INSO
17642-2
1st. Edition
2016

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

استاندارد ملی ایران
۱۷۶۴۲-۲
چاپ اول
۱۳۹۴

فناوری اطلاعات - فنون امنیتی - چارچوبی برای مدیریت هویت - قسمت ۲: الزامات و معماری مرجع

Information technology — Security techniques — A framework for identity management — Part 2:Reference architecture and requirements

ICS:35.040

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج ، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: http://www.isiri.org

Iranian National Standardization Organization (INSO)

No.1294 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: http://www.isiri.org

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفهٔ تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی 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 واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های 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.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1]، کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی 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 مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه 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، 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 for Legal Metrology (Organisation Internationale de Metrologie Legals)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات - فنون امنیتی - چارچوبی برای مدیریت هویت – قسمت ۲: الزامات و معماری مرجع»

رئیس:	**سمت و / یا نمایندگی**
ترابی، مهرنوش (فوق لیسانس فناوری اطلاعات– تجارت الکترونیک)	کارشناس تجزیه و تحلیل سیستم شرکت برق منطقه‌ای هرمزگان
دبیر:	
مشرف، بهنوش (فوق لیسانس فناوری اطلاعات– شبکه‌های کامپیوتری)	کارشناس پایگاه داده‌ها شرکت برق منطقه‌ای هرمزگان
اعضاء: (اسامی به ترتیب حروف الفبا)	
ابراهیم نژاد، پوریا (فوق لیسانس مهندسی برق- مخابرات)	کارشناس شبکه‌های بی سیم شرکت ایرانسل
آذرکار، سید علی (فوق لیسانس مهندسی کامپیوتر- نرم افزار)	عضو سازمان نظام صنفی رایانه
احمدی، محمد (فوق لیسانس مهندسی برق- مخابرات)	کارشناس فیبر نوری شرکت برق منطقه‌ای هرمزگان
اشرفی، رضا (فوق لیسانس مهندسی برق- ICT)	مدیر بخش توسعه شرکت تامین تله کام
ایزدپناه، سحرسادات (فوق لیسانس مهندسی فناوری اطلاعات)	رییس اداره استاندارد سازمان فناوری اطلاعات
عروجی، سید مهدی (فوق لیسانس فناوری اطلاعات)	مدیر گروه استاندارد سازمان تنظیم مقررات
قطب الدینیان - نیما (فوق لیسانس فناوری اطلاعات-مدیریت فناوری اطلاعات)	کارشناس دیتا شرکت مخابرات استان هرمزگان

فهرست مندرجات

پیش‌گفتار

استاندارد «فناوری اطلاعات - فنون امنیتی - چارچوبی برای مدیریت هویت - قسمت ۲: الزامات و معماری مرجع»، که پیش نویس آن درکمیسیون‌های مربوط توسط سازمان ملی استاندارد ایران تهیه و تدوین‌شده و در سیصد و نود و ششمین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۴/۱۲/۰۳ 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، به عنوان استاندارد ملی‌ایران منتشر می‌شود .

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علـوم و خـدمات، استانداردهای ملی‌ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیـل‌ایـن استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفـت. بنـابراین، 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 24760-2:2015: Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements.

فناوری اطلاعات - فنون امنیتی - چارچوبی برای مدیریت هویت - قسمت ۲: الزامات و معماری مرجع

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد تعیین:

- رهنمودهایی در جهت پیاده‌سازی سامانه‌هایی برای مدیریت اطلاعات هویت و
- الزاماتی برای پیاده‌سازی و بهره‌برداری از چارچوبی برای مدیریت هویت

می‌باشد.

این استاندارد برای مورد زیر کاربرد دارد:

هر سامانه اطلاعاتی که در ان اطلاعات مرتبط با هویت پردازش یا ذخیره می‌شود.

۲ مراجع الزامی

مدارک الزامی زیر شامل 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 صورتی‌که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن موردنظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

۲-۱- استاندارد ملی ایران شماره ۱-۱۷۶۴۲، فناوری اطلاعات - فنون امنیتی - چارچوبی برای مدیریت هویت - قسمت ۱: واژگان و مفاهیم

۲-۲- استاندارد ملی ایران شماره ۱۷۹۱۳، فناوری اطلاعات - فنون امنیتی - چارچوب تضمین اصالت‌سنجی هستار

۳ اصطلاحات وتعاریف

در این استاندارد علاوه بر اصطلاحات و تعاریف به کار برده شده در استاندارد ملی ایران شماره ۱-۱۷۶۴۲، اصطلاحات و تعاریف زیر نیز به کار می‌رود.

۳-۱

طرح مستندشده[1]

توصیف موثق از جنبه‌های ساختاری، کارکردی و سامانه عملیاتی می‌باشد.

1-Documented desighn

یاداوری۱- طراحی مستند سندی است که ایجاد شده تا به عنوان راهنمایی برای پیاده‌سازی یک سامانه فناوری اطلاعات و ارتباطات به کار رود.

یاداوری۲- طراحی مستند به طور معمول توصیفی از معماری یکپارچه یک سامانه فناوری اطلاعات و ارتباطات را شامل می‌شود.

۲-۳

نهاد مدیریت هویت[1]

هستاری که مسئول تنظیم و اجرای خط‌مشی‌های عملیاتی برای یک سامانه مدیریت هویت می‌باشد (به بند ۳-۳ مراجعه کنید).

یاداوری- یک نهاد مدیریت هویت، به طور معمول طراحی، پیاده‌سازی، و استقرار سامانه مدیریت هویت را بر عهده می‌گیرد.

مثال: مدیریت اجرایی شرکت، یک سامانه مدیریت هویت در حمایت از خدمات خود مستقر می‌کند.

۳-۳

سامانه مدیریت هویت[2]

سازوکار شامل خط‌مشی‌ها، رویه‌ها، فناوری، و دیگر منابع برای حفظ اطلاعات هویت از جمله فراداده است.

یاداوری- مدیریت هویت معمولا برای شناسایی یا اصالت‌سنجی هستارها استفاده می‌شود. می‌توان آن را برای پشتیبانی از دیگر تصمیم‌گیری‌های خودکار بر اساس اطلاعات هویتی برای یک هستار به کار برد. که در حوزه برنامه‌کارکردی سامانه مدیریت هویت به رسمیت شناخته شده است.

۴-۳

اصل[3]

موضوع

هستاری که اطلاعات هویت در یک سامانه مدیریت هویت به آن مربوط است (به بند ۳-۳ مراجعه کنید).

یاداوری- در زمینه الزامات مربوط به حفظ حریم خصوصی، یک اصل به شخص اشاره دارد.

۵-۳

صحه‌گذاری نشده[4]

فرایندی که در یک سامانه مدیریت هویت (به بند ۳-۳ مراجعه کنید) زمانی که یک مشخصه خاص، دیگر برای یک هستار خاص معتبر نیست، انجام می‌شود، تا این مشخصه خاص را برای استفاده در آینده نامعتبر اعلام کند.

یاداوری۱- صحه‌گذاری نشدن مشخصه‌ها ممکن است بخشی از به روز رسانی ارزش مشخصه باشد، مثلا با یک تغییر آدرس.

1-Identity management authority
2- Identity management system
3-Principal
4-Invalidation

یاداوری۲- صحه‌گذاری نشده، معمولا برای یک مشخصه است که قبل از پایان مدت اعتبارخود، نامعتبرشناخته شده است.

یاداوری۳- اصطلاح «لغو» معمولا برای صحه‌گذاری نشدن مشخصه‌هایی استفاده می‌شود که دارای اعتبار هستند.

یاداوری۴- صحه‌گذاری نشدن معمولا بلافاصله پس از تشخیص این موضوع اتفاق می‌افتد که یک مشخصه دیگر برای یک هستار خاص معتبرنیست.

۳-۶
ارگان مقررات گذار[1]

ارگانی که توسط قانون، مقررات و یا توافقنامه توانمند شده است تا بر عملکرد سامانه‌های مدیریت هویت نظارت کند.

۳-۷
ذی‌نفع[2]

فرد، تیم، سازمان و یا رده‌هایی که منافعی در یک سامانه دارند.

۴ نمادها و کوته نوشت ها

ICT Information Technology and Communication	فناوری اطلاعات و ارتباطات
IMS Identity Management System	سامانه مدیریت هویت
PII Personal Identifiable Information	اطلاعات شناسایی شخصی

۵ معماری منبع

۵-۱ کلیات

این بند عناصر معماری یک سامانه مدیریت هویت و روابط متقابل آن‌ها را توضیح می‌دهد.

طراحی مستندشده برای معماری یک سامانه مدیریت اطلاعات بهتر است بر اساس استاندارد ISO/IEC 42010 باشد.

یاداوری- معماری منبع و توصیف معماری توصیف شده در این استاندارد بر اساس استاندارد ISO/IEC 42010 است.

طراحی مستندشده برای معماری یک سامانه مدیریت هویت، بهتر است سامانه را در زمینه مورد استفاده آن بر اساس ذی‌نفعان وکنشگرها تعریف شده در این استاندارد مشخص کند.کنشگرهای سطح کسب و کار، ذی‌نفعان هستند. برخی از ذی‌نفعان با سامانه برهم کنش ندارند. طراحی مستندشده باید الزامات مربوط به ذی‌نفعان کنشگر و نیز غیر کنشگر را در نظر داشته باشد. طراحی مستندشده باید به طور جامع کنشگرها را توصیف کند.

1-Regulatory body
2-Stakeholder

یک طراحی مستندشده از یک سامانه مدیریت هویت مطابق با این استاندارد، باید از یک زبان توصیف معماری مناسب و مولفه‌های معماری مرجع و توابع آن‌ها توسط عبارات تعریف شده در این استاندارد بهره جوید.

۵-۲ عناصر معماری

۵-۲-۱ مرور کلی

عناصر تشکیل دهنده این معماری مرجع به قرار زیر است

- ذی‌نفعان (به بند ۵-۳-۱ مراجعه کنید)،
- کنشگرها (به بند ۵-۳-۲ مراجعه کنید)،
- دیدگاه‌ها (به بند ۵-۳ و بند ۵-۴ مراجعه کنید)،
- مدل‌ها (به بند ۵-۳-۳ و بند ۵-۳-۴ و ۵-۳-۵ و ۵-۴-۱ و ۵-۴-۳ مراجعه کنید)،
- مولفه‌ها (به بند ۵-۴-۱ مراجعه کنید)،
- فرایندها (به بند ۵-۴-۲ مراجعه کنید) و
- جریان‌های اطلاعات و اقدامات (به بند ۵-۴-۲ مراجعه کنید).

۵-۲-۲ نقطه نظرات

۵-۲-۲-۱ کلیات

طراحی مستند از یک سامانه مدیریت هویت باید یک دیدگاه زمینه‌ای ویک دیدگاه کارکردی را شامل شود. این امر ممکن است یک دیدگاه فیزیکی را شامل شود. طراحی مستند ممکن است حاوی دیدگاه‌های دیگر نیز باشد، به عنوان مثال دیدگاه اطلاعاتی.

یاداوری- مجموعه کمینه الزامات نقطه نظرات، برهم‌کنش‌های سامانه با محیط خود و مولفه‌های داخلی سامانه و برهم‌کنش‌های آن‌ها را توصیف می‌کند.

توصیف یک دیدگاه بهتر است متمرکز باشد. هرکدام از نمودارهای شرح دیدگاه‌ها بهتر است با متنی همراه باشد که عناصر نشان داده شده را تعریف کند.

یاداوری- توصیف نقطه نظرات در این بند بر اساس شماره ۲ مراجع الزامی است.

۵-۲-۲-۲ نقطه نظر زمینه‌ای

تعریف - در طراحی مستندشده، نقطه نظر زمینه‌ای به توصیف روابط، وابستگی‌ها و برهم‌کنش‌ها بین سامانه و محیط اطرافش (مردم، سامانه‌ها، و هستارهای بیرونی که با آن‌ها برهم‌کنش دارد) توصیف می‌کند.

نگرانی‌ها- حوزه سامانه و مسئولیت‌ها، هویت هستارها و خدمات و داده‌های استفاده شده بیرونی، ماهیت و مشخصه‌های هستارهای بیرونی، هویت و مسئولیت‌های واسطهای بیرونی، ماهیت و مشخصه‌های واسطهای بیرونی، دیگر وابستگی‌های متقابل بیرونی، تاثیر سامانه بر محیط خود و به طور کلی،کمال، سازگاری و همدوسی سامانه.

مدل‌ها - یک نقطه نظر زمینه‌ای ممکن است حاوی یک مدل زمینه‌ای، مورد کاربری و فرانامه‌های برهم‌کنش باشد. مدل زمینه‌ای یک نمودار جعبه و خطی[1] غیر رسمی است که سامانه مورد بحث را به عنوان یک جعبه سیاه با واسطها، برهم‌کنش‌ها در سطح بالا و وابستگی به هستارهای بیرونی نشان می‌دهد. به بند ۵-۳-۳ مراجعه کنید.

نکات مورد توجه - هستارهای بیرونی از دست رفته و یا نادرست، وابستگی‌های ضمنی از دست رفته، توصیف‌های نادرست و یا بی‌پایه واسطها، سطح نامناسب جزئیات، خزش دامنه، زمینه یا دامنه کاربرد فرضی یا ضمنی، برهم‌کنش‌های بیش از حد پیچیده، استفاده بیش از حد از اصطلاحات.

۵-۲-۲-۳ نقطه نظر کارکردی

تعریف – در طراحی مستندشده نقطه نظر کارکردی به توصیف عناصر کارکردی کلیدی با مسئولیت‌های عملیاتی، واسطها، و برهم‌کنش‌های اولیه می‌پردازد.

نگرانی‌ها– اشاره به قابلیت‌های کارکردی، واسطهای بیرونی، ساختار داخلی و فلسفه طراحی کارکردی دارد.

مدل‌ها - یک نقطه نظر کارکردی ممکن است حاوی یک مدل ترکیبی، مدل فیزیکی و یا یک مدل زیرساختی باشد.

در طراحی مستندشده نقطه نظر کارکردی باید استانداردها و ره‌نمون‌های قابل اجرای مربوط به هرکدام از کارکردهایی که توصیف می‌کند را مورد شناسایی قرار دهد.

برای راهنمایی در مورد مشخص کردن نقطه نظر کارکردی به بند ۵-۴ مراجعه کنید.

۵-۳ دیدگاه زمینه‌ای

۵-۳-۱ ذی‌نفعان

۵-۳-۱-۱ کلیات

این استاندارد ذی‌نفعان زیر را به طورمستقیم و غیرمستقیم با اولویت اهمیت به رسمیت می‌شناسد:

- اصل،
- نهاد مدیریت هویت،
- نهاد اطلاعات هویت،
- طرف مورد اعتماد،
- ارگان مقررات گذار،
- ممیز، و
- مصرف‌کننده / نماینده یا حمایت‌کنندگان شهروندی.

هرکدام از ذی‌نفعان یک کارکرد جداگانه در سامانه مدیریت هویت انجام می‌دهد. این کارکردها، مسئولیت‌ها و تعهدات خاصی را به طور ضمنی می‌رسانند. به غیر از ارگان‌های مقررات گذار و نمایندگان

1-Box-and-line diagram

مصرف‌کنندگان، ذی‌نفعان نیز با سامانه مدیریت هویت برهم‌کنش دارند، و در نتیجه به عنوان کنشگر در معماری مرجع حاضر هستند. (به بند ۵-۳-۲ مراجعه کنید).

نگرانی‌های ذی‌نفعان در یک سامانه مدیریت هویت در زیربندهای زیر توصیف شده و بهتر است در طراحی، پیاده‌سازی و بهره‌برداری از سامانه مورد توجه قرار گیرد.

۵-۳-۱-۲ اصل

نگرانی‌های مدیر در سامانه مدیریت هویت عبارتند از:

- صحت اطلاعات هویت که جمع آوری شده، پردازش شده و ذخیره شده است،
- حفاظت از حریم خصوصی،
- به کمینه رساندن اطلاعات هویت که توسط سامانه مدیریت هویت، جمع آوری، پردازش و ذخیره شده است،
- به کمینه رساندن استفاده از اطلاعات هویت توسط سامانه مدیریت هویت در حوزه کارکردی خود،
- خطاها در شناسایی از جمله شناسایی مثبت نادرست و منفی نادرست و تشخیص و رسیدگی به اشتباهات،
- دانش و توافقبه، اشتراک گذاری اطلاعات هویت با طرف سوم،
- ارائه صحیح توسط اطلاعات هویت که گرفته شده، پردازش یا ذخیره شده است،
- صحت عملکرد در تحویل خدمات و فراهم ساختن دسترسی به منابع موجود بر اساس مشخصه‌های ارائه شده در یک موقعیت خاص،
- جمع آوری، پردازش و ذخیره‌سازی اطلاعات هویت تنها با توافقآگاهانه آن رخ می‌دهد،
- رفتار عادلانه در برهم‌کنش با سامانه، و
- یک واسط کاربر موثر، قابل فهم، مناسب.

یاداوری- دغدغه یک مدیر که به خدمات‌دهی طرف سوم با استفاده از اطلاعات هویت به دست آمده از سامانه مدیریت هویت، مربوط است، دغدغه سامانه مدیریت هویت نیست و بنابراین در دامنه کاربرد این استاندارد جای نمی‌گیرد.

۵-۳-۱-۳ نهاد مدیریت هویت

نگرانی‌های نهاد مدیریت هویت در سامانه مدیریت هویت عبارتند از:

- تعریف اهداف مدیریت هویت در حوزه‌هایی که توسط سامانه مدیریت هویت، خدمت رسانی می‌شود،
- مشخص کردن خط‌مشی‌هایی برای حفظ اهداف مدیریت هویت درحوزه‌هایی که سامانه مدیریت هویت خدمت رسانی می‌کند،
- تحقق اهداف کسب و کار سامانه مدیریت هویت با توجه به مدیران و کاربران اطلاعات هویت،
- این که اطلاعات هویت ارائه شده توسط هر مدیر دقیق است و مربوط به آن مدیر و سطح خاصی از اطمینان است، و
- انطباق با مقررات.

۵-۳-۱-۴ نهاد اطلاعات هویت

نگرانی‌های یک نهاد اطلاعات هویت در یک سامانه مدیریت هویت عبارتند از:

- صحت اطلاعات هویت،
- برآورده ساختن الزامات طرف‌های مورد اعتماد،
- انطباق با مقررات، و
- برآورده ساختن تعهدات کسب و کار با اصول.

۵-۳-۱-۵ طرف مورد اعتماد

نگرانی‌های یک طرف مورد اعتماد در سامانه مدیریت هویت عبارتند از:
- محرمانه بودن، دسترس‌پذیری و یکپارچگی و کارکردی بودن آن نسبت به اصل اطلاعات هویت،
- تأمین اطلاعات هویت دقیق مربوط به اصول مربوطه در سطح اطمینان مورد نیاز،
- واسط‌های موثر، مستند و امن،
- انطباق با مقررات مربوطه و قابل اجرا در عملکرد، و
- سازوکار و فرایندهای موثر برای ممیزی.

۵-۳-۱-۶ ارگان مقررات گذار

به عنوان یک سازمان مستقل بیرونی، نگرانی‌های یک ارگان مقررات گذار در سامانه مدیریت هویت عبارتند از:
- مستند سازی مناسب از خط‌مشی‌های عامل،
- صحت کارکرد، به ویژه، در استفاده از خط‌مشی‌های عملکردی،
- پاسخگویی و ممیزی مناسب از عملیات سامانه،
- انطباق خط‌مشی عملکردی و روش عملکردی با الزامات مقررات گذاری و قانونی،
- گزارش‌دهی موثر بر کارکردهای سامانه، از جمله اثربخشی واپایش، حوادث، و اقدامات صورت گرفته شده در غلبه بر حوادث و
- پاسخ موثر به حوادثی که حفاظت از حریم خصوصی را نقض می‌کنند، و یا پتانسیل نقض آن را دارند.

یاداوری- به طور موثر، ممیزها، به عنوان کنشگرها یک سامانه مدیریت هویت (به بند ۵-۳-۲-۹ مراجعه کنید)، در بازرسی کارکرد یک سامانه مدیریت هویت (به بند ۵-۴ مراجعه کنید) ممکن است منافع ارگان‌های مقررات گذار را نمایندگی کنند.

۵-۳-۱-۷ نماینده یا وکیل مصرف‌کننده / شهروند

وکیلان مصرف‌کننده / شهروند افراد یا گروه‌هایی هستند که از جامعه مدنی ظهور کرده و سعی دارند مصرف‌کنندگان و شهروندان را از نظارت محافظت کرده و برای بهبود مقررات حفظ حریم خصوصی اقدام کنند.

مصرف‌کننده / شهروند افراد تعیین شده توسط مدیر یا انتخاب شده توسط سازمان‌های مصرف‌کننده می‌باشند تا حقوق مصرف‌کننده و یا شهروند را با توجه به حریم خصوصی نمایندگی کند.

مهم‌ترین نگرانی‌های وکیلان و نماینده مصرف‌کننده / شهروندان موارد زیر هستند:
- شفافیت، اطلاع‌رسانی، انطباق و محافظت در برابر زبان پیچیده حقوقی، و
- در دسترس کردن خدمات به جمعیت‌های محروم

یاداوری۱- نمایندگان مصرف‌کنندگان و شهروندان در فرایندهای اجتماعی به رسمیت شناخته شده ذی‌نفعان چند جانبه مانند حکومت شرکت می‌کنند و شیوه‌ها و الزامات مناسبی جهت برآورده کردن توسط کسانی که محصولات و خدمات به مصرف‌کنندگان و شهروندان ارائه می‌کنند، ایجاد می‌کنند.

یاداوری۲- نمایندگان مصرف‌کنندگان و شهروندان انتخاب می‌شوند، درجریان قرار داده می‌شوند و در صورت لزوم آموزش می‌بینند تا اطمینان حاصل شود، تا آنجا که ممکن است، بر اساس مدارک با کیفیت خوب از طریق بحث منطقی و مستدل، مشارکت می‌کنند.

۵-۳-۲ کنشگرها

۵-۳-۲-۱ کلیات

یک کنشگر با یک سامانه مدیریت هویت برای مشارکت در عملیات مدیریت هویت، برهم‌کنش دارد. یک هستار ممکن است به عنوان چندین کنشگر متفاوت با یک سامانه مدیریت هویت، برهم‌کنش داشته باشد. طراحی مستند باید همه برهم‌کنش‌هایی را تعریف کند که توسط هر کنشگر پشتیبانی شده توسط سامانه، انجام می‌شود.

طراحی مستند بهتر است برهم‌کنش‌های کنشگر از نظر برهم‌کنش‌های مربوط به آن را توصیف کند. جایی که در آن کنشگری که با سامانه مدیریت هویت برهم‌کنش دارد قبل از اینکه مجاز به ادامه برهم‌کنش‌ها باشد، نیاز به اصالت‌سنجی داشته باشد، طراحی مستند باید اساس این نیاز به اصالت‌سنجی (به عنوان مثال اصالت‌سنجی بر اساس هستار؛ بر اساس نقش و غیره)، روش اصالت‌سنجی و سطح اطمینان مورد نیاز برای هر برهم‌کنش را مشخص کند همان‌گونه که در استاندارد ملی ایران شماره ۱۷۹۱۳ تعریف شده است.

یاداوری- یکی از اهداف مشخص کردن کنشگرها در طراحی یک سامانه مدیریت هویت، این است که آنان را قادر سازد، همه برهم‌کنش‌ها در نظر گرفته شده با سامانه را توصیف کنند.

یک طراحی مستند، کنشگرهای زیر را به رسمیت می‌شناسد:

- مدیر؛
- نهاد مدیریت هویت؛
- نهاد ثبت هویت؛
- طرف مورد اعتماد؛
- ارائه دهنده اطلاعات هویت؛
- نهاد اطلاعات هویت؛
- تصدیق کننده؛
- ممیز.

طراحی مستند باید سطح اطمینان مورد نیاز برای شناسایی و اصالت‌سنجی هستارهایی را تعیین کند که درخواست دسترسی به اطلاعات هویت موجود در سامانه مدیریت هویت خود را دارند، همان گونه که در استاندارد ملی ایران شماره ۱۷۹۱۳، مشخص شده است. سطح اطمینان ممکن است برای انواع مختلف

اطلاعات و انواع دسترسی‌های داده شده به عنوان مثال، خواندنی، نوشتنی و غیره، متفاوت باشد. مجوز ممکن است همان گونه که در استاندارد ISO / IEC 29146 مشخص شده است، اجرا شود.

۵-۳-۲-۲ مدیر

یک مدیر کنشگری است که اطلاعات هویت را برای ایجاد و اعتباربخشی به هویتش، در فرایندهای مدیریت هویت، فراهم می‌کند. مدیر، وظایف و مسئولیت‌های زیر را داراست:

- به عنوان یک هستار در هنگام درخواست ثبت نام در یک حوزه کارکردی، به ارائه دقیق اطلاعات هویت برای ثبت نام به عنوان یک مدیر جدید، اقدام کند،
- پس از ثبت نام به عنوان کاربر سامانه، درخواست کند که توسط سامانه مدیریت هویت به رسمیت شناخته شود و تصویب شود که به خدمات و منابع موجود در حوزه کارکردی مرتبط با سامانه مدیریت هویت، دسترسی داشته باشد، و
- به عنوان موضوع مشاهده، به منظور تسهیل مشاهدات برای به دست آوردن اطلاعات هویت اقدام کند.

یاداوری- به عنوان موضوع مشاهده اطلاعات هویت به دست آمده ناشناس است، تا زمانی که ارتباط آن با مدیر ایجاد شود.

یک مدیر می‌تواند از یک سامانه مدیریت هویت استفاده کند تا:

- درخواست دهد توسط اطلاعات موجود در سامانه مدیریت هویت به رسمیت شناخته شود و برای دسترسی به خدمات و یا استفاده از منابع موجود در حوزه کارکردی مرتبط با سامانه مدیریت هویت، پذیرفته شود، و
- به عنوان انسان، از اطلاعات هویتی مربوط به خود که در سامانه مدیریت هویت نگه‌داری می‌شود مطلع باشد و درخواست اصلاح هر گونه خطا در اطلاعات هویت را بدهد.

یاداوری- در شرایط مناسب، یک نماینده که از نظر قانونی مجاز شناخته می‌شود ممکن است به نمایندگی از مدیر اقدام کند.

۵-۳-۲-۳ نهاد مدیریت هویت

یک نهاد مدیریت هویت با حوزه کارکردی وظایف و قابلیت‌ها در ارتباط است تا اهداف کسب و کار را برای مدیریت هویت در آن حوزه تعریف و تنظیم کند و خط‌مشی‌های مدیریتی برای برآوردن این اهداف را تنظیم کند.

یک نهاد مدیریت هویت از این خط‌مشی‌ها برای قانونمند کردن استفاده از اطلاعات هویت ثبت‌شده استفاده می‌کند. خط‌مشی‌ها ممکن است سطوح خدمات ارائه شده از جمله سطح اطمینان از اطلاعات هویت که ممکن است توسط سامانه مدیریت هویت ارائه شود را مشخص کنند. خط‌مشی‌ها ممکن است چگونگی به دست آوردن مجوز برای دسترسی و اصلاح اطلاعات هویت در شرایط پیش بینی نشده را مشخص کنند.

نهاد مدیریت هویت باید اهداف مدیریت هویت برای حوزه کارکردی را تعریف کند که تحت نهاد آن سامانه مدیریت هویت، خدمات ارائه می‌کنند. نهاد مدیریت هویت باید خط مشی‌ها برای رسیدن به اهداف مدیریت هویت حوزه مربوطه را مشخص کند.

مسئولیت‌های یک نهاد مدیریت هویت عبارتند از:

- ایجاد، تغییر و یا لغو خط‌مشی‌های عملیاتی،

- اطمینان از انطباق مقررات گذاری و قانونی خط‌مشی‌ها با عملکرد سامانه مدیریت هویت،
- نیاز و تصویب اصلاحات سازوکارها برای ایجاد یک سطح اطمینان مورد نیاز در اصالت‌سنجی هستار برای دسترسی به اطلاعات هویت و کارکردهای واپایش سامانه،
- پاسخگویی به حوادث،
- تصویب تغییرات در نوع اطلاعات مستندشده در ثبت هویت،
- شروع ممیزی به طور منظم، و
- بازبینی گزارش‌های ممیزی، به ویژه در اثربخشی خط‌مشی‌ها،

یک نهاد مدیریت هویت ممکن است با یک یا چند تن از نهادهای مدیریت هویت دیگر به یک انجمن رسمی وارد و یک «اتحادیه» تشکیل دهند.

یاداوری- هدف این است که دامنه کارکردی مدیران با دامنه‌های کارکردی دیگر در یک اتحادیه گسترش یابد. این گسترش با به اشتراک گذاری به شدت واپایش شده اطلاعات هویت به دست می‌آید.

در یک اتحادیه، مسئولیت هر یک نهادهای مدیریت هویت عبارتند از:
- ارائه سطحی از اطمینان از اطلاعات هویت که مطابق با الزامات مشخص هرکدام از دیگر اعضای این اتحادیه باشد،
- حفظ واپایش بر دسترسی به اطلاعات هویت موجود در سامانه مدیریت هویت،
- مشخص کردن این نکته که سطح اطمینان شناخته شده توسط هر عضو دیگری از اتحادیه در اجازه دسترسی به اطلاعات هویت در سامانه‌های مدیریت هویت متحد مطابق باالزامات دسترسی به اطلاعات هویت خودشان باشد،
- عمل کردن با خط‌مشی‌های مشترک برای به اشتراک گذاری اطلاعات، و
- مشخص کردن خط‌مشی‌هایی برای حفظ اعتماد خودشان، در سطح اطمینان اصالت‌سنجی هویت.

یاداوری ۱- به طور معمول، در یک اتحادیه، برخی از خط‌مشی‌های مدیریت هویت، به ویژه در مجوز برای دسترسی، بخشی از یک توافق بین نهادهای مدیریت هویت درگیر دراین حوزه، خواهد بود.

یاداوری ۲ - خط‌مشی‌های مدیریت هویت برای استفاده در حوزه‌های مختلف کارکردی ممکن است توسط استانداردهای بین المللی ایجاد شود.

یاداوری ۳- تغییرات ساختاری، سازمانی و میزانی اتحادیه داده‌ها ممکن است در معرض محدودیت‌های بیرونی از جمله الزامات قانونی و یا مقررات گذار و یا صدور اجازه از ارگان های مقررات گذار قرار بگیرد.

یاداوری ۴- اعضای یک اتحادیه ممکن است موافق واگذاری مسئولیت‌های عملیاتی نهاد مدیریت هویت به یک متصدی مشترک، باشند، که به عنوان «نهاد اتحادیه» تعیین شده باشد.

۵-۳-۲-۴ نهاد ثبت هویت

یک نهاد ثبت هویت کنشگری است در یک سامانه برای مدیریت هویت با وظیفه و قابلیت‌هایی برای تنظیم و اجرای خط‌مشی‌های کارکردی برای جمع آوری، ضبط و به‌روزرسانی اطلاعات هویت در ثبت هویت.

خط‌مشی‌های ثبت هویت باید انواع مختلف اصلاحات اعمال شده دراطلاعات هویت و شرایط کارکردی و امنیتی را شناسایی کند که تحت آن این تغییرات مجاز است. این خط‌مشی‌ها باید رویه‌هایی برای دستیابی به سطح اطمینان در اطلاعات هویت جمع آوری شده را مشخص کنند.

مسئولیت‌های یک نهاد ثبت هویت عبارتند از:

- تغییر، ایجاد و یا لغو خط‌مشی‌های عملیاتی،
- تصویب تغییرات در نوع اطلاعات ثبت‌شده در مخزن اطلاعات، و
- تصویب اصلاح اطلاعات هویتی ثبت‌شده در مخزن اطلاعات.

۵-۳-۲-۵ طرف مورد اعتماد

یک طرف مورد اعتماد کنشگری است که مورد اعتماد اطلاعات هویت یک مدیر خاص توسط سامانه مدیریت هویت می‌باشد. طرف مورد اعتماد از اطلاعات صحت سنجی شده برای دسترسی به خدمات و منابع تحت واپایش استفاده می‌کند.

مسئولیت‌های طرف مورد اعتمادعبارتند از:

- پردازش و ذخیره اطلاعات هویت مطابق با خط‌مشی‌های تعیین شده توسط نهاد مدیریت هویت، به ویژه برای حفاظت از حریم خصوصی،
- تعیین سطح اطمینان مورد نیاز که برای واپایش دسترسی به اطلاعات هویت استفاده می‌شود متناسب با ارزش خدمات و منابع خاص، و
- ارائه اطلاعات مربوط به برهم‌کنش‌ها با سامانه مدیریت هویت برای ممیزی.

۵-۳-۲-۶ نهاد اطلاعات هویت

یک نهاد اطلاعات هویت در یک سامانه مدیریت هویت کنشگری است که اقدام به ارائه وضعیت معتبر برای اطلاعات هویت ارائه شده به طرف‌های مورد اعتماد می‌کند. یک نهاد اطلاعات هویت، اطلاعات هویت هستارهای شناخته شده در حوزه را فراهم می‌کند. از نظر عملکرد، نهاد اطلاعات هویت ممکن است یک ارائه دهنده خدمات باشد که مجهز به عرضه فراداده معتبر مرتبط با اطلاعات هویت است. فراداده ممکن است با اطلاعاتی تکمیل شود تا اعتمادسازی کند، به عنوان مثال اصالت‌سنجی داده‌های استحکام رمز نگاشتی.

در یک حوزه ممکن است یک یا چند نهاد اطلاعات هویت حمایت شوند. یک نهاد اطلاعات هویت ممکن است از نهاد مدیریت هویت متمایز باشد. یک ارائه دهنده خدمات مستقل ممکن است به عنوان یک نهاد اطلاعات هویت عمل کند.

یادآوری- واگذاری اطلاعات هویت به ارائه دهنده خدمات مستقل معمولا شامل یک توافقنامه سطح خدمات می‌باشد.

رویه‌های ایجاد یک هستار به عنوان نهاد اطلاعات هویت فراتر از محدوده این استاندارد هستند.

طراحی مستند یک سامانه مدیریت هویت باید خط‌مشی‌ها را با فرایندها و معیارها مشخص کند تا سطح اطمینان از اطلاعاتی که ممکن است از یک نهاد اطلاعات هویت خاص به دست آمده تعیین شود. معیارهای زیر بهتر است در این خط‌مشی‌ها در نظر گرفته شود:

- کیفیت قطعی بودن هویت؛

- سطح اطمینان از اطلاعات ثبت‌شده در ثبت نام؛
- کیفیت مولد شناسامه مرجع (به بند ۵-۴-۲-۳-۳ مراجعه کنید)؛
- کیفیت نگهداری اطلاعات هویت؛
- ماهیت رویه‌های مورد استفاده برای به دست آوردن ارزش‌های خصیصه‌ها؛
- قواعد نحوی و معنایی خصیصه‌ها؛
- امنیت سامانه مدیریت هویت؛
- کیفیت پروتکل‌های ارتباطی امن استفاده شده برای تأمین اطلاعات.

طراحی مستند یک سامانه مدیریت هویت ممکن است خط‌مشی‌هایی برای اضافه کردن، حذف کردن و واجد شرایط کردن یک نهاد اطلاعات هویت به عنوان نهاد مناسب در حمایت از عملکرد سامانه مدیریت هویت تعیین کند. این خط‌مشی‌ها باید به حفظ سطح اطمینان مورد نیاز در زمانی رسیدگی کند که نهاد یک اطلاعات هویت خاص با دیگری جایگزین می‌شود.

اگر سامانه مدیریت هویت از چنین کارکردی حمایت کند، طراحی مستند یک سامانه مدیریت هویت باید فرایندهایی برای حل تفاوت در اطلاعات هویت برای یک هستار مشخص که به طور همزمان از دو نهاد اطلاعات هویت مختلف به دست آمده تعیین کند.

۵-۳-۲-۷ ارائه دهنده اطلاعات هویت

ارائه دهنده اطلاعات هویت در یک سامانه مدیریت هویت کنشگری است که اطلاعات هویت برای یک هستار خاص فراهم می‌کند.

مسئولیت‌های اصلی ارائه دهنده اطلاعات هویت به این قرار است:

- جمع آوری مشخصه‌های هویت از مدیران،
- اطمینان حاصل کردن از این که مجموعه‌ای PII مطابق با قوانین و خط‌مشی‌های سامانه مربوطه است،
- اطلاع رسانی به مدیر در مورد جمع آوری PII ، مورد استفاده‌ای که برای PII مقرر شده است و هرکدام از طرف‌های سومی که PII به آن تحویل داده خواهد شد،
- به دست آوردن توافقمدیر برای جمع‌آوری PII،
- جمع کردن مشخصه‌های لازم هویتی به صورت اطلاعات هویت که توسط سامانه مدیریت هویت برای شناسایی مدیران استفاده می‌شود،
- قالب‌بندی کردن اطلاعات هویت داخل یک رکورد هویت و ذخیره رکورد برای ثبت در سامانه مدیریت هویت،
- حفظ اطلاعات هویت در ثبات هویت برای انعکاس تغییراتی که ممکن است در مشخصه‌های هویت مدیران رخ دهد،
- استخراج اطلاعات هویت از ثبات هویت و ارائه آن به طرف‌های مورد اعتماد، و
- اطمینان حاصل کردن از این نکته که اطلاعات هویت که به دیگران منتقل می‌شود با از بین بردن داده حساس شخصی به کمینه برسد مگر اینکه به طور خاص به منظور پردازش اطلاعات توسط طرفی که به آن‌ها اطلاعات هویت داده می‌شود مورد نیاز و مجاز باشد.

یاداوری- اگر چه نهاد مدیریت هویت مسئول ایجاد و تصویب خط‌مشی‌های مربوط به نگرانی‌های ذکر شده است، ارائه‌دهنده اطلاعات هویت به عنوان مسئول پیاده‌سازی وانجام این خط‌مشی‌ها، شناخته می‌شود.

طراحی مستندشده از یک سامانه مدیریت هویت باید خط‌مشی‌هایی برای نظارت، محاسبه، تولید و تأمین اطلاعات هویت مشخص کند، تا سطح اطمینان دراین رویه متناسب با سطح اطمینان از اطلاعات هویت حاصل شده باشد. استاندارد ISO / IEC 29003 راهنمایی‌هایی در فرایندها برای به دست آوردن اطلاعات هویت ارائه می‌کند.

ارائه دهنده اطلاعات هویت نیز ممکن است برای توصیف اطلاعات هویت، فراداده ایجاد کند که می‌تواند شامل موارد زیر باشد:

- توصیف انواع مشخصه هویتی که اطلاعات هویت را شامل می‌شود،
- قالب‌های مناسب برای نام‌ها، مشخصه‌ها و ارزش‌های مشخصه به منظور نمایش به بازدیدکنندگان انسانی،
- جزئیات ساختاری و قالب اطلاعات هویت مورد استفاده توسط سامانه مدیریت هویت برای ذخیره‌سازی و ارتباطات،
- تاریخ و زمان ایجاد اطلاعات هویت،
- تاریخ و زمان انقضای اعتبار اطلاعات هویت،
- اشاره به منبع اطلاعات هویت، و
- داده‌های استحکام رمزنگاشتی برای محافظت از محرمانه بودن و یکپارچگی اطلاعات هویت ذخیره شده و ابلاغ شده، و هر فراداده مرتبط، استفاده می‌شود.

ارائه دهنده اطلاعات هویت ممکن است یک اعتبارنامه ایجاد کند که در اصالت‌سنجی مدیرانی که این اعتبارنامه را منعقد می‌کنند مورد استفاده قرار گیرد. اعتبارنامه ممکن است حاوی داده‌های رمز نگاری ایجاد شده توسط یک نهاد اطلاعات هویت باشد. یک اعتبار نامه ممکن است به شکل یک نمودافزار[1] فیزیکی حاوی اطلاعات هویت باشد که توسط انسان و یا ماشین قابل خواندن است.

صدور اعتبارنامه‌های فیزیکی فراتر از محدوده این استاندارد است.

۵-۳-۲-۸ بازبین

بازبین در یک سامانه مدیریت هویت کنشگری است که اعتبار، صحت و دقت اطلاعات هویت که مربوط به یک هستار خاص است، را تعیین می‌کند.

فعالیت‌های یک بازبین ممکن است شامل بررسی‌های پس زمینه با استفاده از شواهد هویت ارائه شده توسط یک هستار باشد. اگر شواهد هویت با یک اعتبارنامه، پشتیبانی شود، بازبین بهتر است اعتبار زمانی اطلاعات هویت که اعتبار نامه حاوی آن است را ایجادکند.

یک سامانه مدیریت هویت ممکن است بازبینان مکمل متعدد داشته باشد. برای جلوگیری از ابهام در طراحی مستند،

1-token

- کنشگر اختصاص داده شده برای بررسی‌کردن پس زمینه با استفاده از مدارک ارائه شده هویت بهتر است «بازبین تصدیق»[1] نامیده شود.
- یک کنشگر اختصاص داده شده به ایجاد یک هستار اصلی که ادعا می‌کند در دوره روند اصالت‌سنجی هستار حضور دارد باید برچسب «بازبین اصالت‌سنج»[2] دریافت کند، و
- یک کنشگر که در ابتدا از اطلاعات هویت معتبر ارائه شده توسط یک سامانه مدیریت هویت بیرونی استفاده می‌کند بهتر است دارای برچسب «مصرف‌کننده اظهار نامه»[3] باشد.

یاداوری- بازبین تصدیق، به فرایند تصدیق هنگام ثبت مربوط است. عملکرد صحیح آن پایه و اساس عملکرد صحیح یک سامانه مدیریت هویت را فراهم می‌کند.

۵-۳-۲-۹ ممیز

نقش ممیز این است که تایید کند سامانه مطابق با خط‌مشی‌ها و رویه‌های مستند خود عمل می‌کند و مطابق با قانون و الزامات بیرونی اعمال شده دیگر است. ممیز یافته‌های خود را عمدتا به نهاد مدیریت هویت گزارش می‌کند اما همچنین ممکن است تعهد داشته باشد یافته‌های خود را بر اساس الزامات مقررات گذار و اعمال شده بیرونی به ارگان‌های مقررات گذار بیرونی دیگر نیز گزارش کند.

یاداوری- ممیزی به طور معمول شامل بررسی و تجزیه و تحلیل سوابق عملیات سامانه و تراکنش‌ها است و در نتیجه به دسترس‌پذیری این چنین سوابقی وابسته است.

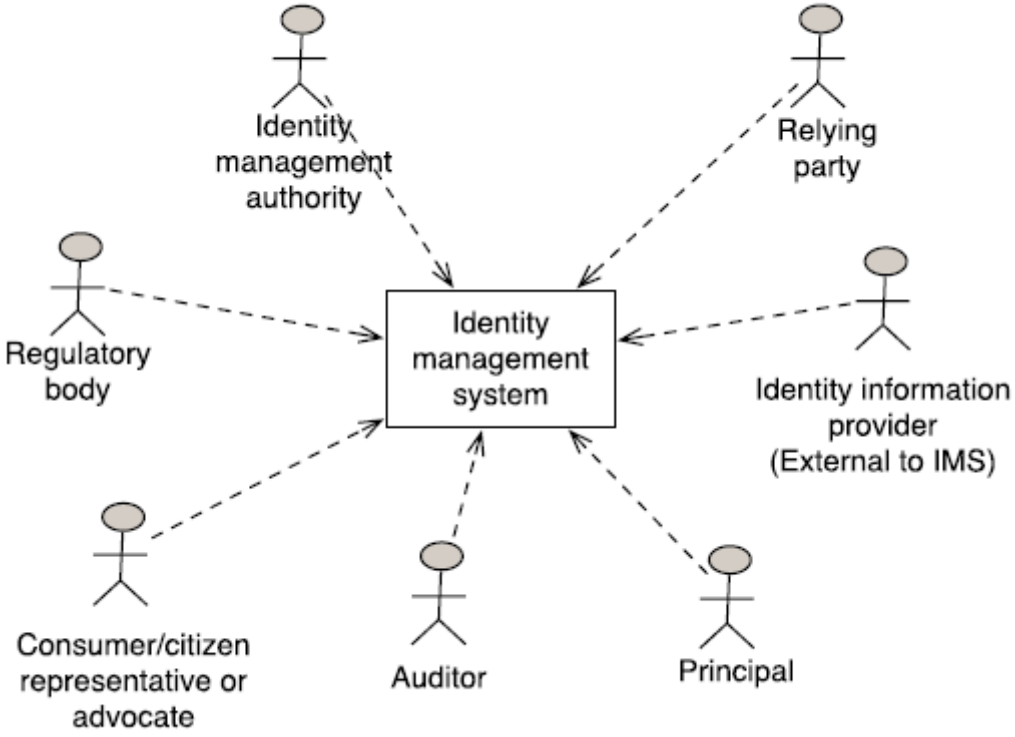
نگرانی‌های یک ممیز شامل:
- اسناد خط‌مشی شفاف برای بهره برداری از سامانه مدیریت هویت،
- دسترس‌پذیری سوابق اطلاعات مدیریت هویت در تمام مراحل مربوط به تراکنش‌های مدیریت هویت از جمله جمع آوری، ذخیره‌سازی ، استفاده، انتقال و در معرض گذاری اطلاعات هویت، و
- معیارهای روشن و قابل دسترسی برای ممیزی.

مسئولیت‌های یک ممیز شامل:
- به عنوان یک گزارشگر، به صورت دوره‌ای آماده کردن بیانیه شرح عملیات انجام شده توسط یک سامانه مدیریت هویت، به ویژه در رابطه با تناسب کارکردها با خط‌مشی‌های کارکردی،
- به عنوان پایش، به موقع به دست آوردن گزارش عملیات‌های خاص انجام شده توسط سامانه مدیریت هویت، برای بازبینی این که عملیات، خط‌مشی‌های قابل اجرا را برآورده می‌کند و برای هشدار هر گونه اختلاف به نهاد مدیریت هویت،
- به عنوان مشاور، توصیه به نهاد مدیریت هویت برای بهبودهای امکان‌پذیر در خط‌مشی‌های عملیاتی و اجرای آن‌ها، و
- به عنوان ناظر، گزارش به طرف‌های بیرونی، از جمله ارگان‌های مقررات گذار، برای انطباق عملیات با خط‌مشی‌ها، قوانین و مقررات قابل اجرا.

1-Proofing verifier
2-Authentication verifier
3-Assetion consumer

۵-۳-۳ مدل زمینه

شکل۱ مدل زمینه برای یک سامانه مدیریت هویت را نشان می‌دهد، با نشان دادن ذی‌نفعان کنشگر و غیرکنشگر همان گونه که در این استاندارد مشخص شده است.



شکل۱- مدل زمینه برای مدیریت هویت

طراحی مستند باید بازنمایی‌های منسجمی از ذی‌نفعان وکنشگرها همان‌گونه ارائه کند که به ترتیب در بند ۵-۳-۱ و بند ۵-۳-۲ تعریف شده است. طراحی مستند ممکن است ذی‌نفعان و یا کنشگرها دیگری را اضافه کند. ممکن است ذی‌نفعان و کنشگرهای مشخص شده در شکل را با بازنمایی‌های متعدد مجزا تعیین کند.

۵-۳-۴ مدل مورد کاربری[1]

۵-۳-۴-۱ کلیات

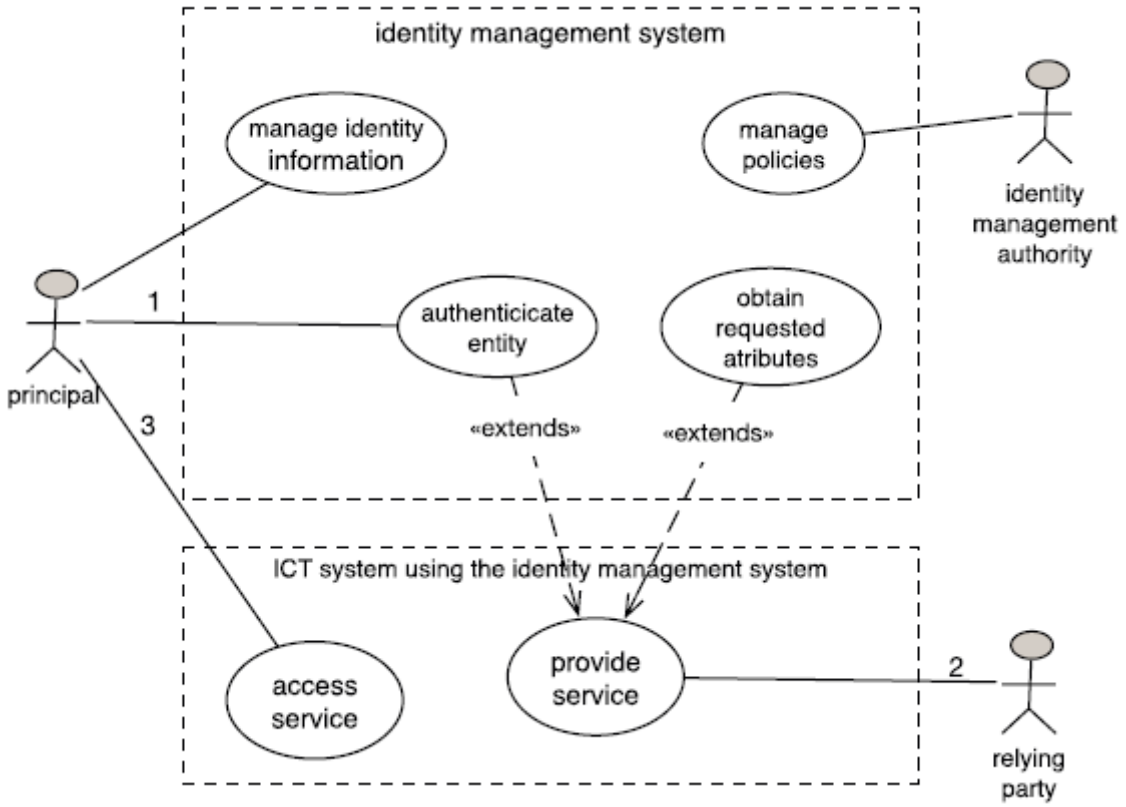
مدل مورد کاربری، برهم‌کنش‌های کنشگرها با سامانه مدیریت هویت را تعریف می‌کند. این مدل الزامات عملکردی را شناسایی می‌کند.

شکل۲ یک مورد کاربری ساده همراه با کنشگرهای استفاده شده که در برهم‌کنش با یک سامانه مدیریت هویت هستند، توسط یک طرف مورد اعتماد برای واپایش دسترسی به خدمات و یا منابع در حوزه کارکردی خود را نشان می‌دهد. موارد کاربری گسترش یافته و نمودار مولفه‌ای مربوط به پوشش جنبه‌های مهم یک سامانه مدیریت هویت در پیوست ب قرار داده شده است.

1-Use case model

شکل ۲ نشان می‌دهد:

- یک مدیر با یک سامانه مدیریت هویت تحت واپایش یک نهاد مدیریت هویت، یک رابطه ایجاد می‌کند؛
- یک مدیر، اطلاعات هویت را به منظور به دست آوردن دسترسی به منبع به یک بخش مورد اعتماد ارائه می‌کند؛
- یک طرف مورد اعتماد درخواست تایید هویت از مدیر می‌کند؛
- یک طرف مورد اعتماد درخواست مشخصه‌ها برای یک مدیر اصالت‌سنجی‌شده می‌دهد؛
- یک طرف مورد اعتماد اجازه دسترسی به یک منبع تحت واپایش خود می‌دهد؛
- یک مدیر دسترسی به یک منبع تحت واپایش طرف مورد اعتماد پیدا می‌کند.



شکل۲- مورد کاربری اصلی اطلاعات هویت

نمودار مورد کاربری نمونه در این شکل شامل هر دو فعالیت‌های مدیریتی (مدیریت اطلاعات هویت، مدیریت خط‌مشی‌ها) و فعالیت دسترسی به منبع می‌شود، که دربردارنده اصالت‌سنجی و به دست آوردن اطلاعات هویت است.

به منظور تسهیل در توصیف الزامات کارکردی موارد کاربری، یک مورد کاربری و دیدگاه کارکردی ممکن است کنشگرهای را متعلق به جوامع مختلف ارائه کند. یک جامعه نشان دهنده منافع مشترک در بهره برداری از سامانه مدیریت هویت است. جوامع عبارتند از:

- کاربران سازمانی،
- کاربران اداری، و

- کاربران غیرسازمانی است.
هستارهای غیرفردی نیز می‌توانند درخواست‌های دسترسی به منابع در سامانه‌های فناوری اطلاعات، بدهندکه نیاز به اصالت‌سنجی آن هستار دارد. هستارهای غیرفردی می‌توانند حاوی افزاره‌هایی علاوه بر هستارهای منطقی، از قبیل خدمات و نرم‌افزار باشند.

۵-۳-۴-۲ موارد کاربری کارمند

یک کارمند از سامانه برای بازیابی اطلاعات استفاده می‌کند. توافقبرای پردازش و دسترسی اطلاعات ضمنی است.
بر اساس وظایف کار اختصاص داده شده، یک کارمند انتظار اطلاعات هویت دقیق و دسترسی به اطلاعات هویت از سامانه مدیریت دارد. از نقطه نظر کارکنان، بهتر است این اطلاعات را به دقت به دست آورد تا از تمامیت منشاء و حفظ آن بتوان دفاع کرد.

۵-۳-۴-۳ موارد کاربری کارفرما

یک کارفرما مسئولیت مدیریت اجزای سامانه را به عهده دارد. برهم‌کنش‌ها با سامانه مدیریت هویت، با یک کارفرما می‌تواند همان گونه رفتار کرد که با یک کارمند رفتار می‌شود (به بند ۵-۳-۴-۲ مراجعه کنید).
از نقطه نظر کارفرما، اطلاعات هویت بهتر است به دقت نگهداری شده و تنها در صورت توافق پردازش شود.

۵-۳-۴-۴ موارد کاربری مدیر

در موارد کاربری مدیر، شناسایی بدون ابهام مهم ترین اصل است. دسترسی به اطلاعات یا توسط مدیر، توسط دستور از طرف مدیر و یا توسط طرف‌های کسب و کار با توافقصریح و روشن انجام می‌گیرد.
موارد کاربری مصرف‌کننده، مخاطرات، و کاهش ممکن، سوء استفاده از اطلاعات هویت در یک سامانه مدیریت هویت برای اهداف کسب و کار خارج از آن چه در طراحی مستند مشخص شده است، را توصیف می‌کند.
برای پرداختن به این نگرانی‌ها، موارد کاربری مصرف‌کننده معمولا جنبه‌ای از انطباق با الزامات مقررات گذار و قانونی را توصیف می‌کند.
مورد کاربری مدیر ممکن است یک فرایند خاص، برای ثبت نام مجدد از یک هستار به منظور ایجاد هویت دوباره خود توصیف کند. که شامل فرایندهایی برای به روز رسانی اطلاعات هویت و هرگونه اطلاعات هویت ذخیره شده در طرف‌های مورد اعتماد مربوط به ثبت نام دوباره هستار می‌شود.
از نقطه نظر مدیر، اطلاعات هویت برای جلوگیری از هر گونه نشت اطلاعات اساسا باید با شیوه‌ای محافظت شده در دسترس قرار گیرد. همانند جمع‌آوری اطلاعات برای یک هدف خاص هر استفاده دیگر بهتر است با توافقاز مدیر باشد. اطلاعات بهتر است از هر گونه خطر فساد و تبانی محافظت شود.

۵-۳-۴-۵ موارد کاربری افزاره

موارد کاربری افزاره، استفاده از افزاره‌ها به عنوان مدیر را در یک سامانه مدیریت هویت توصیف می‌کنند. افزاره‌ها به طور معمول از طرف و یا تحت واپایش هستارهای دیگر عمل می‌کنند، که ممکن است مدیرباشد

یا نباشد. خطرات ناشی از دست دادن واپایش فیزیکی و یا تطابق یکپارچگی افزاره ممکن است درموارد کاربری از افزاره مورد توجه قرار گیرد.
از نقطه نظر افزاره، اطلاعات هویت بهتر است از مخاطره فساد و تبانی محافظت می‌شود.

۵-۳-۵ مدل انطباق و حاکمیت

مدل انطباق و نظارت، سازوکارهای مفهومی را نشان می‌دهد که می‌تواند برای منطبق شدن با قانونمندی و سایر محدودیت‌های بیرونی قرار داده شده در یک سامانه مدیریت هویت اعمال شود. این امر شامل:
- اطمینان از دقت و صحت اطلاعات هویت به دست آمده از هستارهای مدیریتی در سطح مناسب از اطمینان، نه تنها در مقداردهی اولیه بلکه برای تمام طول عمر اطلاعات هویت مدیر؛
- اطمینان از منحصر به فرد بودن اطلاعات هویت مربوط به یک مدیر خاص؛
- اطمینان از اطلاعات هویتی که به دقت به دست آورده شده است؛
- اطمینان از این که دسترسی به انواع مختلف اطلاعات هویت به کاربرانی محدود شود که مجاز به دسترسی به نوع اطلاعات هستند و این امر با سطح مطلوب اطمینان تصدیق شود؛
- اطمینان از این که دسترسی به اطلاعات هویت برای ممیزی و ثبت در دسترس خواهد بود؛
- جلوگیری از پردازش و دسترسی به اطلاعات هویت بدون توافقمدیر در حدود مقررات محلی، منطقه‌ای و جهانی؛
- مطابقت با مقررات محلی، منطقه‌ای و جهانی، و براوردن انطباق و الزامات نظارتی.

۵-۴ دیدگاه کارکردی

۵-۴-۱ مدل مولفه

۵-۴-۱-۱ کلیات

طراحی مستند یک سامانه مدیریت هویت ممکن است اجزای توصیف شده به شرح زیر را به رسمیت بشناسد. پیوست پ نموداری که نشان دهنده اجزای یک سامانه مدیریت هویت است و برهم‌کنش‌های مربوط به آن‌ها را ارائه می‌کند. طراحی مستند، هر مولفه را که می‌بایست برطبق مفاهیم مشخص شده در دیدگاه‌های معماری آن، مورد انطباق با الزامات عملیاتی مورد نیاز باشد مشخص می‌کند.
طراحی مستند از یک سامانه مدیریت هویت باید عناصر عملیاتی یک سامانه از جمله ذی‌نفعان، کنشگرها، ساختمان داده‌ها، مولفه‌ها و واسطهای کارکردی را توصیف کند. ساختارهای داده‌ای که باید تعریف شود شامل:
- کلیدهای رمزنگاری و خصیصه‌ها، خدمات اکتشاف، خط‌مشی‌ها و دیگر قابلیت‌ها و الزامات؛
- قواعد نحوی و معنایی داده مشخصه هویت، و در جای مناسب، نگاشت قواعد به داده هویت معادل در سامانه‌های دیگر؛
- ساختارهای داده‌ای استفاده شده در انجام تراکنش‌هایی مثل درخواست‌های اصالت‌سنجی، اظهارات و کلیدهای جلسات.

۵-۴-۱-۲ مدیر

مدیران کنشگرهایی در سامانه مدیریت هویت هستند، که به خدمات و منابع موجود در حوزه کارکردی دسترسی دارند.
الزامات مورد نیاز برای دسترسی یک مدیر به منابع و خدمات موجود درحوزه کارکردی در استاندارد ISO/IEC 29146 مورد توجه واقع شده است.

۵-۴-۱-۳ ثبات هویت

هدف از ثبات هویت ارائه کردن یک مرجع ذیصلاح برای کسب اطلاعات هویت در حوزه یک سامانه مدیریت هویت است. ثبات هویت ممکن است از راه‌های مختلف پیاده‌سازی شود برای مثال، متمرکز، توزیع شده. برخی از اطلاعات هویت در یک ثبات هویت نیز ممکن است در یک افزاره ذخیره شود که توسط خود هستار نگهداری می‌شود، به عنوان مثال یک کارت هوشمند.
طراحی مستند از یک سامانه مدیریت هویت باید سازوکاری برای واپایش دسترسی به اطلاعات هویت موجود در ثبات هویت مشخص کنند. (به بند ۶-۲ مراجعه کنید).
اطلاعات هویت که هویت یک هستار را تعریف می‌کند ممکن است در یک یا چند عدد از سوابق مربوط به ثبات هویت ذخیره شده باشد. بخش‌بندی اطلاعات هویت به سوابق متعدد ممکن است بر اساس عواملی باشد که می‌تواند شامل:
- تفاوت‌ها در شرایط دسترسی، به عنوان مثال، برای پیاده‌سازی کمینه افشا؛
- تفاوت‌ها در مدت زمانی که اطلاعات هویت در ثبات هویت حفظ خواهد شد؛
- تفاوت‌ها در محل ذخیره‌سازی، به عنوان مثال، در یک مخزن مرکزی و / یا در یک افزاره شخصی.
ساختار ذخیره‌سازی داده‌ها برای اطلاعات هویتی و روش‌های پیاده‌سازی یک ثبات هویت و واپایش دسترسی فراتر از محدوده این سند است.

۵-۴-۲ فرایندها و خدمات

۵-۴-۲-۱ مستندات

طراحی مستند بهتر است توصیف مولفه‌ها و عملیات را بر اساس اصطلاح‌شناسی در جداول این بند پایه‌گذاری کند.
طراحی مستند بهتر است شامل نمودارهای UML برای توصیف فرایندها باشد.
یادآوری- نمودارها در پیوست پ از این استاندارد می‌تواند به عنوان قالب استفاده شود.

طراحی مستند ممکن است مشخص‌کننده یک پیاده‌سازی باشد که مولفه‌هایی استفاده می‌کند که زیرمجموعه‌ای از فرایندها در این جداول را انجام می‌دهند.

۵-۴-۲-۲ فرایندهای مدیریت اطلاعات هویت

۵-۴-۲-۲-۱ کلیات

پردازش اطلاعات در سامانه مدیریت هویت، فرایندهایی به شرح زیر است اما به آن‌ها محدود نمی‌شود:
- تأمین اطلاعات هویت،

- پردازش اطلاعات هویت، و
- اعطای دسترسی به پردازش هویت.

یاداوری- فرایندهای این بند اشاره به اطلاعات هویت موجود در ثبات هویت دارد. فرایندهای وارد شدن به اطلاعات هویت در اینجا شرح داده نشده است. به استاندارد ISO / IEC 29003 مراجعه کنید.

جدول۱، یک مرور کلی از اطلاعات مبادله شده در سامانه مدیریت هویت مربوط به فرایندهای شرح داده شده در این بند، ارائه می‌کند.

جدول۱- مرور کلی اطلاعات مبادله شده در فرایندهای مدیریت اطلاعات هویت

فرایند	کنشگرها			
	منبع		گیرنده	
	عنصر معماری	اقدام	عنصر معماری	اقدام
پردازش اطلاعات هویت	فراهم کننده اطلاعات هویت	عملیات‌های پردازش اطلاعات را اعمال می‌کند	فراهم کننده اطلاعات هویت	نتایج را نگه‌داری می‌کند
			ثبات	نتیجه پردازش را ذخیره می‌کند، ممکن است اطلاعات را در یک یا بیشتر از هویت‌ها به‌روزرسانی کند
اعطا کردن مجوز پردازش اطلاعات هویت	نهاد مدیریت هویت	در مورد پردازش اطلاعات هویت اطلاع‌رسانی می‌کند اجازه عملیات‌های پردازش را خواستار می‌شود	مدیر	عملیات‌های پردازش اطلاعات را رد یا اعطا می‌کند
	مدیر	اطلاعات در مورد پردازش هویت را درخواست می‌کند	نهاد مدیریت هویت	اطلاعات درخواست شده را فراهم می کند
آماده سازی	طرف مورد اعتماد	خدمات آماده‌سازی را درخواست می‌دهد	نهاد مدیریت هویت	خدمت آماده‌سازی را رد یا اعطا می‌کند، شرایط را مشخص می‌کند
			فراهم کننده اطلاعات هویت	طرف مورد اعتماد را به عنوان دریافت کننده خدمت آماده‌سازی ثبت می‌کند
	فراهم کننده اطلاعات هویت	اطلاعات هویت را می‌فرستد	طرف مورد اعتماد	اطلاعات به‌روز شده را به پردازش خدمت‌اش اعمال می‌کند
	نهاد اطلاعات هویت	با اعلان و سطح اطمینان، اطلاعات هویت را تکمیل می‌کند	طرف مورد اعتماد	تایید می‌کند که اعلان‌ها معتبر هستند و الزامات سطح اطمینان را برآورده می‌سازد

۵-۴-۲-۲-۲ نگهداری اطلاعات هویت

تأمین اطلاعات هویت، فرایند ارائه اطلاعات هویت به روزشده، است که به مدیران مربوط می‌شود چه زمانی یک هویت ایجاد شده است و یا اطلاعات قبلا ارائه شده دیگر درست نیست. دسترسی به اطلاعات هویت توسط مجوزهای واگذار شده به طرف مورد اعتماد، واپایش می‌شود.

طراحی مستند باید رویه‌ها و شرایطی برای شروع تأمین یک طرف مورد اعتماد مشخص کند.

۵-۴-۲-۲-۳ تأمین اطلاعات هویت

پردازش اطلاعات هویت باید با توجه به خط‌مشی‌ها انجام پذیرد. پردازش اطلاعات هویت ممکن است اطلاعات هویت جدیدی با دسترسی به اطلاعات هویت مربوط به یک و یا چند تن از مدیران تولید کند.

۵-۴-۲-۲-۴ اعطای دسترسی به پردازش هویت

دسترسی به اطلاعات هویت برای پردازش اطلاعات هویت و اطلاعات تولید شده باید مطابق با خط‌مشی‌های قابل اجرا، واپایش شود.

۵-۴-۲-۳ فرایندهای خاص مدیریت اطلاعات هویت

۵-۴-۲-۳-۱ کلیات

این بند فرایندهای اضافی مخصوص پیاده‌سازی‌های مختلف یک سامانه مدیریت هویت را مشخص می‌کند.

این فرایندها شامل موارد زیر است:

- ممیزی،
- تولید هویت‌های مرجع، و
- نامعتبر.

جدول۲ یک مرور کلی از اطلاعات مبادله در سامانه مدیریت هویت مربوط به فرایندهای شرح داده شده در این بند ارائه می‌کند.

جدول۲- مرور کلی اطلاعات مبادله شده در فرایندهای مدیریت اطلاعات هویت خاص

فرایند	کنشگرها			
	منبع		گیرنده	
	عنصر معماری	کنش	عنصر معماری	کنش
ممیزی کردن	نهاد مدیریت هویت	معین می‌کند که عملیات‌ها ثبت شوند و وقایع گزارش شوند	تمام کنشگرها	تعاریف را در پیاده سازی فرایند می‌گنجاند
	مدیر	اعتراض را ثبت می‌کند	ممیز	به اعتراض رسیدگی می‌کند
	نهاد مدیریت هویت	ثبت عملیات‌های مدیریت را برقرار می‌سازد		فهرست ثبت شده‌ها و وقایع را بازبینی می‌کند
	ثبات هویت	ثبت عملیات‌های دسترسی به داده را برقرار می‌سازد		
	فراهم کننده اطلاعات هویت	ثبت درخواست‌های اطلاعات هویت و فعالیت های آماده سازی اطلاعات را برقرار می‌سازد		
	نهاد اطلاعات هویت	ثبت اعلان‌های اطمینان فراهم شده را برقرار می‌سازد وقایع را گزارش می‌دهد		
	ممیز	یافته ها را گزارش می‌دهد تغییرات را توصیه می‌کند.	نهاد مدیریت هویت	خط‌مشی ها و رویه‌ها را برای هر تغییر توصیه شده تنظیم می‌کند
ایجاد کننده شناسانه مرجع	فراهم کننده اطلاعات هویت	شناسانه مرجع را درخواست می‌دهد	ایجاد کننده شناسانه مرجع	شناسانه مرجع را ایجاد می‌کند
	مدیر	اطلاعات هویت را برای استفاده به عنوان شناسانه مرجع فراهم می‌کند	ایجاد کننده شناسانه مرجع	صلاحیت اطلاعات هویت فراهم‌شده را به عنوان شناسانه مرجع اعتبارسنجی می‌ند شناسه مرجع را تولید می‌کند
	ایجاد کننده شناسانه مرجع	شناسانه مرجع ایجاد شده را فراهم می‌کند	فراهم کننده اطلاعات هویت	شناسانه مرجع را با اطلاعات هویت دیگر ربط می‌دهد
ابطال اطلاعات هویت	ممیز	یافته ها را گزارش می‌دهد تغییرات را توصیه می‌کند.	نهاد مدیریت هویت	نامعتبر را تایید می‌کند
	مدیرها	خطا را مشخص می‌سازد	فراهم کننده اطلاعات هویت	اطلاعات را اصلاح می‌کند
	فراهم کننده اطلاعات هویت	در مورد تغییر اطلاع می‌دهد	مدیرها	اعلان تغییر را اعتبارسنجی و تایید می‌کند
			طرف مورد اعتماد	اعلان تغییر را تایید می‌کند

۵-۴-۲-۳-۲ ممیزی

کنشگرها و مولفه‌های مختلف بهتر است در طول زمان برای صحت عملکرد نقش خود در چارچوب مدیریت هویت، مورد ممیزی قرار گیرند:

- ثبات هویت و مولد مرجع هویت بهتر است به طور مداوم برای میزان دقت واپایش یکپارچگی خود مورد ممیزی قرار گیرند،
- ارائه دهنده اطلاعات هویت بهتر است به طور منظم برای دقت و صحت رویه‌های واپایش خود در ارائه اطلاعات هویت مورد ممیزی قرار گیرد،
- نهاد اطلاعات هویت بهتر است به طور منظم برای دقت و صحت رویه‌های واپایشی خود در مدیریت اطلاعات هویت مورد ممیزی قرار گیرد.

ممیزان بهتر است از طریق یک فرایند واپایش معتبر برای بازنگری‌های خود از کنشگرها و مولفه‌های چارچوب مدیریت هویت مورد تایید قرار گیرند.

۵-۴-۲-۳-۳ تولید هویت‌های مرجع

یک هویت مرجع، به عنوان بخشی از ثبت هویت ایجاد شده است و به اطلاعات هویت هستار مربوطه مرتبط است. مولد هویت مرجع که با هر اطلاعات هویت مورد نیاز موجود، فراخوانی می‌شود، و یک ارزش شناسانه تولید می‌کند. هویت مرجع با دیگر اطلاعات هویتی در ثبات هویت بایگانی می‌شود.

۵-۴-۲-۳-۴ نامعتبر

طراحی مستند از یک سامانه مدیریت هویت ممکن است شرایط و رویه‌هایی برای صحه‌گذاری‌نشدن اطلاعات هویت مشخص کند.

یاداوری- صحه‌گذاری‌نشدن اطلاعات هویت مستلزم از نامعتبر بودن هر گونه اظهارات قابل اثبات، به عنوان مثال با رمزنگاری، و ابطال اعتبار اطلاعات هویت که ممکن است توسط کاربری که از اطلاعات استفاده می‌کرده مستندشده باشد، می‌باشد. در عمل، حذف بیانیه‌ای قابل اثبات، به صحه‌گذاری‌نشدن اطلاعات می‌انجامد.

شرایط زیر مجاز است در نظر گرفته شود:

- شواهد هویت پیدا شده که به اشتباه یا رویه نادرست یا فریبکارانه به عنوان معتبر بازبینی شده؛
- خطاهای یافت شده در اختصاص و یا شناخت خواص؛
- تغییرات رخ داده در خط‌مشی‌ها برای ثبت نام یا شناسایی؛
- اطلاعات هویت مدیر توسط شخص دیگری به شیوه‌ای مورد استفاده قرار گرفته که نیاز به ایجاد دوباره مجموعه‌ای جدید از اطلاعات هویت می‌باشد.

سازوکار نامعتبر، در صورت پشتیبانی، باید مطابق با خط‌مشی نامعتبر انجام شود. این خط‌مشی بهتر است موارد زیر را مورد توجه قرار دهد:

- شرایط و سازوکارهایی برای تامین صحه‌گذاری‌نشدن؛
- سطح اطمینان برای صحه‌گذاری‌نشدن پیام؛
- شرایط و سازوکارهایی برای مشاوره به یک مدیر برای صحه‌گذاری‌نشدن یک مشخصه در یکی از هویت‌ها؛

- سازوکار برای پاسخ به درخواست‌ها در مورد وضعیت اعتبار یک مشخصه.

۵-۴-۲-۴ کارکردهای اضافی

۵-۴-۲-۴-۱ کلیات

طراحی مستند یک سامانه مدیریت هویت ممکن است کارکردهای اضافی همچنان که در این بند شرح داده شده است را مشخص کنند. این کارکردها شامل موارد زیر می‌شود:

- رخ‌نمون اطلاعات هویت،
- رضایت،
- کشف نهاد هویت، و
- انتشار.

جدول ۳ یک مرور کلی از اطلاعات مبادله شده در سامانه مدیریت هویت مربوط به فرایندهای شرح داده شده در این بند. ارائه می‌کند.

جدول۳- مرور کلی از اطلاعات مبادله شده در کارکردهای اضافی سامانه مدیریت هویت

فرایند	کنشگرها			
	کنش		گیرنده	
	عنصر معماری	اقدام	عنصر معماری	کنش
رخ‌نمون سازی اطلاعات هویت	فراهم کننده اطلاعات هویت	رخ‌نمون را برای نوع هستار تعیین می‌کند	فراهم کننده اطلاعات هویت	رخ‌نمون هویت را پیاده سازی می‌کند
توافقحریم خصوصی	مدیر	خصیصه اطلاعات هویت را برای بازبینی یا مخفی سازی درخواست می‌دهد	فراهم کننده اطلاعات هویت	خط‌مشی را برای تقاضا صحت سنجی می‌کند، تغییر را بر این اساس پیاده سازی می‌کند، اطلاعات را ارسال می‌کند
کشف نهاد هویت	نهاد ثبت هویت	برقراری اعتماد را با نهاد هویت دیگر درخواست می‌دهد	بخش مورد اعتماد	صلاحیت درخواست اعتماد را بررسی می‌کند
	طرف مورد اعتماد	درخواست اعتماد را ارسال می‌کند	نهاد اطلاعات هویت	برقراری اعتماد را اعتبارسنجی می‌کند
	نهاد اطلاعات هویت	تحویل اطلاعات هویت را تایید می‌کند	فراهم کننده اطلاعات هویت	اطلاعات هویت را تحویل می‌دهد
انتشار	نهاد مدیریت هویت	خط‌مشی انتشار را ایجاد می‌کند	نهاد اطلاعات هویت	خط‌مشی انتشار را اعتبار سنجی می‌کند
	فراهم کننده اطلاعات هویت	خط‌مشی انتشار اعتبار سنجی شده را پیاده سازی می‌کند	طرف مورد اعتماد	اطلاعات منتشر شده را دریافت می‌کند

۵-۴-۲-۴-۲ خدمات رخ‌نمون اطلاعات هویت

خدمات رخ‌نمون اطلاعات هویت نمود مناسبی از اطلاعات هویت برای هستارهای ارائه شده از این نوع، یعنی انسان، افزاره، و هستارهای سازمانی فراهم می‌کند. این امر ممکن است شامل تعریف، و نگهداری، و استفاده از مشخصه‌های هویت مختلف و قالب داده‌های هویت برای هستارهای مختلف باشد.

۵-۴-۲-۴-۳ رضایت

فرایند توافقحریم خصوصی ممکن است کاربردهای زیر را ارائه کند:

- اصالت‌سنجی هویت یک هستار به عنوان یک مدیرشناخته شده و مجاز به دسترسی به اطلاعات هویت؛
- ارائه اطلاعات هویت ثبت شده؛
- تغییر، گسترش و یا حذف اطلاعات هویتی که قبلا توسط مدیر ارائه شده است؛
- درخواست اصلاح اطلاعات هویتی تولیدشده؛
- اطلاع رسانی به مدیر برای استفاده مورد نظر از اطلاعات هویت.

۵-۴-۲-۴-۴ کشف نهاد اطلاعات هویت

فرایند کشف نهاد اطلاعات هویت، توانایی کشف سایر نهادهای اطلاعات هویت و ایجاد همکاری برای دسترسی به اطلاعات هویت در سطح اطمینان مورد نیاز فراهم می‌کند.

این خدمات نامزدهای نهاد اطلاعات هویت طرف سوم و شرایط اشتراک و فرایندهای اطلاع رسانی با این نهادهای را مشخص می‌کند.

خدمات کشف نهاد اطلاعات هویت ممکن است کارکردهای زیر را ارائه کند:

- تصویب یک نهاد اطلاعات هویت دیگر، برای ایجاد رابطه اعتماد بر اساس الزامات تعیین شده از کیفیت و انطباق و اجزای تشکیل دهنده،
- قبول یک هستار به عنوان یک مشترکِ مجاز اطلاعات هویت،
- مشخص کردن نوع اطلاعات هویت مورد نیاز،
- مشخص کردن سطح مورد نیاز از اطمینان در دسترسی به اطلاعات هویت،
- مشخص کردن سازوکارهای امنیتی برای محافظت از اطلاعات هویت ارائه شده،
- مشخص کردن یک هویت برای اطلاع رسانی در مورد اطلاعات هویت مورد نیاز،
- دریافت اطلاعات هویت در صورت درخواست، و
- دریافت اطلاعات هویت زمانی که چنین اطلاعاتی تغییر می‌کند.

فهرست کارکردهای خدمات کشف ممکن است بستگی به اعتماد ایجاد شده با دیگر نهادها و شرایط آن اعتماد، شامل شود.

۵-۴-۲-۴-۵ انتشار

فرایند انتشار توانایی انتشار اطلاعات هویت به درخواست کنندگان خدمات و ایجاد همکاری برای دسترسی به اطلاعات هویت در سطح اطمینان مورد نیاز را فراهم می‌کند. خدمات اشتراک و اطلاع رسانی نیز بخشی از خدمات نشر می‌باشد.

خدمات نشر ممکن است کارکردهای زیر را ارائه کند:
- انتشار و اصلاح انتشار خدمات تأمین اطلاعات هویت و شرایط دسترسی و استفاده از این اطلاعات؛
- قبول یک درخواست کننده برای ارائه اطلاعات هویت بر اساس الزامات تعیین شده از کیفیت و انطباق مولفه؛
- قبول یک هستار به عنوان مشترکِ اطلاعات هویت؛
- مشخص کردن نوع اطلاعات هویت که دسترسی به آن مجاز است؛
- مشخص کردن سطح مورد نیاز از اطمینان در دسترسی به اطلاعات هویت؛
- مشخص کردن سازوکارهای امنیتی برای محافظت از اطلاعات هویت در حال ارائه؛
- مشخص کردن یک شناسانه که اعلان‌های اطلاعات هویت برایش مورد نیاز است؛
- اطلاع از تغییرات اطلاعات هویت زمانی که این تغییر رخ می‌دهد.

فهرست کارکردهای خدمات انتشار ممکن است بستگی به الزامات برای دسترسی به این اطلاعات داشته باشد.

۵-۴-۳ مدل فیزیکی

این دیدگاه به توصیف پیاده‌سازی هر یک از عناصر سامانه‌های مدیریت هویت می‌پردازد که قابلیت کارکردی برای پیاده‌سازی دیدگاه فرایندی را ارائه می‌کند. نمایش فیزیکی ممکن است پیاده‌سازی‌های فیزیکی جایگزین، به عنوان مثال، تفاوت در هزینه و عملکرد، ارائه کند.

این استاندارد دیدگاه فیزیکی را تنها در سطح مولفه‌های ساختاری مورد توجه قرار می‌دهد. جنبه‌های پیاده‌سازی دیدگاه فیزیکی فراتر از دامنه کاربرد این استاندارد می‌باشد.

۵-۵ فرانامه‌های مدیریت هویت

۵-۵-۱ کلیات

یک سامانه مدیریت هویت ممکن است مطابق فرانامه‌های مختلف گسترش یابد. فرانامه‌ی استقرار، بر اداره امور سامانه مدیریت هویت اثر خواهد گذاشت. فرانامه‌ی استقرار روابط اعتمادی که نیاز است بین طرف‌های درگیر در کار و اداره امور سامانه مدیریت هویت وجود داشته باشد تعیین خواهد کرد.

فرانامه‌ی استقرار ممکن است زمان گسترش یک سامانه مدیریت هویت‌های موجود انتخاب شود. مدل گسترش استقرار ممکن است متفاوت از مدل استقرار اصلی باشد.

فرانامه‌های مختلف که ممکن است در پیاده‌سازی سامانه مدیریت هویت استفاده شود عبارتند از:
- فرانامه‌ی سازمانی،
- فرانامه‌ی متحدان،
- فرانامه‌ی خدمت، و
- فرانامه‌ی ناهمگن.

۵-۵-۲ فرانامه‌ی سازمانی

با یک فرانامه‌ی سازمانی، یک سامانه مدیریت هویت در زمینه یک سازمان واحد استقرار می‌یابد که در آن اعتماد به عملیات و اداره امور از ساختار اداری سازمان به ارث برده شده است و سازمان، مسوول مدیریت اطلاعات جمع آوری شده ذخیره شده و پردازش شده توسط سامانه می‌باشد.

یک مدل سازمانی یک مدل متمرکز است (به استاندارد ملی ایران شماره ۱-۱۷۶۴۲ مراجعه کنید).

۵-۵-۳ فرانامه متحد

یک سامانه مدیریت هویت متحد شامل زیر سامانه‌های چندگانه، با نوع اداره مستقل سامانه‌های فرعی است. اعتماد در عملیات، و اداره امور یک اتحادیه از طریق موافقت مذاکره‌شده پایه‌گذاری شده است. اداره امور ممکن است به یک سازمان با ساختار یا اساسنامه رسمی واگذار شود که شامل قوانین عملیاتی، مسئولیت‌ها و تعهدات تعریف شده برای اعضای شرکت است.

هنگامی که یک دامنه کارکردی به منظور اتصال به و یا همکاری با دیگر دامنه‌ها نیاز به توسعه یافتن داشته باشد، یک رویکرد فرانامه متمرکز در حوزه‌های اصلی یکپارچگی و یک دامنه بزرگتر تکی به وجود می‌آید که توسط یک سامانه مدیریت هویت واحد، واپایش می‌شود. یک فرانامه‌ی متحد یک رویکرد جایگزین ارائه می‌دهد که اجازه می‌دهد سامانه‌های مدیریت هویت به تبادل اطلاعات بین حوزه‌ها بدون نیاز به یکپارچگی دامنه‌ها بپردازند.

یاداوری- یکپارچگی کامل سامانه، یکپارچگی الزامات دو حوزه در یک رویکرد معماری جدید تحمیل می‌کند، در عین حالی که از تمام دیدگاه‌های مختلف معماری از دو حوزه جدا، حمایت می‌کند. در عوض مدل اتحادی ساختار را بدون تغییر رها می‌کند، اما سازوکار جدیدی در نظر گرفته که اجازه می‌دهد تا ساختارهای جداگانه با یکدیگر ارتباط برقرارکنند.

سازوکارهای حمایت از اتحادیه باید سطح محرمانه، یکپارچگی و اعتماد مورد نیاز میان حوزه‌های از هم جدا را فراهم کند تا، به تبادل اطلاعات هویت بپردازند، واطلاعات هویت حوزه‌های دیگر را استفاده کنند.

۵-۵-۴ فرانامه خدمت

صرف نظر از اینکه استقرار فرانامه، متعهد یا متحد باشد، مولفه‌های کارکردی در سامانه مدیریت هویت ممکن است به عنوان خدمات شناخته شوند.

طراحی مستند یک سامانه مدیریت هویت استقرار یافته به عنوان مدل خدمات، باید اعتماد و مولفه‌های انتشار مشخص کند و سازوکارهایی تعیین کند تا اطمینان حاصل شود که زمانی که خدمات اطلاعات هویت ارائه می‌شود سطح مورد نیاز از محرمانه بودن، یکپارچگی و اعتماد به دست آید.

۵-۵-۵ فرانامه ناهمگن

یک فرانامه‌ی ناهمگن فرانامه‌یی است که در آن سازمان‌های مستقل، اعتبارهای هویت برای مدیران صادر می‌کنند که با مشخصات و سطح اطمینان شناخته شده مطابقت داشته باشد. طرف‌های مورد اعتماد ممکن است با استفاده از این اعتبارهای هویت به اصالت‌سنجی مدیران اقدام کنند زمانی که مخاطره همراه خط‌مشی مدیریت، قابل قبول تلقی شده است.

۶ الزامات مدیریت اطلاعات هویت

۶-۱ کلیات

این بند الزامات مدیریت اطلاعات هویت توسط یک سامانه مدیریت هویت بر اساس مدل مرجع و انواع بکارگیری و ذی‌نفعان مشمول را توضیح می‌دهد. این بند الزامات کارکردی را برای حمایت از برهم‌کنش‌های کنشگرها با سامانه را از الزامات غیر کارکردی متمایز می‌کند که مربوط به شرایط عملیاتی دیگری می‌شود که یک سامانه مدیریت هویت باید به آن احترام بگذارد.

الزامات کارکردی موارد زیر را در بر می‌گیرد:

- خط‌مشی دسترسی؛
- شرایط مدیریت؛
- شرایط نگهداری.

الزامات این بند شامل واپایش‌هایی که قسمتی از رویه هستند نمی‌شود. (به استاندارد ISO/IEC 24760-3 مراجعه کنید).

۶-۲ خط‌مشی دسترسی برای اطلاعات هویت

طراحی مستند یک سامانه مدیریت هویت باید یک خط‌مشی دسترسی اطلاعات فراهم کند تا مشخص سازد:

- شرایط و سازوکارهایی برای دسترسی به مقدار هر مشخصه در سامانه؛
- معیاری برای اجازه دسترسی با سطوح مناسبی از اطمینان؛
- کدام عملیات‌های دسترسی به اطلاعات هویت نیاز به ثبت شدن دارند، و با چه جزئیاتی؛
- چگونه ثبات هویت محافظت از اطلاعات هویتی را که در بردارد به اجرا در می‌آورد؛
- مدت زمان نگهداری رکوردهای دسترسی اطلاعات هویت.

۶-۳ الزامات کارکردی برای مدیریت اطلاعات هویت

۶-۳-۱ خط‌مشی برای چرخه حیات اطلاعات هویت

طراحی مستند یک سامانه مدیریت هویت، باید یک خط‌مشی برای مدیریت چرخه حیات اطلاعات هویت فراهم کند که مشخص سازد:

- الزامات اطمینان برای دقت اطلاعات هویت مورد نیاز برای ثبت نام؛
- شرایط و رویه فعال کردن یک هویت؛
- شرایط و رویه نگه داشتن یک هویت برای مثال بررسی دقت و درستی اطلاعات هویت؛
- شرایط و رویه تنظیم کردن اطلاعات هویت برای یک مدیر؛
- شرایط و رویه معلق کردن یک هویت؛
- شرایط و رویه تشخیص هویت برای دوباره فعال کردن یک هویت؛
- شرایط و رویه برای حذف یا بایگانی یک هویت؛
- شرایط و رویه برای حفظ اطلاعات؛
- شرایط و رویه برای بازگردانی یک هویت؛

- اطلاعاتی که باید بایگانی شود و مدت زمان بایگانی و شرایط نگهداری یک هویت بایگانی شده؛
- شرایط و رویه پایان دادن یا حذف یک هویت.

۶-۳-۲ شرایط و رویه حفظ اطلاعات هویت

طراحی مستند یک سامانه مدیریت هویت باید مشخص سازد که چگونه دقت اطلاعات هویتی که مدیریت می‌کند حفظ می‌شود.

طراحی مستند یک سامانه مدیریت هویت باید شامل رویه‌هایی برای پایش کیفیت اطلاعات هویت در ثبات هویت به خصوص برای مشخصه‌هایی باشد که:

- جنبه‌هایی از یک هستار را ارائه دهد که ممکن است در گذر زمان تغییر کنند؛
- ممکن است بر درجه اطمینان اطلاعات مستندشده تاثیر بگذارند.

طراحی مستند یک سامانه مدیریت هویت باید خط‌مشی‌هایی را برای عملیات‌ها جهت شناسایی تغییرات در اطلاعات هویت به خصوص در مورد مشخصه‌هایی که ممکن است مقدارشان در گذر زمان تغییر کند و درجایی فراهم کند. که تغییرات بر سطح اطمینان هویت مستندشده تاثیر می‌گذارد.

طراحی مستند یک سامانه مدیریت هویت باید خط‌مشی‌هایی جهت حفظ یکپارچگی اطلاعات هویت و فراداده در ثبات هویت فراهم آورد. چنین خط‌مشی‌هایی می‌توانند موارد زیر را مشخص سازند:

- رویه‌هایی جهت جلوگیری از به هم ریختگی اطلاعات مستندشده؛
- رویه‌هایی جهت شناسایی فساد اطلاعات مستندشده، و
- رویه‌هایی جهت تصحیح کردن فساد اطلاعات مستندشده.

طراحی مستند یک سامانه مدیریت هویت باید سازوکاری را برای بخش‌های مورد اعتماد جهت گزارش رفتار مشکوک یا جعل نسبت به ثبات هویت فراهم کند.

۶-۳-۳ واسط اطلاعات هویت

یک سامانه مدیریت هویت مجاز است شامل مولفه‌هایی با یک واسط کاربری برای ارائه اطلاعات هویت باشد. دسترسی به اطلاعات هویت در یک واسط کاربر باید توسط خط‌مشی‌ای اداره شود که مشخص می‌سازد:

- واپایش دسترسی و
- ممیزی.

اهداف واسط ارائه اطلاعات شامل

- ارائه اطلاعات هویت؛
- ارائه فراداده اطلاعات هویت؛
- ارائه اطلاعات در مورد عملیات های در جریان و گذشته سامانه؛
- فراهم کردن واپایش‌هایی جهت پردازش یا اصلاح اطلاعات کنونی، و
- اعمال خط‌مشی‌های کاربری برای اطلاعات ارائه شده مربوط به کنشگر.

طراحی مستند یک سامانه مدیریت هویت باید قالب و شرایط ارائه اطلاعات هویت به شکل قابل خواندن توسط انسان را مشخص سازد (به بند۶-۲ مراجعه کنید). الزامات در طراحی مستند در ارائه اطلاعات هویت به شکل قابل دسترسی توسط انسان باید توانایی ها و محدودیت‌های کاربر اطلاعات را در نظر بگیرد.

۶-۳-۴ شناسانه مرجع

یک سامانه مدیریت هویت می‌تواند شامل مولفه‌ای جهت ایجاد یک شناسانه مرجع باشد. وظیفه یک شناسانه مرجع اطمینان دادن از این است که یک هویت مشخص شناخته شده در سامانه اطلاعات هویت منحصر بفرد باشد.

دسترسی به مقدار یک شناسانه مرجع ممکن است محدود شده باشد برای مثال منحصرا از داخل سامانه مدیریت هویت. طراحی مستند باید خط‌مشی دسترسی برای شناسانه مرجع را مشخص سازد.

یاداوری- دسترسی محدود به شناسانه مرجع از استفاده آن در دیگر سامانه‌های مدیریت هویت جلوگیری می‌کند.

طراحی مستند یک سامانه مدیریت هویت باید ثبات هویت آن را با یک مولد شناسانه مرجع مرتبط سازد. مولد شناسانه مرجع باید یک مقدار منحصر به فرد برای هر اصل ایجاد کند که از آن، اطلاعات هویت در ثبات هویت ذخیره می‌شوند.

یاداوری۱- معمولا شناسانه مرجع هنگامی ایجاد می‌گردد که یک هستار در یک دامنه وارد می‌شود.

یاداوری۲- شناسانه مرجع ایجاد شده ممکن است بر اساس اطلاعات دریافت شده از هستار باشد برای مثال یک نام مستعار برگزیده که برای منحصر به فرد بودن بررسی شده است.

یاداوری۳- شناسانه مرجع ممکن است تولید شده از اطلاعات هویتی برای همان اصلی باشد که از یک دامنه دیگر گرفته شده باشد که در آن، اصل شرکت داشته است. این امر می‌تواند شامل شناسانه مرجع از دامنه دیگر باشد.

در حالی که سازوکار دقیق برای ایجاد ارزش‌های مشخصه منحصر به فرد فراتر از حوزه این استاندارد می‌باشد، طراحی یک مولد شناسانه مرجع باید مشخص سازد:

- الگوریتم به کار برده شده برای ایجاد یک مقدار منحصر به فرد همراه با توضیحات مستدلی از شایستگی‌اش؛
- واسطی که یک مقدار جدید را برای یک هستار جدید یا یک هستار موجود دریافت می‌دارد، به صورتی که منحصر به فرد بودن را حفظ کند؛
- الزامات برای ورودی مورد نیاز الگوریتم، اگر موجود باشد؛
- اگر ثبت وقایع پشتیبانی می‌شود، الزامات برای ثبت وقوع تولید یک شناسانه مرجع؛
- سنجه‌های امنیتی که از عملیات‌های سامانه (ICT) محافظت می‌کند که مولد شناسانه مرجع را میزبانی می‌کند.

یاداوری۱- وقتی هیچ اتصال یا ارتباط قابل اطمینان بین دامنه‌ها وجود نداشته باشد، هر دامنه شناسانه مرجع خودش را ایجاد می‌کند و احتمال ایجاد شدن شناسانه مشابه برای اصل‌های متفاوت یا مشابه عضو شده در چندین دامنه انتظار می‌رود که بسیار کم باشد.

یاداوری۲- به صورت کلی مقدار یک شناسانه با یک دامنه منشا که نامربوط به سامانه مدیریت هویت باشد نمی‌تواند جهت برآورده ساختن معیارهای یک شناسانه مرجع جدید تضمین شده باشد و برای اینکه مستقیما به کار برده شود نا مناسب می‌باشد. با این وجود، هر هنگام دانسته شود که چگونه شناسانه مرجع در یک دامنه نامربوط بخصوص ساخته شده است، برای

مثال: در تطابق با یک استاندارد بین المللی، چنین مقدار شناسانه مرجع می‌تواند با فراهم شدن اینکه مقدارش به صورت اطمینان بخشی به دست بیاید، به کار برده شود.

اگر یک سامانه مدیریت هویت از ثبت وقایع عملیات‌های مولد شناسانه مرجع پشتیبانی کند، درایه ثبت وقایع بهتر است شامل:

- شناسانه مرجع ایجاد شده؛
- مجوز شروع ساخت شناسانه؛
- هر داده‌ای که به عنوان ورودی فراهم می‌شود؛ و
- یک مهر زمان باشد.

یک مولد شناسانه مرجع مجاز است پیکربندی شود تا شناسانه‌های مرجع را که برای کاربرد خارج از دامنه منشا در نظر گرفته شده، ایجاد کند. در این مورد:

- مقدار شناسانه مرجع باید به صورتی امکان‌پذیر شود که پیوستگی آن را تضمین کند،
- اگر مقدار شناسانه مرجع به شکل الکترونیک موجود باشد، دسترسی به آن باید واپایش شود تا از حریم خصوصی اصل محافظت کند،
- بهتر است مراقبت شود تا منحصر به فرد بودن این شناسانه مرجع برای هر هستار متفاوت در دامنه‌های بیرونی تضمین شود که در آن‌ها نیز شناسانه مرجع به کار برده می‌شود،
- اطلاعات برای بازبینی سطح اطمینان جهت منحصر به فرد بودن مقدار بهتر است موجود باشد، و
- بهتر است نسبت به محدودیت های ممکن، (برای مثال قانونی و مقرراتی) و معایب اعمال به برخی انواع شناسانه مرجع خارج از دامنه‌شان، مانند برخی مراجع دولتی یا مراجع مربوط به حریم خصوصی، مراقب بود.

۶-۳-۵ انطباق و کیفیت اطلاعات هویت

طراحی مستند یک سامانه مدیریت هویت، باید مولفه‌های کارکردی برای کیفیت و انطباق را مشخص سازد که اطلاعات هویت به دست آمده را بررسی می‌کند که با واپایش‌های کافی پردازش شده باشد و مطابق باشد با:

- خط‌مشی‌های اجرا شدنی،
- رویه‌ها و سازماندهی برای به روز نگه داشتن اطلاعات در گذر زمان،
- رویه‌هایی برای سروکار داشتن با تشخیص هویت مثبت اشتباه،
- رویه‌هایی برای سروکار داشتن با تشخیص هویت منفی اشتباه،
- الزامات کسب و کار، و
- مقررات جهانی، منطقه ای و محلی.

۶-۳-۶ بایگانی کردن اطلاعات

طراحی مستند یک سامانه مدیریت هویت، باید خط‌مشی‌هایی را برای مشخص کردن شرایط و رویه‌ها جهت بایگانی کردن اطلاعات هویت فراهم آورد.

اطلاعات هویت بایگانی شده باید ناشناس باشد، چه از طریق ناشناس سازی فعال یا حذف اطلاعات هویت.

۶-۳-۷ پایان دادن و حذف اطلاعات هویت

طراحی مستند یک سامانه مدیریت هویت باید خط‌مشی‌هایی را فراهم کند برای مشخص کردن شرایط و رویه‌هایی جهت بنیاد نهادن حذف اطلاعات هویت توسط:

- اصل یا یک هستار مجاز جهت اقدام از جانب مدیر،
- سامانه، بعد از انقضای دوره نگهداری یک هویت بایگانی شده، یا
- نهاد مدیریت هویت.

اطلاعات هویت حذف شده باید جهت پشتیبانی از درخواست و ممیزی ثبت شود. این رکورد باید آماده‌ساز و دلیل حذف، و هر فراداده دیگری که توسط خط‌مشی‌های حذف مشخص شده است را تعیین کند. رکورد اطلاعات هویت حذف شده باید مدتی بعد از ایجاد، همانگونه حذف گردد که در خط‌مشی حذف مشخص شده است.

یاداوری- یک پیاده‌سازی نوعی حذف شامل بایگانی کردن اطلاعات هویت برای یک دوره گذار تا طی شدن زمان مورد نیاز برای تکمیل حذف، می‌باشد.

حذف تمام اطلاعات هویت برای یک اصل باید هر اطلاعاتی را که می‌تواند در ادامه موجب شناسایی اصل شود و تحت واپایش نهاد مدیریت هویت می‌باشد برای مثال درون فایل های ثبتی، پشتیبان گیری‌ها و دنباله‌های ممیزی می‌باشند که ممکن است خارج از سایت ذخیره شده باشند، محو کند. حذف بهتر است کامل، در نظر گرفته نشود مگر اینکه چنین اطلاعات اضافی پاک شده باشند.

در یک مدل متمرکز، اگر هر سامانه مدیریت هویت آماده سازی خودکار انجام دهد، هر بخش مورد اعتماد که اطلاعات هویت از قبل دریافت شده را ذخیره کرده باشد باید نسبت به حذف اطلاعات مطلع گردد. به محض دریافت اطلاع رسانی حذف اطلاعات، بخش مورد اعتماد باید هر اطلاعاتی را از بین ببرد که اصل را با دامنه اطلاع دهنده ربط می‌دهد. در این حالت، انتقال چرخه حیات حذف بهتر است کامل در نظر گرفته نشود مگر اینکه تاییدیه مبنی بر حذف ارتباط‌ها دریافت شده باشد.

یاداوری- یک بخش مورد اعتماد که از حذف اطلاعات مطلع شده است مجاز است که اطلاعات هویت برای اصلی که نگه داری می‌کند که وابسته به ارتباط اصل با دامنه اطلاع دهنده نباشد، حفظ کند.

۶-۴ الزامات غیرکارکردی

الزامات غیرکارکردی جنبه‌هایی از یک سامانه مدیریت هویت را مشخص می‌سازند که مستقیما از دید فیزیکی، منطقی یا کارکردی پیروی نمی‌کنند. جزئیات الزامات غیرکارکردی فراتر از هدف و دامنه کاربرد این استاندارد می‌باشد.

هرچند برآورده کردن یک یا بیشتر از الزامات غیرکارکردی زیر برای بیشتر سامانه‌های مدیریت هویت به کار گرفته شده، ضروری می‌باشد:

- دسترس‌پذیری؛
- واپایش‌های یکپارچگی؛
- عملکرد؛

- تضمین حریم خصوصی؛
- قابلیت استفاده از دسترسی؛
- متعهد بودن و ارائه آن در سطح فنی؛
- واپایش‌های مرجع زمانی؛
- محدودیت‌های انطباق از جنبه‌های سازمانی، مقرراتی (جهانی، منطقه‌ای و محلی) و قراردادی (به پیوست الف مراجعه کنید)

طراحی مستند یک سامانه مدیریت هویت باید مشخص سازد که چگونه پیاده‌سازی‌اش با استاندارد ISO/IEC 27002 مطابقت دارد تا قابلیت دسترسی و الزامات زمان واکنش بخش‌های مورد اعتماد، محافظت از یکپارچگی داده را برآورده سازد و جایی که نیاز باشد واپایش‌هایی را پیاده‌سازی کند تا تضمین کند که محرمانه بودن اطلاعات حساس حفظ می‌شود و الزامات حریم خصوصی برآورده می‌شود.

پیوست الف
(اطلاعاتی)
جنبه‌های مقرراتی و قانونی

یک سامانه مدیریت هویت نیاز دارد که با الزامات قانونی تطابق داشته باشد. به صورت کلی چنین الزاماتی خواستار این هستند که چنین سامانه‌ای با مقاصد مجاز و اعلام شده به کار برده شود. برای مثال قوانین و مقررات مربوط به اداره شرکت ها، مخابرات، بهداشت و درمان و پولشویی شامل الزاماتی هستند که بر روی مدیریت هویت تاثیر می گذارند.

یک نهاد مدیریت هویت بهتر است قوانین و مقرراتی که ممکن است بر الزامات سامانه مدیریت هویت‌اش تاثیر بگذارد، را به روز نگاه دارد.

الزامات قانونی و مقرراتی که باید در نظر گرفته شود شامل:

- شناسایی هستاری که مسئول مشخص کردن الزامات مدیریت هویت می‌باشد؛
- ویژگی‌های اطلاعات هویت و خط‌مشی‌های رسیدگی کننده به اطلاعات؛
- ویژگی‌های هدفی که برای آن اطلاعات هویت مجازند به کار برده شوند؛
- دامنه(های) کارکردی خارج از دامنه منشا که در آن اطلاعات هویت مشخص ممکن است به کار برده شوند؛
- مدیریت چرخه حیات یک هویت (به بند ۶-۳ مراجعه کنید)؛
- شناسایی نهاد مدیریت هویت دامنه منشا که در آن اطلاعات هویت ایجاد شده است (به بند ۵-۳-۲-۷ مراجعه کنید)؛
- الزامات اثبات هویت (شامل محافظت از اطلاعات جمع آوری شده در فرایند اثبات هویت) و گزارش الزامات در مواردی که اثبات هویت، اطلاعات هویت نامعتبر را کشف کند؛
- شناسایی هستار مسئول مراقبت از محتوای هر ثبات هویت؛
- جنبه‌های امنیتی اعتبارنامه‌های فیزیکی، به خصوص آن‌هایی که برای کاربرد در تشخیص هویت در نظر گرفته شده است.

پیوست ب
(اطلاعاتی)
مدل مورد کاربری

این پیوست مدلی با جزئیات بیشتر با نمونه تحلیل شده از عناصر معماری مرجع ارائه می‌دهد. این نمونه تحلیل شده شامل کنشگرانی می‌شود که در جدول ب-۱ توضیح داده شده است.

جدول ب-۱- کنشگرهای حاضر در نمودار مورد کاربری

عامل	جزئیات
عملگر سامانه مدیریت هویت	هستار مسئول اجرای خط‌مشی‌های مدیریت هویت، مدیریت داده پیکربندی در کل سامانه و فراهم کردن پشتیبانی عملیاتی روز به روز می‌باشد.
فراهم کننده اعلان هویت	فراهم کننده اعلان هویت مسئولیت تایید کردن احراز هویت و/یا خصیصه‌ها را دارد. این یک تایید کننده را به کار می‌اندازد و مجاز است که به ثبات هویت دسترسی داشته باشد. یک طرف مورد اعتماد ممکن است احراز هویت و/یا آماده‌سازی خصیصه را به یک فراهم‌کننده اعلان هویت محول کند فراهم‌کننده اعلان هویت مطالبه‌کننده را اصالت‌سنجی می‌کند و/یا داده را از ثبات هویت برای اعلان اطلاعات هویت می‌گیرد. در نتیجه یک سامانه مدیریت هویت می تواند خدمات احراز هویت، خدمات خصیصه و یا هر دو را برای یک طرف مورد اعتماد فراهم سازد.
نهاد هویت	یک کنشگر که می‌تواند اظهارات قابل اثبات را در مورد اعتبار و یا درست بودن یک یا بیشتر مقادیر خصیصه در یک هویت ایجاد کند. یک نهاد اطلاعات هویت معمولا در ارتباط با دامنه می باشد، برای مثال دامنه منشا که در آن خصیصه‌ها که نهاد هویت می‌تواند بر روی آنها اعلان داشته باشد اهمیت ویژه‌ای دارند. کنشگر، یک نهاد اطلاعات هویت و یک فراهم کننده خدمت اعتبارنامه را ترکیب می‌کند.
فراهم کننده خدمت اعتبارنامه (CSP)	کنشگر قابل اعتماد که اعتبارنامه‌ها را صادر و/یا مدیریت می‌کند. در این بستر نقش CSP محدود به صدور اعتبارنامه‌ها برای استفاده در احراز هویت هستار می‌باشد.

هدف توصیف موارد کاربری، ارائه قرارداد بین یک کنشگر و سامانه‌ای برای شناسایی برهم‌کنش‌های در دسترس کنشگر می‌باشد. کنشگر یک برهم‌کنش با سامانه را برای حصول یک هدف خاص شروع می‌کند و هر مورد کاربری، رفتار سامانه را در پاسخ به آن توضیح می‌دهد.

یک مورد کاربری همچنین می‌تواند توسط طبقات، نمودارهای پیاپی و دیگر نوشتارهای رسمی توضیح داده شود که اجازه تعیین جزییات بیشتر برهم‌کنش با سامانه را تعیین می‌کند. مدل مورد کاربری که در این پیوست آمده است، یک مدل سطح بالاست که تنها شامل نمودارهای تکمیل شده با توضیحات رسمی برای مورد کاربری «اصالت سنجی» هویت است.

توضیح مورد کاربری می‌تواند طوری بازبینی شود که جزییات بیشتری را شامل شود، که معمولا در چندین سطح انتزاعی ارائه می‌شود. توضیح مورد کاربری سطح پایینتر انتزاعی ممکن است کنشگرهای بیشتری برای زیرسامانه‌ها معرفی کند مانند کنشگرهایی که در کنار مرزهای سامانه هستند.

مورد کاربری شکل ب-۱، دو مورد کاربری اصلی در سامانه مدیریت هویت مشخص می‌کند:

الف- دسترسی به یک منبع محافظت شده؛

ب- تحویل پیامی که بهتر است اصالت سنجی شود.

مدل مورد کاربری جدول ب-۲ کنشگران داخلی را از سامانه مدیریت هویت در جدول ب-۱ توضیح می‌دهد تا مورد کاربری را با جزییات بیشتری توضیح دهد.

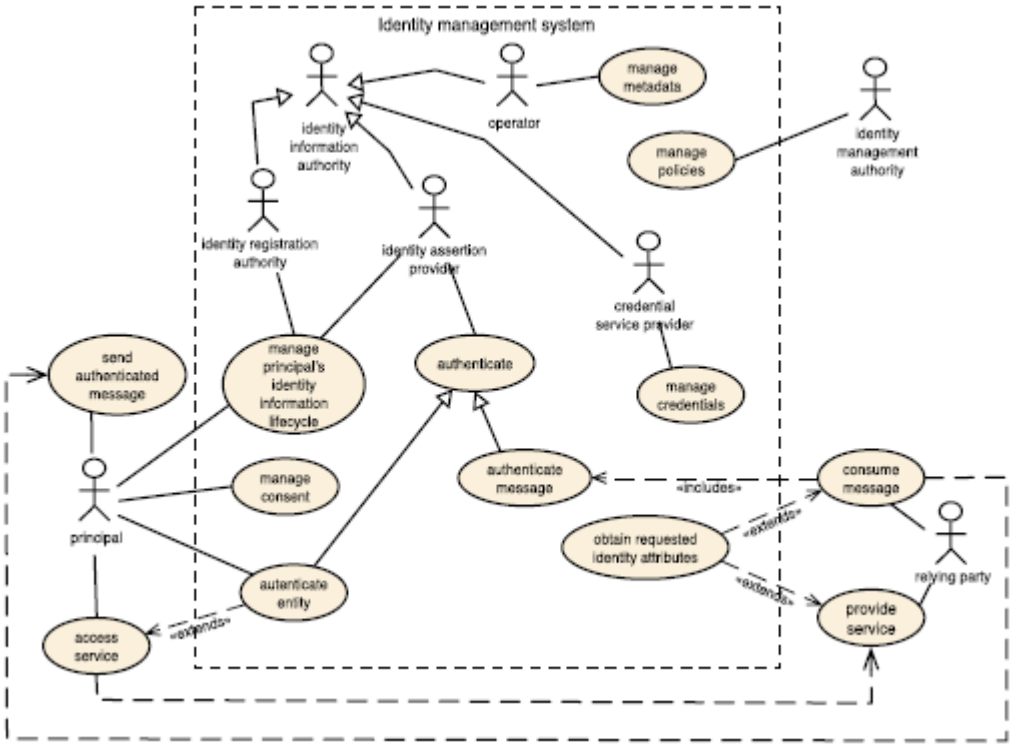
جدول ب-۲- تعریف خلاصه ای از مورد کاربری برای سامانه مدیریت هویت

مورد کاربری	توصیحات
دسترسی به خدمت	یک مدیر خواستار دسترسی به منبعی هست که بعد از اصالت‌سنجی هستار قابل دسترسی می‌باشد.
احراز هویت هستار	فعالیت اصالت‌سنجی یک مدیر در یک تراکنش برخط
احراز هویت پیام	فعالیت اصالت‌سنجی فرستنده یک پیام
مصرف کردن پیام	دریافت یک پیام و اصالت‌سنجی فرستنده آن
مدیریت رضایت	اعطا مجوز، بازبینی و لغو توافقبرای استفاده مدیریت هویت برای اصالت‌سنجی دسترسی منبع
مدیریت اعتبارنامه	فعالیت‌های مربوط به ایجاد، ابطال و تجدید اعتبارنامه‌ها، اغلب شامل مدیریت اعتبارنامه‌های سخت‌افزاری می‌شود
مدیریت فراداده	مدیریت پیکربندی دادهٔ تامین‌کنندگان هویت و طرف‌های مورد اعتماد به یک روش قابل خواندن توسط ماشین، اعتماد و همکاری بینابین. که شامل پارامترهای فنی مثل کلیدهای رمزنگاری و نشانی‌دهی می‌شود
مدیریت چرخه عمر مدیر	نام‌نویسی، به‌روزرسانی، بایگانی و پاک‌سازی مدیریت هویت
مدیریت خط‌مشی	تعیین خط‌مشی و رویه‌هایی برای اجرا و نگهداری سامانه مدیریت هویت
اخذ خصیصه‌های درخواست‌شده	اخذ خصیصه‌ها برای یک مدیر اصالت‌سنجی شده و مورد نیاز به منظور دسترسی به خدمت
فراهم کردن خدمت	طرف مورد اعتماد منابعی که نیاز به دسترسی مجازشناسی دارد فراهم می‌کند
تدارک خدمت	ارائه اطلاعات هویت درباره مدیرها به یک طرف مورد اعتماد
ارسال پیام اصالت‌سنجی	ارسال یک درخواست با خدمت وب، سند و علاقه. هیچ پاسخ مستقیمی در رویه یا تراکنش وجود ندارد. مثال‌ها: الف- یک شرکت یک سند امضا شده را با ترازنامه به بانک برای نگهداری بالاتر از محدوده اعتبار ارائه می‌دهد، روش به کار برده شده، بارگزاری پوشه به صورت کاربر ناشناس است. موارد کسب و کار مشابه دیگر شهروندانی هستند که از بعضی دولت‌هابا یک فرم امضا شده الکترونیکی درخواست ارائه می‌دهند. ب- یک فرستنده پیام غیرهمزمان امضا شده تحویل می‌دهد.

نوشتار مورد کاربری UML می‌تواند به عنوان جدول محتویات نموداری برای مورد کاربری تنظیم تلقی شود. عناصرش موارد زیر هستند:

- بیضی: یک مورد کاربری خاص
-اشکال ثابت: یک کنشگر (به معنی یک نقش نه یک شخص)
- خط بین کنشگر و مورد کاربری خاص: استفاده از رابطه
- جعبه مربعی با خط‌های فاصله دار: مرزهای سامانه
- پیکان شمول. یک مورد کاربری شامل رفتار طرفی است که به آن اشاره دارد مثل فراخوانی یک زیررویه توسط برنامه

- پیکان توسیع. مورد کاربری اشاره شده به آن، چگونه و چه زمان رفتار از پیکان دیگر شامل می‌شود را تعریف می‌کند.
- پیکان با یک مثلث از یک عنصر خاص‌تر (کنشگر، مورد کاربری) به مورد عمومی‌تر اشاره دارد.
- خطوط فاصله دار با یک پیکان یک وابستگی عمومی مورد کاربری است.



شکل ب-۱- نمودار مورد کاربری نمونه برای یک سامانه مدیریت هویت

نام مورد کاربری: اصالت سنجی هستار

کنشگر اصلی: مدیر

دامنه کاربرد: خلاصه

ذی‌نفعان با منافع:

مدیر- به منظور تامین داده تشخیص هویت به خدمت، تنها اگر خدمت حریم خصوصی‌اش را محافظت کند- تا قادر به استفاده از خدمت بدون ثبت نام و تشخیص هویت دست و پاگیر باشد؛

طرف مورد اعتماد- تامین یک آستانه پایین برای مدیران برای استفاده از خدمت برای بار اول و مشاهدات زیر- اخذ اعتماد کافی در حق مدیر برای استفاده از خدمت- مطابق با قوانین و مقررات؛

نهاد مدیریت هویت- نظارت بر انطباق با رویه‌ها و قوانین سامانه.

پیش شرایط:

کنشگر در سامانه ثبت نام کرده است و کاملا یک مدیر است.

تضمین‌های موفقیت: مدیر تشخیص هویت می‌شود و اعلان هویت توسط طرف مورد اعتماد استفاده می‌شود.

چکانه: مدیر تلاش می‌کند تا به خدمت در طرف مورد اعتماد و هنوز تشخیص هویت نشده، دسترسی داشته باشد.

فرانامه موفقیت اصلی:

پیوست پ
(اطلاعاتی)
مدل ترکیبی

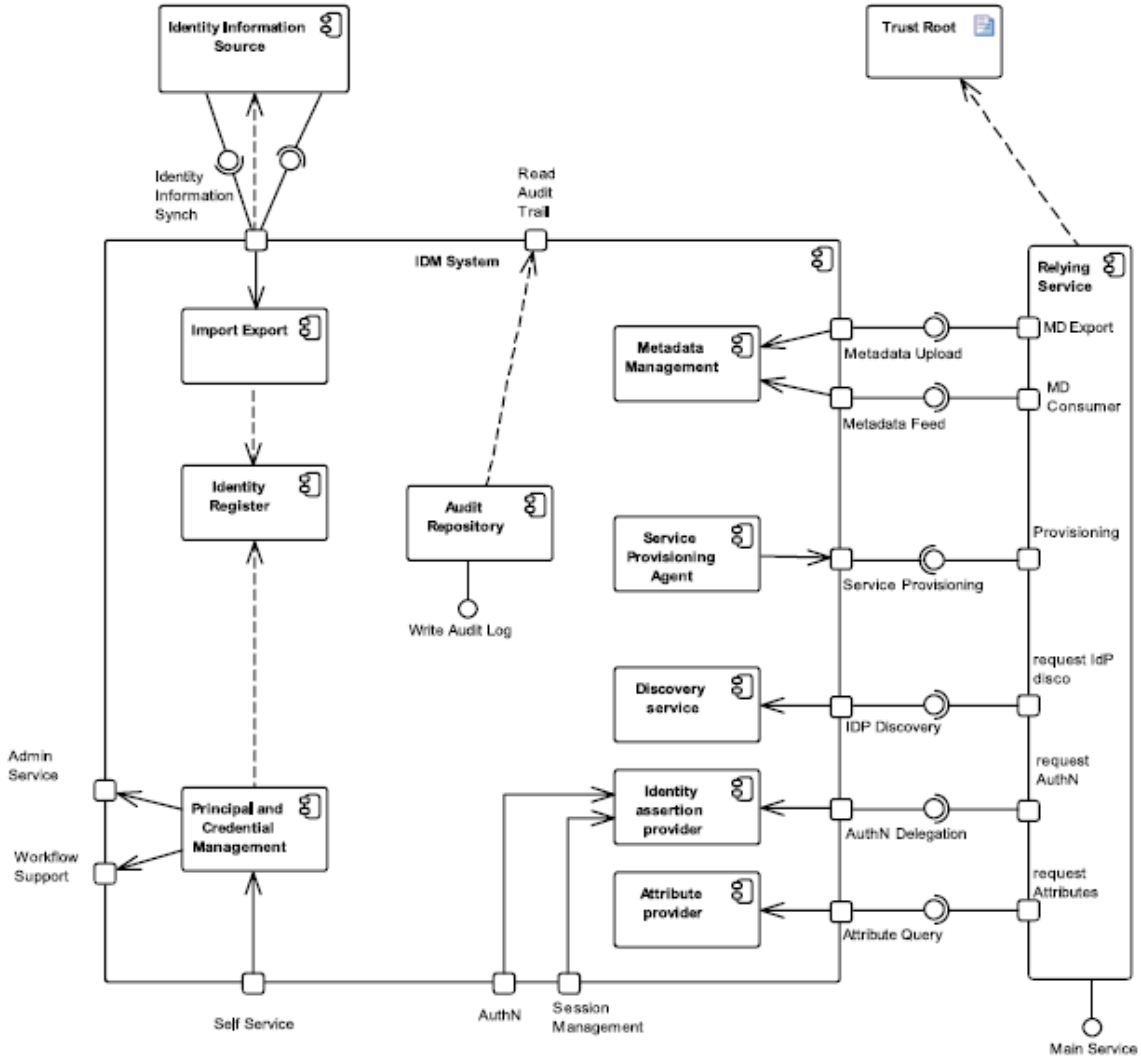
پ-۱ مدل

این پیوست مثال ارائه شده در پیوست ب را به شکل پ-۱، مولفه‌های کارکردی یک سامانه مدیریت هویت، گسترش می‌دهد. مولفه‌های ارائه شده برای پیاده سازی موارد کاربری تعمیم داده شده در پیوست د، کافی هستند. شکل‌ها UML را به کار می‌برند و بند پ-۲ طرحی را برای نمادهای ارائه شده در نمودار ارائه می‌کند.

این نمودار مولفه، قطعه‌های سامانه همانطور نشان می‌دهد که در زمان اجرا سازماندهی می‌شوند. که شامل وابستگی‌ها و واسط‌ها می‌شود. جدول پ-۱ مولفه‌های نشان داده شده را خلاصه می‌کند.

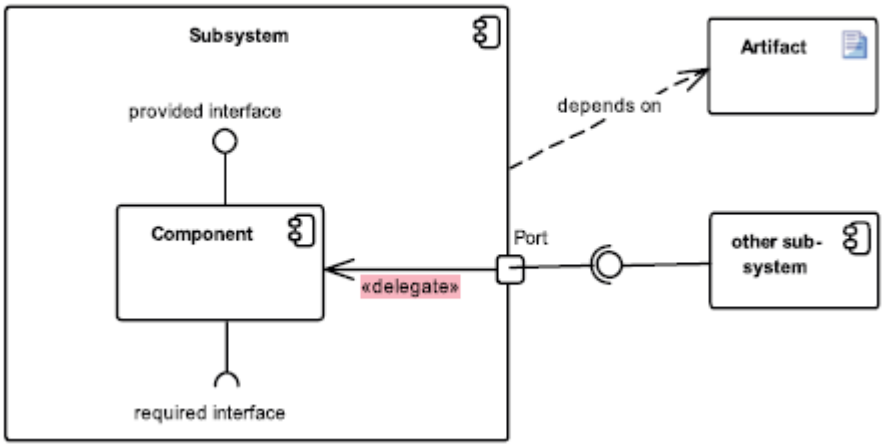
جدول پ-۱- واژه‌شناسی نمودار مولفه UML

نام	توضیحات
مدیریت اعتبارنامه و مدیر	زیرسامانه‌ای برای رسیدگی به چرخه حیات مدیریت اعتبارنامه و مدیر
مدیریت فراداده	این مولفه فراداده را ذخیره می‌کند و امکاناتی را برای نگهداری و انتشار آن فراهم می‌سازد. و این نیاز به سطح امنیتی همتراز یا بهتر از سامانه‌ای دارد که فراداده را بکار می‌برد.
عامل آماده سازی خدمت	این مولفه اطلاعات هویت را به یک خدمت برای مثال بخش متکی می فرستد.
خدمت مورد اعتماد	یک خدمت عملیاتی شده که تحت واپایش یک طرف قابل اعتماد فراهم شده است. فراهم اوردن دسترسی به خدمت‌ها اغلب هدف اولیه یک سامانه مدیریت هویت می‌باشد. بنابراین ارزشی در مشخص کردن واسط‌ها و ارتباط دادن آن‌ها در ابتدای فعالیت‌های خرید و توسعه برای خدمت‌های مورداعتماد وجود دارد.
وارد کردن / صادر کردن	این مولفه می‌تواند با متن‌های ویژه منبع، نرم افزار راهنمافرا یا واسط‌های دیگر پیاده سازی شود
صندوق ممیزی	این مولفه سوابقی از رویدادهای عملیاتی برای ممیزی ذخیره می‌کند. این مولفه دسترسی به فهرست ثبت شده ممیزی را به شکلی واپایش شده فراهم می دارد.
سامانه مدیریت هویت	این مولفه زیرساخت فنی یک سامانه مدیریت هویت را به صورت کلی ارائه می دهد.
ثبات هویت	مخزنی از اطلاعات هویت تلفیق شده برای یک دامنه. می‌تواند به صورت ذخیره سازی فیزیکی مثل یک راهنما، پایگاه داده یا کارت هوشمند یا به شکل مجازی به مانند یک راهنما مجازی باشد.
ریشه اعتماد	معمولا امنیت رمزنگاری برای اطلاعاتی که در یک سامانه مدیریت هویت بکار گرفته می شود از پروتکل‌های کلید عمومی براساس گواهی‌های کلید عمومی استفاده شده توسط سامانه استفاده می‌کنند.



شکل پ-۱- مولفه‌های کارکردی در یک سامانه مدیریت هویت

پ-۲ طرح UML



شکل پ-۲- عناصر پویانمایی در یک نمودار مولفه UML

جدول پ-۲- واژه شناسی نمودار مولفه UML

نماد	توضیحات
تصنعی	مصنوع هر بخش فیزیکی از اطلاعات به کار برده شده یا تولید شده توسط یک سامانه می‌باشد.
مولفه	هر مولفه، بخش پیمانه‌ای از یک سامانه را ارائه می‌دهد که محتوایش را پوشینه دار می‌کند و آشکارسازی اش با محیط اش قابل جابه جایی می‌باشد.
درگاه	درگاه ها بر هم کنش بین یک مولفه و محیط اش را تعریف می‌کنند. می‌تواند چندین واسط برای واپایش این بر هم کنش داشته باشد. درگاه‌ها بر روی مرز یک مولفه پدیدار می‌شوند.
واسط فراهم شده	یک واسط تخصیص رفتاری (قراردادی) است که پیاده ساز ها بر برآورده ساختنش توافق می‌کنند. یک مولفه، رفتار را با بکارگیری واسط فراهم شده پیاده سازی می‌کند.
واسط مورد نیاز	یک واسط ویژگی رفتاری (یا قراردادی) است که پیاده ساز ها بر برآورده ساختنش توافق می کنند. یک مولفه بر چنین رفتاری با بکارگیری واسط مورد نیاز اتکا می‌کند.
زیرسامانه	یک زیرسامانه به عنوان مولفه ای از یک مجموعه بزرگتر از سامانه ها نمایش داده می شود.

پیوست ت
(اطلاعاتی)
مدل پردازش کسب و کار

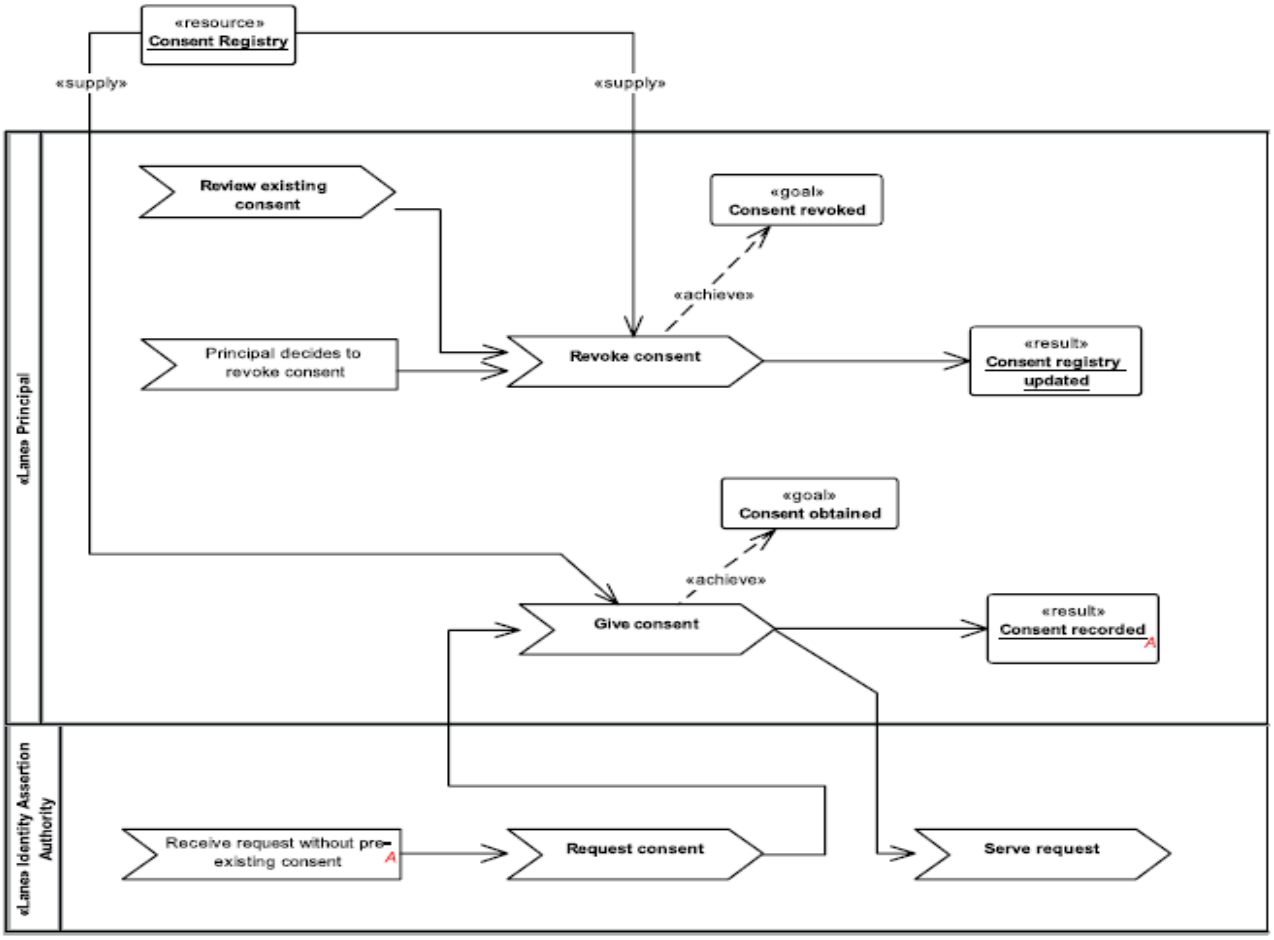
ت-۱ کلیات

این پیوست نمونه ارایه شده در پیوست ب را با یک توصیف نمونه‌ای از پردازش کسب و کار گسترش می‌دهد. یک پردازش کسب و کار مجموعه ای از فعالیت ها یا وظایف ساختاریافته و مرتبط می باشد که یک خدمت یا محصول خاص را (یک هدف خاص را مد نظر دارند) برای یک مشتری یا گروه مشتریان ویژه، تولید میکنند.

در یک طراحی مستند، یک مدل پردازش کسب و کار، توصیفات جریان های واپایش و اطلاعات، رخدادها، اهداف و خروجی هایی برای حمایت از توصیفات مفصل مورد کاربری، ارائه می دهد.

این پیوست، نمودار مدل کسب و کار را با به کار بردن UML تعمیم یافته شده ارائه می‌دهد.

ت-۲ مدیریت رضایت

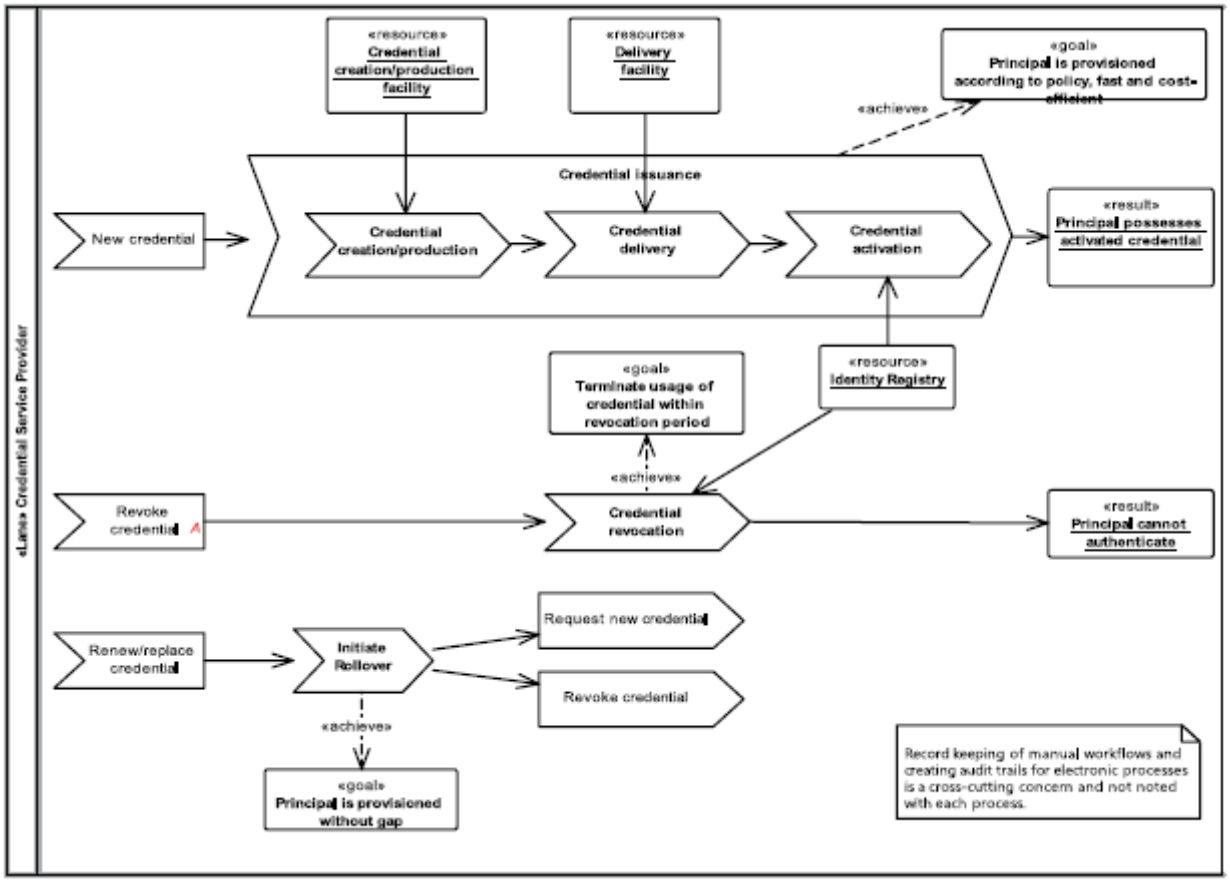


شکل ت-۱- نمودار پردازش برای مدیریت رضایت

جدول ت-۱- توصیف عنصر پردازش کسب و کار مدیریت رضایت

پردازش	جزییات
قطع توافق	در موردی که توافقصریح نیست، مدیر باید یک گزینه قطع توافقداده شده قبلی داشته باشد
مرور توافقموجود	کاربران نیاز دارند تا توانایی بازپس گیری توافقاز قبل داده شده را داشته باشند
اعطا توافق	توافقنیاز است مطابق خط مشی حفظ حریم خصوصی اعطا شود، برای مثال: به طور صریح، به ازائ هر تراکنش کسب و کار برای داده های سلامت؛ به طور صریح، به ازائ هر طرف مورد اعتماد برای همه تراکنش های آتی برای دسترسی به خدمت کتابخانه ای برای یک دانش اموز؛ به طور ضمنی برای دسترسی خدمت ها به یک کاربرد وب به منظور انجام دادن وظایف رسمی برای یک کارمند دولت.
رخداد	**جزییات**
مدیر تصمصم می گیرد که توافقرا قطع کند	این رخداد به طور ضمنی بیان میکند که تسهیلاتی برای مدیر برای قطع رضایت، و برخط بودن از طریق مرکز تماس یا کانال های ارتباطی دیگر فراهم شده است.
دریافت درخواست بدون توافقاز قبل موجود	درخواست اصالت سنجی یا پرسمان خصیصه بدون توافقاز قبل داده شده. توافققبلی وجود ندارد، منقضی شده است، یا برای تراکنش کاربرد ندارد.
هدف	**جزییات**
توافققطع می شود	توافققطع می شود. خط مشی باید تصمیم گرفته شود که به عنوان انکار شده یا حذف شده تلقی شود. در مورد حذف شده، از مدیر باید درخواست توافقدوباره شود.
توافقاخذ می شود	به منظور اشتراک گذاشتن اطلاعات با طرف مورد اعتماد، واپایشگر توافقرا به روش مناسبی اخذ می کند و مستند می کند (به ازائ هر تراکنش، به ازائ هر ارتباط)
منبع	**جزییات**
ثبات رضایت	ثبات رضایت، توافقکاربر را رد یک قالب قابل خواندن توسط ماشین ذخیره میکند. اسناد ساختار نیافته برای اهداف ممیزی مجاز است در نظر گرفته شوند. ثبات توافقمجاز است باارائه کننده اطلاعات هویت یا کنشگرهای دیگر، گروه بندی شود
نتیجه	**جزییات**
ثبات توافقبه روزرسانی میشود	
توافقثبت شود	تصمیم توافقثبت می شود. اگر توافقمثبت باشد، اصالت سنجی و/یا درخواست خصیصه مجاز است.

ت-۳ مدیریت چرخه عمر اعتبارنامه



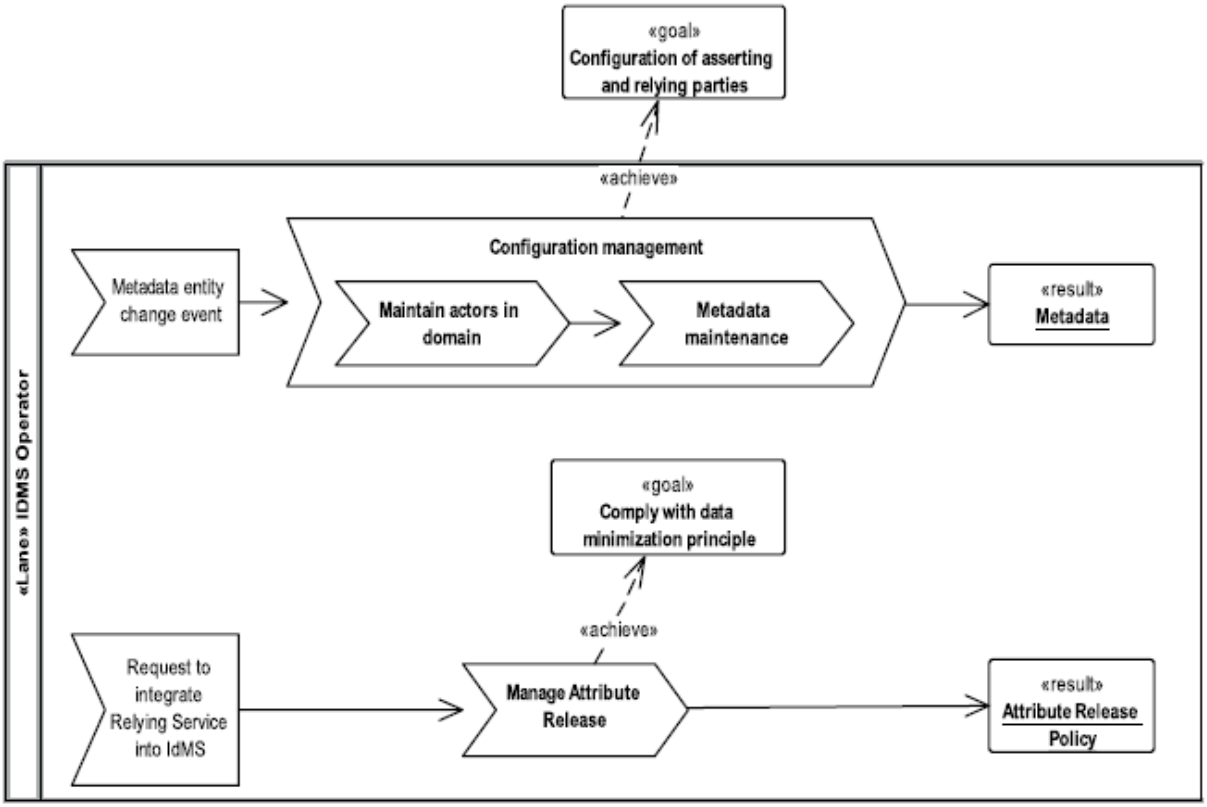
شکل ت-۲- نمودار پردازش برای مدیریت چرخه عمر اعتبارنامه

یاداوری- تعلیق یک اعتبارنامه در این نمودار به علت کم کردن پیچیدگی پشتیبانی نشده است، و در یک معماری ویژه جایی که نیاز است، می تواند اضافه شود.

جدول ت-۲- توصیف عنصر پردازش کسب و کار مدیریت چرخه عمر اعتبارنامه

پردازش	جزییات
جایگزینی اعتبارنامه ها	در موردی که توافقصریح نیست، مدیر باید یک گزینه قطع توافقداده شده قبلی داشته باشد
ابطال اعتبارنامه ها	به روز رسانی ثبات هویت به منظور نشان دادن وضعیت ابطال. پردازش مجاز است همچنین مجموعه ای از اعتبارنامه های فیزیکی مثل نشان OTP، را راه اندازی کند.
پایه گذاری بازگشت نو	ایجاد یک اعتبارنامه جدید و اطمینان یافتن از اینکه هیچ فاصله ای در ترابری وجود ندارد.
انتشار اعتبارنامه	مجهز کردن یک مدیر به یک اعتبارنامه
تولید/ ایجاد اعتبارنامه	این یک نگهدارنده عمومی برای پردازش ساده (مثلا کلمه رمز) یا پیچیده (مثلا کارت های هوشمند، بیومتریک) که یک اعتبارنامه را تحویل می دهد. هَر چند یک اعتبارنامه تنها داده است، پردازشی که آن را تولید می کند، ممکن است همچنین نیاز داشته باشد که شامل تولید یک نشان فیزیکی باشد که حاوی اعتبارنامه است.
تحویل اعتبارنامه	تحویل اعتبارنامه (و یک نشان فیزیکی اش به عنوان مخزنش) ممکن است انقیاد بین اعتبارنامه و مدیر را ایجاد کند یا اجبار کند.
فعال کردن اعتبارنامه	فعال کردن، پردازشی است که هستار را قادر می سازد به منابعی که اعتبارنامه اش را به کار می برند، دسترسی داشته باشد
رخداد	**جزییات**
تجدید / جایگزینی اعتبارنامه	جایگزینی ها ممکن است دلایل مختلفی داشته باشند، مثلا اعتبارنامه مفقود شده باشد یا غیرکارکردی باشد؛ یک حمله روی اعتبارنامه شناخته شده باشد، یا مشکوک باشد؛ اعتبارنامه منقضی شده باشد (مثلا یک کارت هوشمند قبل از پایان پرونده)
ابطال اعتبارنامه	ابطال اعتبارنامه قدیمی با ملاحظه پردازش انتشار
اعتبارنامه جدید	پردازش دیگری، پردازش انتشار اعتبارنامه را راه اندازی می کند.
درخواست اعتبارنامه جدید	راه اندازی پردازش تا یک اعتبارنامه جدید منتشر کند.
ابطال اعتبارنامه	پردازشی که ابطال یک اعتبارنامه را راه اندازی می کند.
منبع	**جزییات**
تسهیل تولید/ ایجاد اعتبارنامه	بسته به نوع اعتبارنامه، این گزینه می تواند تنها یک مولد کلمه رمز باشد یا میتواند برای مثال تولید کارت هوشمند باشد.
تسهیل تحویل	اعتبارنامه میتواند به صورت الکترونیکی، فیزیکیِ رودررو، یا از طریق خدمت تحویل، تحویل داده شود
ثبات هویت	شامل زیرمجموعه ای از اطلاعات هویت است که برای خدمت های ثبت نام، اصالت سنجی و ابطال، ضروری می باشد.

ت-۴ پیکربندی مدیریت داده



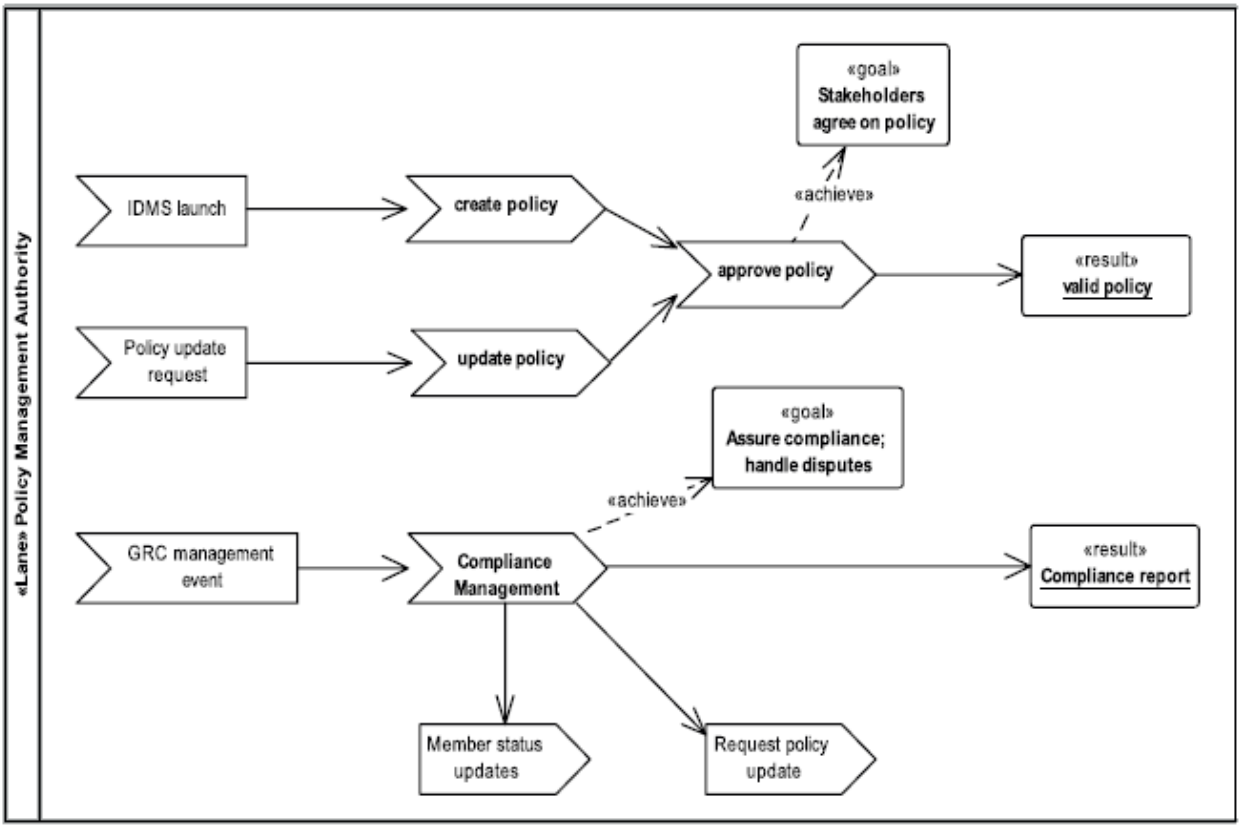
شکل ت-۳- نمودار پردازش برای مدیریت داده پیکربندی

جدول ت-۳- توصیف عنصر پردازش کسب و کار مدیریت پیکربندی

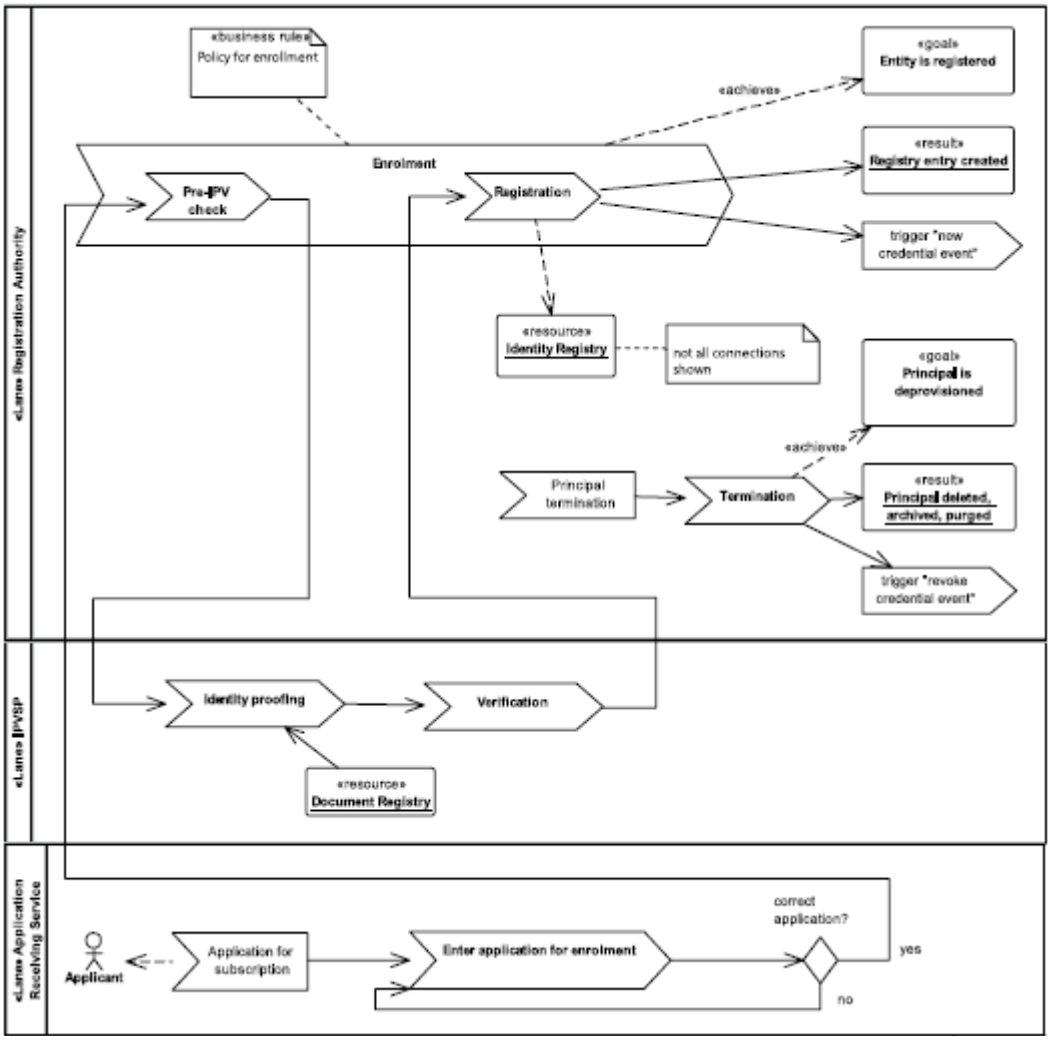
پردازش	جزییات
نگهداری داده پیکربندی	ایجاد پیکربندی یا متا داده ماشین خوانا
نگهداری کنشگرها در دامنه	مدیریت اعضای IMS در سطح کسب و کار و فنی و خصیصه‌هایشان که شامل نظارت و اعتبارسنجی داده خود-مدیر توسط اعضای IMS می‌شود.
مدیریت خصیصه منتشر شده	زمان آماده‌سازی خدمت‌ها، تنها ویژگی‌هایی منتشر می‌شوند که مورد نیاز هستند یا توسط کاربر موافقت می‌شود. برای تحقق این مورد نیاز است تا یک خط مشی انتشار ویژگی زمان اعمال یک خدمت مورد اعتماد به یک IMS تعریف شود.
رخداد	**جزییات**
درخواست یکپارچگی خدمت مورد اعتماد داخل IMS	یک طرف مورد اعتماد درخواست می دهد تا سرویس شان را داخل IMS یکپارچه کند
هدف	**جزییات**
هماهنگ با مدیر کمینه کردن داده	نهاد هویت باید خدمت‌هایش را به طرف‌های مورد اعتماد امین محدود کند، و آزادسازی خصیصه‌هایش را محدود کند به چیزی که مناسب برای خدمت و/یا توسط کاربر توافقداده شده است
پیکربندی اعلان و طرف‌های مورد اعتماد	مدیریت داده فنی درباره اعلان و طرف‌های مورد اعتماد به منظور تسهیل اتصال و ارتباط‌های اعتماد آن‌ها.
نتیجه	**جزییات**
خط مشی انتشار ویژگی	بسته به نوع اعتبارنامه، این گزینه می تواند تنها یک مولد کلمه رمز باشد یا میتواند برای مثال تولید کارت هوشمند باشد.

ت-۵ مدیریت خط مشی

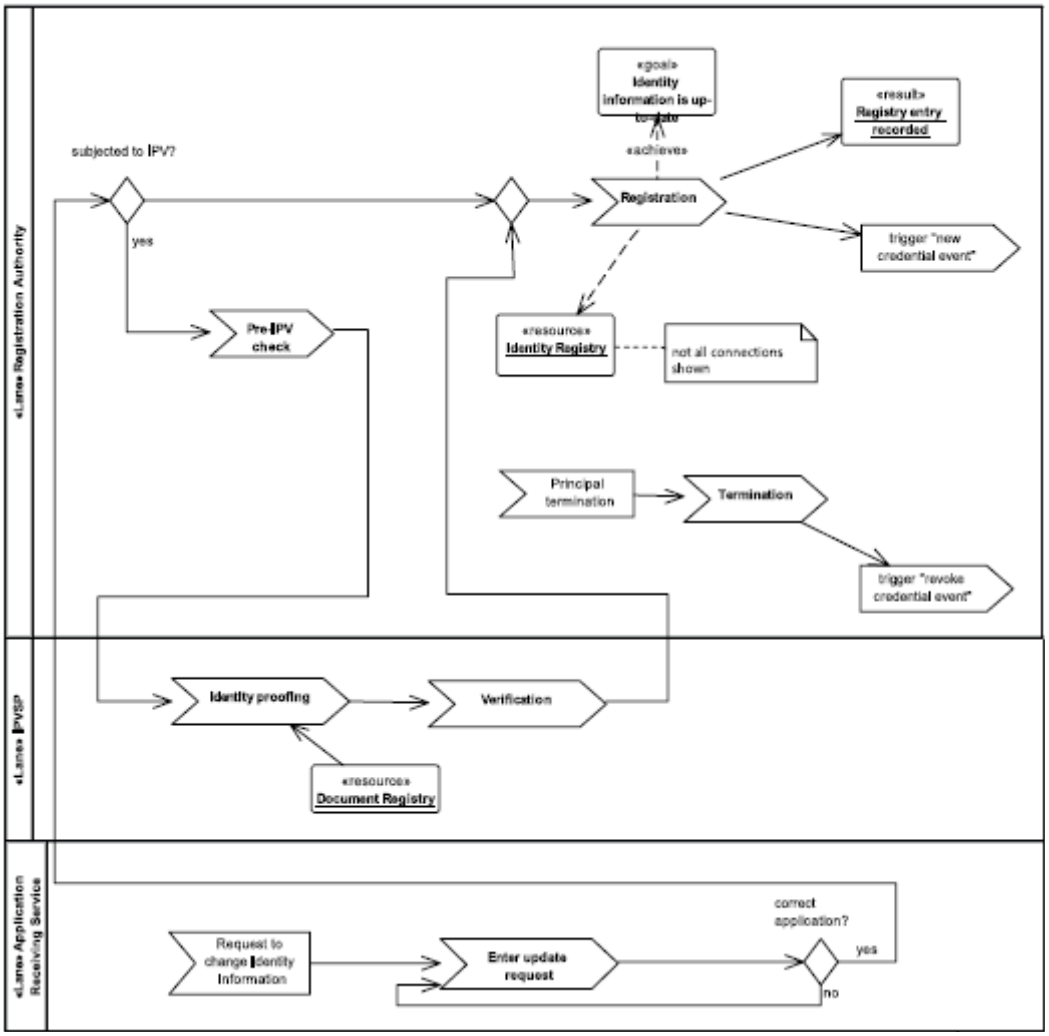
مدیریت خط مشی با ایجاد و نگهداری خط مشی IMS و مدیریت GRC مربوط، مرتبط می‌باشد.



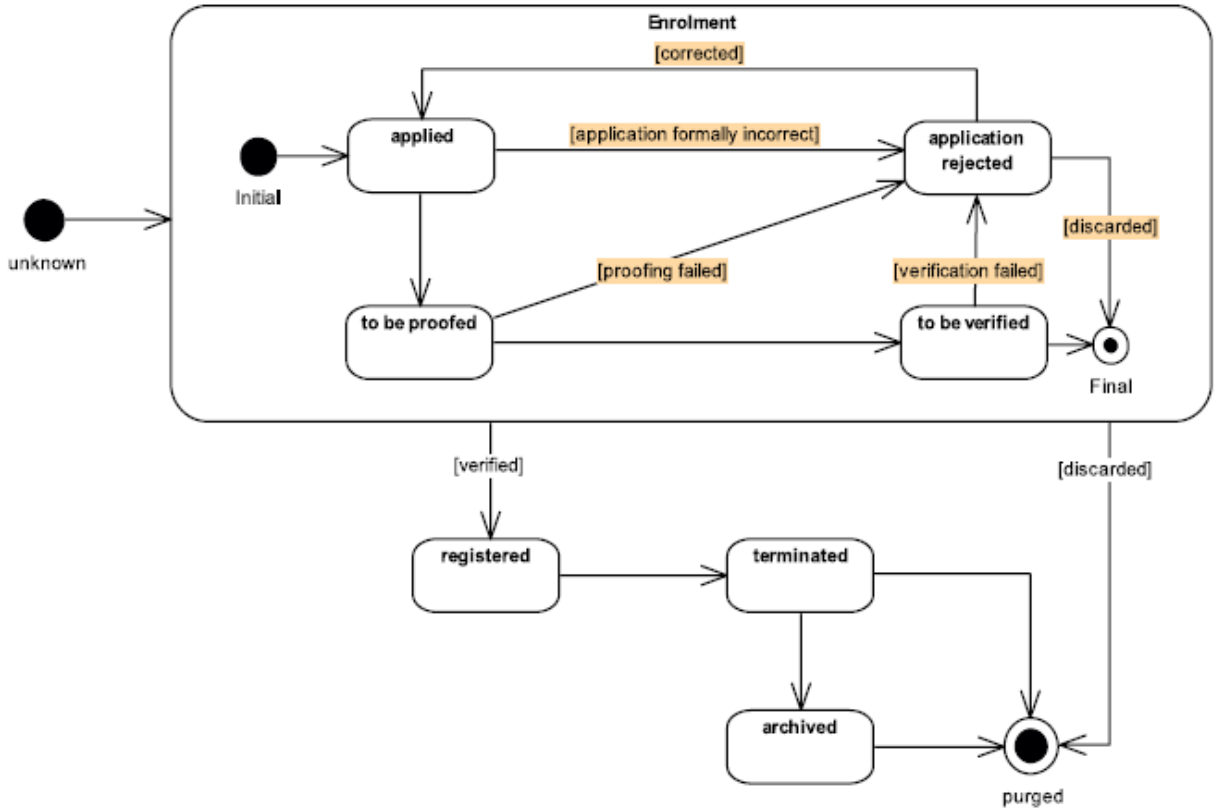
شکل ت-۴- رویه برای مدیریت خط‌مشی‌ها



شکل ت-۵- نمودار رویه برای مدیریت چرخه حیات مدیر



شکل ت-۶- نمودار رویه برای مدیریت هویت



شکل ت-۷- نمودار چرخه حیات برای مدیریت هویت