنهٔ هستند.

شناسایی شامل پیوند مجموعه‌ای از صفت‌ها هم با یک هستار و هم با یک هویت می‌شود. ارزش این صفت‌ها می‌تواند

- از طریق مشاهده تعیین شود،
- از سوی هستار ارائهٔ شود،
- از ثبت نام هویت بازیابی شود،
- به وسیلهٔ منبع دیگر ارائهٔ شود، یا
- طی فرآیند اختصاص یابد.

شناسایی می‌تواند به وسیلهٔ اصالت‌سنجی در برقراری حقوق برای هستار جهت دسترسی منابع و تعامل با سرویس‌های ارائهٔ شده به وسیلهٔ دامنهٔ دنبال شود. به ۷-۲ :فعال سازی، مراجعه شود.

در سامانهی‌که دسترسی به منابع یا تعامل با سرویس‌ها شامل خطرات مرتبط با هویت می‌شود، سطح مورد نیاز تضمین در شناسایی باید مبتنی بر نوع و سطح خطر هویت برای منبع مشخص شود و نوع تعامل با سرویسی که حقوق می‌تواند برقرار شود. به ۹ مراجعه شود.

شناسایی می‌تواند برای یک هدف منفرد، مخصوص به دامنه یا برای چندین هدف مختلف باشد. شناسایی قسمتی از بسیاری از فرآیندهای مدیریت هویت است، برای مثال همانطور که در [11]ISO/IEC 29115 برای سامانه‌های فناوری اطلاعات تعریف شده است.

فرآیندی برای شناسایی باید با اصول زیر مشخص شود:

خطر خطرات مرتبط با استفاده از هویت هستارها باید با درجهٔ لازم برای آنها برای قابل قبول شدن ارزیابی و رفتار شود؛

یادآوری ۱- سطوح مختلف تضمین در شناسایی می‌تواند با سطوح مختلف خطر می‌تواند با دسترسی به منابع مختلف و تعامل با سرویس‌های مختلف مرتبط باشد.

کیفیت اطلاعات اطلاعات هویتی باید جهت فراهم کردن سطح کافی از تضمین صحت در جهت اهداف استفاده از آن درستی‌سنجی شود؛

کمینه سازی داده‌ها هنگام شناسایی افراد، اطلاعات اضافی نباید بیش از حد مورد نیاز جمع‌آوری شود.

یادآوری ۲- ارزیابی خطرات شامل ملاحظات کیفیت اطلاعات در دسترس و از این رو برقراری صحت آن می‌شود.

یادآوری ۳- انتخاب گزینه‌های مناسب کاهش خطر شامل تضمین اینکه هزینه متناسب با خطر است می‌باشد.

۸-۲ درستی‌سنجی

اطلاعات جدید هویتی باید درستی‌سنجی شود. درستی‌سنجی می‌تواند اطلاعات هویتی نیز اجرا شود که از ثبت نام هویت یا از یک ارائهٔ دهنده اطلاعات هویتی بازیابی شود.

درستی‌سنجی اطلاعات هویتی باید تضمین کند که

- در یک قالب تصویب شده ارائهٔ شود،
- حاوی ارزشیء باشد که مطابق معیارهای خاص برای دامنهٔ یا هدف شناسایی است،
- در یک دوره اعتبار مورد نیاز ایجاد شود، یا
- از یک منبع قابل اطمینان ایجاد شود.

یادآوری- درستی‌سنجی می‌تواند ورودی جهت شناسایی را نیز فراهم آورد و نتیجهٔ آن می‌تواند در شرایط خاص، برای مثال محل و زمان آن فرآیند ویژه باشد.

درستی‌سنجی می‌تواند اثبات کند که یک صفت به وجود فیزیکی یک هستار مربوط است، برای مثال مطابقت نمونه زیست سنجی از هستار با یک الگوی زیست سنجی در در هویت آن وجود دارد.

درستی‌سنجی می‌تواند اثبات کند که تمام صفت‌های ارائه شده به هستار مشابه مربوط است و با وجود فیزیکی آن سازگار است.

درستی‌سنجی می‌تواند شامل بررسی اعتبار صفت‌هایی باشد که برای فرآیند شناسایی مورد نیاز نیستند که ممکن است طی تعامل با سرویس‌ها مورد استفاده قرار گیرند و به منابع فراهم شده به وسیلهٔ دامنهٔ پس از شناسایی دسترسی داشته باشد، برای مثال اولویت زبانی، شمارهٔ حساب.

۸-۳ ثبت

ثبت می‌تواند نتیجهٔ ایجاد یک یا چند هویت برای هستار ثبت شده باشد. به طور خاص، شناسانه مرجع می‌تواند ایجاد شود. اطلاعات هویتی ایجاد شده به‌عنوان هویت هستار ثبت شده، در دامنهٔ ثبت نام می‌شود؛ اطلاعات هویتی انتخاب شده از گواه هویتی نیز می‌تواند در زمان ثبت با این هویت ثبت نام شود.

ارزش صفت‌های منحصر به فرد در یک هویت ایجاد شده می‌تواند به وسیلهٔ هستار انتخاب شود یا می‌تواند به وسیلهٔ سامانه مدیریت هویت اختصاص یابد، برای مثال مبتنی بر شناسانه مرجع ایجاد شده در ثبت نام هویت برای هستار ثبت شده.

ثبت می‌تواند شامل گرفتن اطلاعات زیست سنجی به‌عنوان اطلاعات هویتی برای هستار ثبت شده باشد.

یادآوری ۱- درصورتی که هستار ارزش یک شناسانه ایجاد شده را طی ثبت تعیین کند، IDMS باید منحصر به فرد بودن آن را تضمین کند.

یادآوری ۲- یک شیء فیزیکی، برای مثال، کارت عضویت، می‌تواند حاوی یک شناسانه باشد که طی ثبت ایجاد شده است.

۸-۴ ثبت نام

یک سامانه مدیریت هویت می‌تواند اطلاعات هویتی نهایی را که قصد دارد آنها را در یک ثبت نام هویتی شناسایی کند، وارد کند. ثبت شامل ثبت نام اولیهٔ اطلاعات هویتی می‌شود. ثبت نام متعاقب می‌تواند در موقعیت‌های دیگر رخ دهد.

یادآوری ۱- پس از ثبت نام، یک هستار در دامنهٔ شناخته می‌شود و چرخهٔ حیات هویت آن آغاز می‌شود.

ثبت نام می‌تواند برای یک دوره مشخص یا نامعین باشد. قانون ملی ممکن است محدودیت‌هایی را درمورد دوره واقعی ثبت نام نامحدود، شامل زمان و چگونگی اتمام ثبت نام نامحدود وضع کند.

ثبت نام نامحدود جز در مورد مواردی که براساس الزامات قانونی وضع می‌شود، باید به درخواست یا درخواست از جانب هستار برای از بین بردن به اتمام برسد. با حذف تمام اطلاعات هویتی برای هستار، هستار باید از ثبت نام هویتی از بین برود. اگرچه براساس تصمیم اتخاذ شده طبق یک خط مشیء مناسب، یک دامنهٔ می‌تواند برخی از اطلاعات هویتی را برای اهداف بایگانی و بازبینی حفظ کند و در این مورد، هویت در مرحله چرخهٔ حیات *بایگانی شده* خواهد بود (به ۷,۲ مراجعه شود). به طور خاص، یک شناسانه ممکن است جهت جلوگیری از استفاده مجدد از آن به‌عنوان مرجع برای هستار دیگر حفظ شود.

هویت ذخیره شده در ثبت نام یک هویت باید دارای یک شناسانه مرجع باشد که در میان تمام هویت‌های ذخیره شده منحصر به فرد است. یک شناسانه مرجع باید دارای ارزش‌های مشابهی برای دوره ثبت نام اطلاعات هویتی برای یک هویت خاص باشد.

یک شناسانه مرجع می‌تواند برای استفاده انحصاری در داخل دامنه‌ای که سامانه مدیریت هویت عمل می‌کند در نظر گرفته شود.

یادآوری ۲- یک شناسانه مرجع، درصورتی که به‌صورت انحصاری مورد استفاده قرار نگیرد، ممکن است برای استفاده به‌عنوان یک صفت در هویتی که یک هستار برای شناسایی در دامنهٔ دیگر ارائهٔ می‌دهد، قابل دسترسی باشد.

اطلاعات هویتی ذخیره شده در یک ثبت نام هویتی می‌تواند شامل چندین شناسانه مرجع باشد. شناسانه مرجع می‌تواند جهت نشان دادن یک هویت جزئی خاص برای هستار در یک دامنهٔ مورد استفاده قرار گیرد.

۹ اصالت‌سنجی

اصالت‌سنجی موفق یک هستار در یک دامنهٔ، در سطح مشخصی از تضمین به قسمت قابل اطمینان صحت و کاربرد پذیری نتیجه درستی‌سنجی را اطمینان می‌دهد. استاندارد بین‌المللی ISO/IEC 29115[11] سطوح تضمین را مشخص می‌کند.

یک سامانه مدیریت هویت مطابق با ISO/IEC 24760 باید برای هر یک از فرآیندهای اصالت‌سنجی خود تعیین شود:

- خط مشیءها برای درستی‌سنجی اطلاعات هویتی،
- سازوکارهای برقراری اعتبار و صحت یک هویت اصالت‌سنجی شده،
- دوره اعتبار یک هویت اصالت‌سنجی شده،
- سازوکارهای ضبط و بازبینی، مراحل پردازش و نتایج پردازش (متوسط).

یادآوری - اصالت‌سنجی به یک مدل امنیتی کنترل محیطی مرتبط می‌شود که درستی‌سنجی دقیق در زمان ورود، اجازه ورود به یک منطقه خاص فعالیتی را برای یک دوره زمانی خاص می‌دهد.

یک سامانه مدیریت هویت می‌تواند از اصالت‌سنجی یک هویت در چندین سطح تضمین مجزا پشتیبانی کند، برای مثال برای برآورده کردن اهداف طراحی یک سامانه خاص در کنترل دسترسی متعاقب.

۱۰ حفاظت

یک سامانه مدیریت هویت می‌تواند حفاظت را در مورد اطلاعات هویتی که به وسیلهٔ تغییر یک یا چند ارزش صفت را در یک هویت ثبت نام کرده است، اجرا کند.

یک سامانهٔ مدیریت هویت باید سازوکارها را برای حفاظت از یکپارچگی و دقت صفت‌هایی که ذخیره می‌کند مشخص می‌کند. این سامانه باید اطلاعات هویتی ذخیره شده در ثبت نام را به‌عنوان یک ارائهٔ دقیق از هویت حفاظت کند.

یک مرجع اطلاعات هویتی باید دقیق ترین داده در دسترس را برای یک هویت در فرآیندی که به حریم شخصی احترام می‌گذارد فراهم آورد.

۱۱ جنبه‌های کاربرد

یک سامانه مدیریت هویت می‌تواند به‌صورت‌های زیر باشد:

متمرکز- یک سامانه کاملا متمرکز دارای یک ثبت نام هویتی منفرد و یک نقطهٔ کنترل منفرد طی ثبت و دسترسی به اطلاعات هویتی ذخیره شده است.

توزیع شده- یک سامانه مدیریت هویت می‌تواند دارای چندین ثبت نام هویتی و چندین نقطه کنترل طی ثبت و دسترسی به اطلاعات هویتی ثبت نام شده باشد.

یادآوری ۱- متمرکزترین سامانه نوعاً کمترین پیچیدگی را به نمایش می‌گذارد اما دارای ساختار انعطاف ناپذیرتری است.

کاربر محور- یک سامانه مدیریت هویت زمانی که به هستارها اجازه می‌دهد تا یک نقش فعال را در مدیریت اطلاعات هویتی ذخیره شده در ثبت نام هویت (به ۸,۴ مراجعه شود) ایفا کند کاربر متمرکز است.
متحد- اتحاد به سامانه مدیریت هویت اجازه می‌دهد که حاوی اطلاعات هویتی مورد نیاز در ثبت نام خود جهت اطمینان به اطلاعات هویتی از سامانه مدیریت هویت دیگر، و اثبات هویت ایجاد شده به وسیلهٔ سامانه مدیریت هویت دیگر، نباشد. در این مورد سامانه مدیریت هویت به‌عنوان یک مرجع اطلاعات هویتی عمل می‌کند.
در موقعیت‌هایی که هستارها با چندین دامنهٔ تعامل دارند، اتحاد هویت جهت دستیابی به موارد زیر در نظر گرفته می‌شود

- تسهیل اثبات هویت،
- تسهیل اصالت‌سنجی،
- تسهیل ثبت،
- افزایش تجربهٔ کاربری.

یادآوری ۲- اتحاد هویت به طور خاص برای هستارها (و دامنه‌ها) که با دامنه‌ها در اینترنت تعامل دارد مناسب است.

۱۲ حریم شخصی

یک سامانه مدیریت هویت مطابق با ISO/IEC 24760 باید از تمام الزامات قانونی و تنظیمی‌جهت حفاظت از حریم شخصی هستارهای انسانی که با آنها تعامل دارد تبعیت کند. طراحی چنین سامانهی باید به طور کامل هر نوع اطلاعات حساسی را که پردازش می‌کند، مشخص کند.
یک سامانه مدیریت هویت مطابق با ISO/IEC 24760 باید قابلیت‌های مرتبط با حریم شخصی را فراهم کند تا:

- سازوکارها، شامل خط مشیءها، فرآیندها و فناوری برای حداقل افشاء را اجرا کند،
- هستارهایی را که از اطلاعات هویتی استفاده می‌کنند اصالت‌سنجی کند،
- توانایی پیوند هویت‌ها را به حداقل برساند،
- استفاده از اطلاعات هویتی را ضبط و بازبینی کند،
- در برابر خطرات به‌صورت سهوی ایجاد شده برای حریم شخصی، برای مثال خطراتی که به وسیلهٔ اطلاعات هویتی در گزارش‌ها و مسیرهای بازبینی به دلیل حفاظت ناکافی ایجاد شده اند محافظت کند،
- خط مشیءها برای افشاء گزینشیء را اجرا می‌کند،
- از استفاده از نام مستعار پشتیبانی می‌کند،
- خط مشیءها برای درگیر کردن یک هستار انسانی برای توافق یا دستورالعمل روشن، برای فعالیت‌های مرتبط با اطلاعات هویتی حساس آنها را اجرا کند.

الزامات برای به‌کارگیری اطلاعات هویتی حساس در استانداردهای زیر تعیین شده اند:

- ISO/IEC 29100[9] فناوری اطلاعات- فنون امنیتی- چهارچوب حریم شخصی
- ISO/IEC 29101[10] فناوری اطلاعات- فنون امنیتی- معماری مرجع حریم شخصی