INSO
17913
1st. Edition
2014

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

استاندارد ملی ایران

۱۷۹۱۳
چاپ اول
۱۳۹۳

فناوری اطلاعات - فنون امنیتی- چارچوب تضمین اصالت‌سنجی هستار

Information Technology – Security techniques – Entity authentication assurance framework

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 تضمین اصالت‌سنجی هستار »

رییس :	**سمت و/ یا نمایندگی**
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات)	کارشناس مسؤول سازمان فناوری اطلاعات ایران
دبیر:	
میر اسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم افزار)	مدیرکل اداره خدمات ارزش افزوده سازمان فناوری اطلاعات
اعضاء : (اسامی به ترتیب حروف الفبا)	
جمیل پناه، ناصر (فوق لیسانس مدیریت)	کارشناس شرکت مخابرات ایران
سجادیه، علیرضا (فوق لیسانس مهندسی کامپیوتر)	مدیرعامل شرکت پردازشگران
سراج زاده، سید هادی (فوق لیسانس فناوری اطلاعات)	پژوهش‌گر دانشگاه شهید بهشتی
سعیدی، عذراء (فوق لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
طی نیا، رضا (فوق لیسانس مدیریت فناوری اطلاعات)	مدیر عامل شرکت کاربرد سیستم
فولادیان، مجید (فوق لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
قسمتی، سیمین (فوق لیسانس مهندسی فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
ناظمی، اسلام (دکترای مهندسی کامپیوتر)	استادیار دانشگاه شهید بهشتی

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد « فناوری اطلاعات - فنون امنیتی - چارچوب تضمین اصالت‌سنجی هستار » که پیش نویس آن در کمیسیون های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده است و در سیصد و چهل و پنجمین اجلاس کمیته ملی استاندارد رایانه و فرآوری داده مورخ ۱۳۹۳/۰۳/۰۵ مورد تصویب قرار گرفته است ، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران ، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می شود .

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

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

ISO/IEC 29115: 2013, Information technology — Security techniques — Entity authentication assurance framework

مقدمه

بسیاری از تراکنش‌های الکترونیکی در درون یا میان سامانه‌های فناوری اطلاعات و ارتباطات(ICT)[1]، الزامات امنیتی دارند که به سطح اعتماد درک شده یا مشخص شده نسبت به هویت[2] هستارهای درگیر وابسته است. چنین الزاماتی ممکن است شامل محافظت از دارایی‌ها و منابع در برابر دسترسی غیرمجاز، که برای آن می‌توان از سازوکارهای کنترل دسترسی استفاده کرد، و/یا اعمال پاسخ‌گویی از طریق نگهداری واقعه‌نگاری‌های ممیزی رویدادهای مرتبط، مانند اهداف حسابداری و اعلام هزینه‌ها[3]، شود.

این استاندارد ملی چارچوبی برای تضمین اصالت‌سنجی هستار فراهم می‌آورد. تضمین در این استاندارد ملی به اعتماد قرار داده شده در تمامی فرآیندها، فعالیت‌های مدیریتی و فناوری‌های استفاده شده جهت استقرار و مدیریت هویت یک هستار برای استفاده در تراکنش‌های اصالت‌سنجی اشاره می‌کند.

مدیریتی و سازمانی	فنی
• استقرار خدمت • انطباق قانونی و قراردادی • شرایط مالی[f] • مدیریت و ممیزی امنیت اطلاعات • مولفه‌های خدمات بیرونی • زیرساخت عملیاتی • سنجش قابلیت‌های عملیاتی	**مرحله نام‌نویسی[a]** • درخواست و شروع • اثبات هویت[b] و درستی‌سنجی اطلاعات هویت[c] • نگهداری رکورد / ثبت[d] • ثبت نام **مرحله مدیریت اعتبارنامه** • ایجاد اعتبارنامه • پیش پردازش اعتبارنامه • صدور اعتبارنامه • فعال‌سازی اعتبارنامه • ذخیره اعتبارنامه • تعلیق، ابطال و انهدام اعتبارنامه[e] • تجدید یا جایگزینی اعتبارنامه • ضبط سوابق **مرحله اصالت‌سنجی هستار** • اصالت‌سنجی • نگهداری رکورد

[a] Enrolment

[b] Identity proofing

1 - Information and communications technology
2 - Identity
3 - Charging

c Identity information verification

d Record keeping / recording

e Credential suspension, revocation, destruction

f Financial provisions

شکل ۱- مرورکلی بر چارچوب تضمین اصالت‌سنجی

این استاندارد ملی، با استفاده از چهار سطح تضمین (LoA)[۱] مشخص، راهنمایی‌هایی در خصوص فناوری‌های کنترل، فرآیندها و فعالیت‌های مدیریتی ارائه می‌کند. همچنین معیارهای تضمینی را جهت کاهش تهدیدهای اصالت‌سنجی توصیف می‌کند که توصیه می‌شود به منظور پیاده‌سازی چهار سطح تضمین به کار گرفته شوند. علاوه بر این برای نگاشت سایر طرح‌های تضمین اصالت‌سنجی به چهار سطح معین شده و همچنین تبادل نتایج تراکنش اصالت‌سنجی، راهنما ارائه می‌کند. در آخر، این استاندارد ملی راهنمای اطلاعاتی در مورد محافظت از اطلاعات قابل شناسایی شخصی (PII)[۲] مرتبط با فرآیند اصالت‌سنجی ارائه می‌کند.

این استاندارد ملی در اصل جهت استفاده توسط ارائه کنندگان خدمات اعتبارنامه (CSP)[۳] و سایر نهادهای ذی‌نفع از خدمات آن‌ها (به عنوان مثال، طرفین اعتماد کننده[۴]، ارزیاب‌ها[۵] و ممیزان[۶] آن خدمات) ارائه شده است. این چارچوب تضمین اصالت‌سنجی (EAAF)[۷] کمینه الزامات فنی، مدیریتی و فرآیندی را برای چهار سطح تضمین مشخص می‌کند تا تعادل بین اعتبارنامه‌های صادر شده توسط CSPهای متفاوت تضمین شود. همچنین ملاحظات مدیریتی و سازمانی اضافی ارائه می‌کند که ممکن است بر تضمین اصالت‌سنجی هستار تاثیر بگذارند، اما معیارهای معینی را برای این ملاحظات پیشنهاد نمی‌کند. این استاندارد ملی می‌تواند برای طرفین اعتماد کننده (RP) و سایرین جهت به دست آوردن درکی از هر سطح تضمین مفید واقع شود. علاوه بر این، می‌توان این استاندارد ملی را در درون یک چارچوب اعتماد[۸] جهت تعریف الزامات فنی برای سطوح تضمین به کار گرفت. چارچوب تضمین اصالت‌سنجی هستار برای موارد کاری مبتنی بر نشست و مستند با فناوری‌های اصالت‌سنجی مختلف پیشنهاد شده است، هر چند به این محدود نمی‌شود. فرانامه‌های[۹] اعتماد مستقیم و از طریق واسطه، در زمینه‌های حقوقی دولتی[۱۰] و دو جانبه، امکان‌پذیر هستند.

1 - Level of Assurance
2 - Personally identifiable information
3 - Credential service provider
4 - Relying party
5 - Assessors
6 - Auditors
7 - Entity authentication assurance framework
8 - Trust framework
9 - Scenario
10 - Federated legal constellations

فناوری اطلاعات – فنون امنیتی – چارچوب تضمین اصالت‌سنجی هستار

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین چارچوبی برای مدیریت تضمین اصالت‌سنجی هستار در یک زمینه مشخص است. به طور خاص، این استاندارد برای موارد زیر کاربرد دارد:

- مشخص‌سازی چهار سطح تضمین اصالت‌سنجی هستار؛
- مشخص‌سازی معیارها و راهنماهایی برای دستیابی به هر یک از چهار سطح تضمین اصالت‌سنجی هستار؛
- ارائه کردن راهنمایی در مورد نگاشت سایر طرح‌های تضمین اصالت‌سنجی با چهار سطح اصالت‌سنجی؛
- ارائه کردن راهنمایی در مورد تبادل نتایج اصالت‌سنجی که بر مبنای چهار سطح اصالت‌سنجی تهیه شده‌اند؛ و
- ارائه کردن راهنمایی در مورد کنترل‌هایی که توصیه می‌شود جهت کمینه کردن تهدیدهای اصالت‌سنجی به کار گرفته شوند.

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 محسوب می شوند.

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

۲-۱ توصیه‌نامه‌ها | استانداردهای بین‌المللی مشابه

هیچ مورد

۲-۲ توصیه‌نامه‌ها | استانداردهای بین‌المللی جفت شده

هیچ مورد

۲-۳ مراجع افزوده

هیچ مورد

۳ اصطلاحات و تعاریف

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

۳-۱

اظهارنامه[1]

بیانیه‌ای که یک هستار اعلام می‌کند بدون اینکه برای اعتبار آن مدرکی ارائه کند.

[ITU-T X.1252]

یادآوری- معنای واژه‌های ادعا[2] و اظهارنامه به طور عمومی با تفاوت اندکی در معنا، مشابه پنداشته می‌شوند. در این استاندارد ملی، اظهارنامه بیانیه‌ای قوی‌تر از ادعا در نظر گرفته می‌شود.

۳-۲

اصالت‌سنجی

ارائه تضمین در مورد هویت یک هستار است.

[ISO/IEC 18014-2][3]

۳-۳

عامل اصالت‌سنجی[4]

قطعه‌ای از اطلاعات و/یا فرآیندی که برای اصالت‌سنجی یا درستی‌سنجی هویت یک هستار استفاده می‌شود.

[ISO/IEC 19790]

یادآوری- عوامل اصالت‌سنجی به چهار دسته تقسیم می‌شوند:

- چیزی که هستار دارد (به عنوان مثال امضا افزاره، گذرنامه، افزاره سخت‌افزاری که دارای اعتبارنامه است، کلید محرمانه)؛
- چیزی که هستار می‌داند (به عنوان مثال اسم رمز[5]، شماره شناسایی شخصی (PIN)[6])؛
- چیزی که هستار از جنس آن است (به عنوان مثال خصوصیت زیست‌سنجی[7])؛
- چیزی که هستار به طور معمول انجام می‌دهد (به عنوان مثال الگو رفتاری).

۳-۴

قرارداد اصالت‌سنجی

دنباله تعریف شده از پیام‌ها بین یک هستار و یک درستی‌سنج[8] که به درستی‌سنج امکان می‌دهد اصالت‌سنجی را روی یک هستار اجرا کند.

---

1 - Assertion
2 - Claim
۳ - استاندارد بین‌المللی ISO/IEC 18014-2:2002 در سال ۱۳۸۷ با شماره ملی ۱۱۳۱۰-۲ منتشر شده است.
4 - Authentication factor
5 - Password
6 - Personal identification number
7 - Biometric characteristic
8 - Verifier

۵-۳
منبع معتبر[1]
مخزنی است که به عنوان یک منبع اطلاعات دقیق و به روز شناخته می‌شود.

۶-۳
ادعا
بیانیه‌ای در مورد مصداق بودن یک موضوع، بدون ارائه اثبات برای آن است.

[ITU-T X.1252]

یادآوری- معنای واژه‌های ادعا و اظهارنامه به طور عمومی با تفاوت اندکی در معنا، مشابه پنداشته می‌شوند. در این استاندارد ملی، یک اظهارنامه بیانیه‌ای قوی‌تر از ادعا در نظر گرفته می‌شود.

۷-۳
زمینه[2]
محیطی با شرایط مرزی تعریف شده که هستارها در آن قرار دارند و با هم تعامل می‌کنند.

[ITU-T X.1252]

۸-۳
اعتبارنامه[3]
مجموعه‌ای از داده که به عنوان اثبات هویت ادعا شده یا اظهار شده و/ یا حقوق مطالبه شده[4] ارائه می‌شود.

یادآوری- برای آشنایی با سایر خصوصیات یک اعتبارنامه به پیوست ب مراجعه شود.

۹-۳
ارائه کننده خدمات اعتبارنامه
شخص مورد اعتمادی است که اعتبارنامه‌ها را صادر و / یا مدیریت می‌کند.

۱۰-۳
هستار
چیزی است که وجود مجزا و قابل تمایز دارد و در یک زمینه قابل شناسایی است.

[ITU-T X.1252]

یادآوری- در این استاندارد ملی، هستار در مورد خاص به عنوان چیزی که ادعا هویت می‌کند نیز به کار گرفته می‌شود.

---

1 - Authoritative Source
2 - Context
3 - Credential
4 - Entitlement

۱۱-۳
تضمین اصالت‌سنجی هستار
درجه اعتماد حاصل شده در فرآیند اصالت‌سنجی است که هستار همانی است که ادعا می‌کند، یا انتظار می‌رود آن باشد.

[ITU-T X.1252]

یادآوری- اعتماد بر مبنای درجه اعتماد در پیوند میان هستار و هویتی که ارائه شده است، بنا می‌شود.

۱۲-۳
شناسانه[1]
یک یا چندین صفت که یک هستار را در یک زمینه خاص به صورت منحصر به فرد توصیف می‌کند.

۱۳-۳
هویت[2]
مجموعه‌ای از صفات مربوط به یک هستار است.

[ISO/IEC 24760]

یادآوری- یک هویت می‌تواند در یک زمینه خاص یک یا چندین شناسانه داشته باشد تا امکان شناخته شدن به صورت منحصر به فرد در آن زمینه فراهم شود.

۱۴-۳
درستی‌سنجی اطلاعات هویت
فرآیند بررسی اطلاعات هویت و اعتبارنامه‌ها با صادر کنندگان، منابع داده یا سایر منابع داخلی و خارجی در ارتباط با اصالت‌سنجی، اعتبار، صحت و انقیاد به هستار است.

۱۵-۳
اثبات هویت
فرآیندی که مرجع ثبت (RA)[3] را از طریق آن اطلاعات کافی برای شناسایی یک هستار در سطح تضمین معین و درک شده را جمع‌آوری و بررسی می‌کند.

1- Identifier
2- Identity
3- Registration authority

۱۶-۳
حمله فرد در میان (MITM)[1]
حمله‌ای است که در آن مهاجم قادر به خواندن، درج و اصلاح پیام‌های بین دو طرف است، بدون اینکه آن‌ها مطلع شوند.

۱۷-۳
اصالت‌سنجی چندعامله[2]
اصالت‌سنجی که حداقل دو عامل اصالت‌سنجی مستقل در آن استفاده شده‌اند.

[ISO/IEC 19790]

۱۸-۳
اصالت‌سنجی متقابل[3]
اصالت‌سنجی هستارهایی است که به هر طرف در مورد هویت طرف دیگر تضمین ارائه می‌کند.

۱۹-۳
انکار ناپذیری[4]
توانایی محافظت در برابر انکار توسط یکی از هستارهای درگیر در یک اقدام در مورد مشارکت در کل یا بخشی از آن اقدام است.

[ITU-T X.1252]

۲۰-۳
حمله صیادی[5]
نوعی کلاه‌برداری[6] است که در آن یک کاربر رایانامه فریب داده می‌شود تا اطلاعات شخصی یا محرمانه‌ای را افشا کند که کلاه‌بردار می‌تواند از آن به صورت غیر قانونی استفاده کند.

۲۱-۳
مرجع ثبت
شخص مورد اعتمادی است که هویت یک هستار را نزد یک CSP تصدیق یا تضمین می‌کند.

۲۲-۳
طرف اعتماد کننده
شخصی است که به اظهارنامه یا ادعای هویت اعتماد می‌کند.

---

1 - Man-in-the-middle
2 - Multifactor authentication
3 - Mutual authentication
4 - Non-repudiation
5 - Phishing
6- Scam

۲۳-۳
انکار[1]

انکار مشارکت در تمام یا بخشی از یک اقدام توسط یکی از هستارهای درگیر است.
[ITU-T X.1252]

۲۴-۳
سالت[2]

مقداری غیر مخفی و اغلب تصادفی است که در فرآیند درهم‌سازی[3] استفاده می‌شود.

یادآوری- این مقدار با نام شن[4] نیز شناخته می‌شود.

۲۵-۳
راز به اشتراک گذاشته شده[5]

راز استفاده شده در اصالت‌سنجی که فقط هستار و درستی‌سنج از آن مطلع هستند.

۲۶-۳
مُهر زمانی[6]

پارامتر متغیر زمانی قابل اعتمادی است که نقطه‌ای در زمان را با توجه به یک مرجع مشترک مشخص می‌کند.

۲۷-۳
تراکنش[7]

رویدادی گسسته بین یک هستار و ارائه دهنده خدمت است که از یک هدف کسب و کار یا برنامه حمایت می‌کند.

۲۸-۳
چارچوب اعتماد

مجموعه‌ای از الزامات و سازوکارهای اجرایی برای طرفینی است که اطلاعات هویت خود را تبادل می‌کنند.

1- Repudiation
2 - Salt
۱ - در رمزنگاشتی در الگوریتم‌های درهم‌ساز، salt شامل بیت‌های تصادفی است که ورودی‌های یک تابع یک طرفه را ایجاد می‌کند
3 - Hashing process
4 - Sand
5 - Shared secret
6 - Time stamp
7- Transaction

۲۹-۳
طرف سوم مورد اعتماد
مرجع یا عامل آن است که برای انجام فعالیت‌های معینی (به عنوان مثال فعالیت‌های مرتبط با امنیت) مورد اعتماد اشخاص دیگر است.

یادآوری- یک هستار یا درستی‌سنج برای اهداف اصالت‌سنجی به یک طرف سوم مورد اعتماد، اعتماد می‌کنند.

۳۰-۳
مدت اعتبار
مدت زمانی است که طی آن یک هویت یا اعتبارنامه می‌تواند در یک یا چند تراکنش استفاده شود.

۳۱-۳
درستی‌سنجی
فرآیند بررسی اطلاعات از طریق مقایسه اطلاعات ارائه شده با اطلاعات تایید شده پیشین است.

۳۲-۳
درستی‌سنج
شخصی است که اطلاعات هویت را تایید می‌کند.

یادآوری- درستی‌سنج می‌تواند در چندین مرحله از چارچوب تضمین اصالت‌سنجی هستار شرکت کند و درستی‌سنجی اعتبارنامه یا درستی‌سنجی اطلاعات هویت را انجام دهد.

۴ کوته‌نوشت‌ها

در این استاندارد کوته‌نوشت‌های زیر نیز به کار می‌رود:

CAs	Certificate Authorities	مراجع صدور گواهی
CSP	Credential Service Provider	ارائه کننده خدمات اعتبارنامه
CV	Card Verifier	درستی‌سنج برگه
EAA	Entity Authentication Assurance	تضمین اصالت‌سنجی هستار
EAAF	Entity Authentication Assurance Framework	چارچوب تضمین اصالت‌سنجی هستار
Idm	Identity Management	مدیریت هویت
ICT	Information and Communications Technology	فناوری اطلاعات و ارتباطات
IP	Internet Protocol	قرارداد اینترنت
LoA	Level of Assurance	سطح تضمین
LoAs	Levels of Assurance	سطوح تضمین
MAC	Media Access Control	کنترل دسترسی رسانه
NPE	Non-Person Entity	هستار غیر انسان

PII	Personally Identifiable Information	اطلاعات قابل شناسایی شخصی
PIN	Personal Identification Number	شماره شناسایی شخصی
RA	Registration Authority	مرجع ثبت
RP	Relying Party	طرف اعتماد کننده
SAML	Security Assertion Markup Language	زبان نشانه‌گذاری اظهارنامه امنیتی
SSL	Secure Sockets Layer	لایه دریچه امن
TCP/IP	Transmission Control Protocol/Internet Protocol	قرارداد کنترل انتقال / قرارداد اینترنت
TLS	Transport Layer Security	امنیت لایه انتقال
TPM	Trusted Platform Module	پودمان بستر مورد اعتماد
TTP	Trusted Third Party	طرف سوم مورد اعتماد
URL	Uniform Resource Locator	موقعیت‌یاب همسان منبع

۵ قراردادها

این استاندارد ملی از راهنمای استاندارد ملی کشور در خصوص شکل کلامی برای بیان شروط پیروی می‌کند.

الف- «باید[1]» نشان دهنده یک الزام است.

ب- «توصیه می‌شود[2]» نشان دهنده یک توصیه است.

پ- «مجاز است[3]» نشان دهنده اجازه است.

ت- «می‌تواند/ممکن[4]» است نشان دهنده یک احتمال و قابلیت است.

۶ سطوح تضمین

این چارچوب تضمین اصالت‌سنجی هستار (EAAF)، چهار سطح تضمین (LoAs) برای اصالت‌سنجی هستار تعریف می‌کند. هر LoA درجه اطمینان به فرآیند پیش از اصالت‌سنجی و خود فرآیند اصالت‌سنجی را توصیف می‌کند و از این رو تضمین می‌دهد که هستاری که از یک هویت خاص استفاده می‌کند، در حقیقت همان هستاری است که هویت به آن اختصاص داده شده است. در این استاندارد ملی، LoA کارکردی از فرآیندها، فعالیت‌های مدیریت و کنترل‌های فنی است که برای هر یک از مرحله‌های EAAF بر مبنای معیارهای معین شده در بند ۱۰ توسط یک CSP پیاده‌سازی شده‌اند. تضمین اصالت‌سنجی هستار (EAA) از

1 - Shall
2 - Should
3 - May
4 - Can

ملاحظات مدیریتی و سازمانی متاثر می‌شود، اما این استاندارد ملی برای آن ملاحظات معیارهای اصولی صریح ارائه نمی‌کند. هستار می‌تواند یک انسان یا یک هستار غیر انسان (NPE) باشد.

برای مثال، LoA یک شبکه می‌تواند کارکرد LoAهای تمامی مولفه‌هایی باشد که شبکه را شکل می‌دهند و شامل NPEها یا افزاره‌های نقطه پایانی (به عنوان مثال تلفن‌های همراه، لپ تاپ‌ها، دستیار رقمی شخصی(PDA)[1]، افزاره‌های set-top) می‌شود. در برخی موارد، افزاره‌های نقطه پایانی ممکن است خود را به جای هستارهای قانونی جا بزنند. در نتیجه، توانایی شناسایی، با درجه‌ای از اطمینان، افزاره‌ای مورد اعتماد از یک افزاره متقلب برای EAA بنیادی است.

در این استاندارد ملی پایین‌ترین سطح تضمین LoA1 و بالاترین سطح تضمین LoA4 معین شده است. تعیین اینکه برای هر موقعیت چه سطح تضمینی مناسب است به عامل‌های مختلفی بستگی دارد. تعیین LoA مورد نیاز عمدتا بر مبنای مخاطره انجام می‌گیرد: پی‌آمدهای خطای اصالت‌سنجی یا سوءاستفاده از اعتبارنامه‌ها، آسیب و اثرات ناشی از آن و احتمال وقوع مخاطرات. LoAهای بالاتر باید برای مخاطرات بالاتر استفاده شوند.

چارچوب تضمین اصالت‌سنجی هستار (EAAF) برای هر یک از چهار سطح LoA الزامات و راهنمای پیاده‌سازی ارائه می‌کند. به طور خاص، الزامات پیاده‌سازی فرآیندها را برای مرحله‌های زیر ارائه می‌کند:

الف- نام‌نویسی (به عنوان مثال اثبات هویت، درستی‌سنجی اطلاعات هویت، ثبت نام)

ب- مدیریت اعتبارنامه (به عنوان مثال صدور اعتبارنامه، فعال‌سازی اعتبارنامه)

پ- اصالت‌سنجی.

علاوه بر این در مورد ملاحظات مدیریتی و سازمانی (به عنوان مثال الزامات قانونی، مدیریت امنیت اطلاعات) که بر تضمین اصالت‌سنجی هستار اثر می‌گذارند نیز راهنمایی‌هایی ارائه می‌شود.

تعریف LoAها در جدول ۱ نشان داده شده است.

جدول۱- سطوح تضمین[2]

سطح	توصیف
۱- پایین	اطمینان در مورد هویت اظهارنامه یا ادعا شده ناچیز است یا اصلا وجود ندارد
۲- متوسط	تا حدودی در مورد هویت اظهارنامه یا ادعا شده اطمینان وجود دارد
۳- بالا	اطمینان بالایی در مورد هویت اظهار شده یا ادعا شده وجود دارد.

1 - Personal digital assisstant

۲- LoA کارکردی از فرایندها، فعالیت‌های مدیریتی، و کنترل‌های فنی است که برای هر یک از مرحله‌های EAAF بر مبنای معیارهای معین شده در بند ۱۰ توسط یک CSP پیاده‌سازی شده‌اند.

سطح	توصیف
۴- بسیار بالا	اطمینان بسیار بالایی در مورد هویت اظهارنامه یا ادعا شده وجود دارد.

این چارچوب، الزامات دستیابی به سطح LoA مطلوب برای هر یک از مرحله‌های چارچوب تضمین اصالت‌سنجی هستار را دربرمی‌گیرد. LoA کلی حاصل از پیاده‌سازی با استفاده از این چارچوب، سطح مرحله‌ی خواهد بود که پایین‌ترین LoA را دارد.

۶-۱ سطح تضمین یک (LoA1)

در LoA1 کمینه اطمینانی به هویت اظهارنامه یا ادعا شده هستار وجود دارد، اما تا حدودی اطمینان وجود دارد که هستار در رویدادهای اصالت‌سنجی متوالی یکسان بوده است. این LoA هنگامی استفاده می‌شود که مخاطره کمینه به اصالت‌سنجی نادرست نسبت داده شده باشد. هیچ گونه الزام خاصی برای سازوکار اصالت‌سنجی استفاده شده، وجود ندارد؛ فقط کافی است که یک تضمین کمینه‌ای را فراهم کند. طیف وسیعی از فناوری‌های موجود، از جمله اعتبارنامه‌های اختصاص داده شده به LoAهای بالاتر، می‌توانند الزامات تضمین اصالت‌سنجی هستار برای این LoA را برآورده کنند. در این سطح به روش‌های اصالت‌سنجی رمزنگاشتی (به عنوان مثال قرارداد چالش-پاسخ مبتنی بر رمزنگاشتی[1]) نیاز نیست.

برای مثال، LoA1 ممکن است در اصالت‌سنجی که در آن یک هستار برای ایجاد صفحه‌ای سفارشی‌سازی شده در یک وبگاه شناسانه کاربری و اسم رمز ثبت شده ارائه می‌کند، یا تراکنش‌های وبگاه‌هایی که برای دسترسی به مواد و مستندات، مانند مستندات محصولات یا اخبار، به ثبت نام نیاز دارند کاربرد داشته باشد.

برای مثال، در LoA1، آدرس کنترل دسترسی رسانه (MAC) ممکن است الزام اصالت‌سنجی افزاره را برآورده کند. با این حال، اطمینان کمی وجود دارد که یک افزاره دیگر قادر به استفاده از همان آدرس MAC نخواهد بود.

۶-۲ سطح تضمین دو (LoA2)

در LoA2 تا حدودی در مورد اظهارنامه یا ادعا هویت هستار اطمینان وجود دارد. این LoA زمانی استفاده می‌شود که مخاطره متوسطی به اصالت‌سنجی نادرست نسبت داده شده باشد. اصالت‌سنجی تک عاملی[2] قابل قبول است. اصالت‌سنجی موفقیت‌آمیز به این وابسته است که هستار از طریق یک قرارداد اصالت‌سنجی امن ثابت کند که بر اعتبارنامه کنترل دارد. توصیه می‌شود کنترل‌هایی در نظر گرفته شوند تا اثربخشی استراق سمع کننده[3] و حملات حدس زدن بر خط[4] را کاهش دهند. باید کنترل‌هایی در نظر گرفت تا در برابر حملات به اعتبارنامه‌های ذخیره شده محافظت شود.

1 - Cryptographic-based challenge-response protocol
2 - Single-factor
3 - Eavesdropper
4 - Online guessing attack

برای مثال، یک ارائه کننده خدمات ممکن است وبگاهی را اداره کند که به مشتریانش اجازه تغییر آدرس رکورد خود را می‌دهد. تراکنشی که در آن یک ذی‌نفع آدرس رکورد خود را تغییر می‌دهد، می‌تواند یک تراکنش اصالت‌سنجی LoA2 در نظر گرفته شود، زیرا که تراکنش ممکن است مخاطره ناسازگاری متوسطی داشته باشد. از آنجا که آگهی‌های رسمی در مورد مبالغ پرداختی، وضعیت حساب و رکوردهای تغییرات به طور معمول به آدرس رکورد ذی‌نفع فرستاده می‌شوند، تراکنش همچنین مخاطره متوسط انتشار غیرمجاز PII را به همراه دارد. در نتیجه، ارائه کننده خدمات باید حداقل تضمین اصالت‌سنجی را قبل از دادن اجازه انجام تراکنش به دست آورده باشد.

۳-۶ سطح تضمین سه (LoA3)

در LoA3، اطمینان بالایی در مورد اظهارنامه یا ادعا هویت هستار وجود دارد. این LoA زمانی استفاده می‌شود که مخاطره قابل توجهی به اصالت‌سنجی نادرست نسبت داده شده باشد. این LoA باید اصالت‌سنجی چند عامله را به کار گیرد. هر گونه اطلاعات محرمانه مبادله شده در قراردادهای اصالت‌سنجی باید از طریق رمزنگاشتی در ارسال و دریافت محافظت شده باشد (البته LoA3 به استفاده از قرارداد چالش-پاسخ مبتنی بر رمزنگاشتی احتیاج ندارد). هیچ گونه الزامی در خصوص تولید و ذخیره‌سازی اعتبارنامه‌ها وجود ندارد؛ آن‌ها می‌توانند در رایانه‌های کاربرد عمومی یا سخت‌افزارهای کاربرد خاص تولید و ذخیره شوند.

برای مثال، تراکنشی که در آن یک شرکت اطلاعات محرمانه خاصی را به صورت الکترونیکی به نهادی دولتی ارسال می‌کند ممکن است به تراکنش اصالت‌سنجی LoA3 نیاز داشته باشد. فاش‌سازی نادرست ممکن است به مخاطره ضرر مالی قابل توجهی منجر شود. مثال‌های دیگری از تراکنش‌های LoA3 شامل دسترسی بر خط هستار به حساب‌هایی که امکان انجام تراکنش‌های مالی خاصی را می‌دهند، یا استفاده پیمانکار طرف سوم از یک سامانه راه دور برای دسترسی احتمالی به اطلاعات حساس کارمندان مشتری، می‌شوند.

۴-۶ سطح تضمین چهار (LoA4)

در LoA4 اطمینان بسیار بالایی به اظهارنامه یا ادعا هویت هستار وجود دارد. این LoA زمانی استفاده می‌شود که مخاطره بالایی به اصالت‌سنجی نادرست نسبت داده شده باشد. LoA4 بالاترین سطح تضمین اصالت‌سنجی هستار تعریف شده در این استاندارد ملی را فراهم می‌کند. LoA4 مشابه LoA3 است، اما الزام اثبات هویت شخصی برای هستارهای انسانی و استفاده از افزاره‌های سخت‌افزاری مقاوم در برابر مداخله[1] برای ذخیره‌سازی تمامی کلیدهای رمزنگاشتی محرمانه یا سری را اضافه می‌کند. علاوه بر این، همه PII و سایر داده‌های حساس در قرارداد اصالت‌سنجی باید در ارسال و دریافت با رمزنگاشتی محافظت شوند.

برای مثال، در خدماتی که احتمال مخاطره آسیب یا ضرر در حالت شکست اصالت‌سنجی بالا است ممکن است به محافظت LoA4 نیاز داشته باشند. طرف مسؤول به تضمین کامل نیاز دارد که هستار درست اطلاعات حیاتی معینی را ارائه کرده است و طرف مسؤول حتی ممکن است در قبال هر گونه شکست در

1- Tamper-resistant hardware device

ارزیابی اطلاعات از نظر جنایی مسؤول باشد. در آخر، تایید یک تراکنش که شامل مخاطره بالای ضرر مالی می‌شود می‌تواند یک تراکنش LoA4 باشد.

در LoA4، گواهینامه‌های رقمی (به عنوان مثال X509، گواهینامه‌های درستی‌سنج برگه (CV)) می‌توانند برای اصالت‌سنجی NPEها، مانند لپ‌تاپ‌ها، تلفن‌های همراه، چاپگرها، افزاره‌های نمابر و سایر افزاره‌های متصل به شبکه، استفاده شوند. برای مثال، فرآیند نام‌نویسی تلفن هوشمند ممکن است نیازمند به کار بردن گواهینامه‌های رقمی در تلفن هوشمند باشد. همچنین، به منظور جلوگیری از دسترسی غیرمجاز به شبکه برق می‌توان از گواهینامه‌های رقمی در استقرار فناوری‌های سنجش‌گر هوشمند استفاده کرد.

۶-۵ انتخاب سطح تضمین مناسب

توصیه می‌شود انتخاب LoA مناسب بر مبنای ارزیابی مخاطره تراکنش‌ها یا خدماتی که هستارها برای آن اصالت‌سنجی می‌شوند، صورت پذیرد. با نگاشت سطوح تاثیر به LoAها طرفین تراکنش اصالت‌سنجی می‌توانند LoA مورد نیاز خود را معین کرده و مطابق با آن خدمات را تدارک ببینند و اعتماد خود را بر هویت‌های تضمین شده قرار دهند. جدول ۲ پی‌آمدها و اثرات احتمالی شکست اصالت‌سنجی را در LoAهای مختلف نشان می‌دهد.

جدول۲- اثر احتمالی در هر سطح تضمین

پی‌آمدهای احتمالی شکست اصالت‌سنجی	تاثیر احتمالی شکست اصالت‌سنجی بر اساس LoA			
	۱	۲	۳	۴
ناسازگاری، توقیف، یا صدمه به شهرت یا اعتبار	کمینه	متوسط	قابل توجه	بالا
ضرر مالی یا بدهکاری سازمان	کمینه	متوسط	قابل توجه	بالا
ضرر به سازمان، برنامه‌های آن یا منافع عمومی	نامعین	کمینه	متوسط	بالا
انتشار غیرمجاز اطلاعات حساس	نامعین	متوسط	قابل توجه	بالا
امنیت شخصی	نامعین	نامعین	کمینه- متوسط	قابل توجه - بالا
تخلف مدنی یا جنایی	نامعین	نامعین	قابل توجه	بالا

تعیین اینکه چه مواردی مخاطره کمینه، متوسط، قابل توجه و بالا محسوب می‌شوند به معیارهای مخاطره تعریف شده برای هر یک از پی‌آمدهای احتمالی وابسته است که توسط سازمانی که از این استاندارد ملی استفاده می‌کند مشخص می‌شوند. علاوه بر این، وجود چندین فرانامه تاثیرگذار نیز محتمل است (به عنوان مثال، پی‌آمدها ممکن است شامل ضرر به سازمان و همچنین انتشار غیرمجاز اطلاعات حساس شوند). در فرانامه‌های تاثیرگذار چندگانه، توصیه می‌شود بالاترین LoA متناظر با پی‌آمدها استفاده شود.

هر LoA باید بر اساس دوام و دقت کنترل‌ها و فرآیندهای هر مرحله از EAAF که CSP بر تدارک خدمات خود اعمال می‌کند، معین شود. EAAF نیاز تعریف معیارهای تضمین خدمات اجرایی در هر LoA را برای

CSPها به وجود می‌آورد. معیارهای تضمین خدمات در بند ۱۱ معرفی می‌شوند، اما الزامات خاص خارج از محدوده این استاندارد ملی است.

هنگام استفاده از نتایج ارزیابی مخاطره برای تعیین LoA کاربرد پذیر ممکن است عامل‌های مرتبط با کسب و کار دیگری، فراتر از محدوده امنیت، وجود داشته باشند که باید در نظر گرفته شوند. چنین عامل‌های کسب و کاری می‌تواند شامل موارد زیر شود:

الف- رویکرد سازمان به مدیریت مخاطره باقیمانده؛

ب- میل سازمان به پذیرش مخاطره از لحاظ اثرات نشان داده شده در جدول ۲؛ و

پ- اهداف کسب و کار خدمت (به عنوان مثال، اگر سازمان فرآیندهایی برای محدود کردن جعل دارد و پذیرش مخاطره جعل برای آن راحت است، بهتر است در خدمتی که هدف کسب و کار آن افزایش جذب مشتریان[1] است، از LoA سطح پایین و اعتبارنامه‌ای مانند اسم رمز استفاده کند).

ارزیابی مخاطره یک تراکنش می‌تواند به عنوان بخشی از ارزیابی مخاطره امنیتی کلی سازمان انجام شود (به عنوان مثال استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷) و توصیه می‌شود بر نیاز خاص امنیت در تراکنش‌های مورد بررسی تمرکز شود. ارزیابی مخاطره باید مخاطرات مرتبط با EAA را در نظر بگیرد. نتیجه ارزیابی مخاطره باید با چهار LoA مقایسه شود. LoAای که بیشترین تطابق را با ارزیابی مخاطره دارد باید انتخاب شود.

در مواردی که با رده‌های[2] چندگانه تراکنش مواجه است، احتمال دارد که یک LoA متفاوت برای هر تراکنش یا گروه از تراکنش‌ها کاربرد پذیر باشد. به عبارت دیگر، مطابق با تراکنش خاص مورد نظر ممکن است چندین LoA توسط یک سازمان پذیرفته شوند.

۶-۶ نگاشت LoA و قابلیت همکاری متقابل[3]

دامنه‌های متفاوت ممکن است LoAها را به صورت‌های مختلف تعریف کنند. این LoAها به طور الزامی نگاشت یک به یک با چهار LoA توصیف شده در این چارچوب را پشتیبانی نمی‌کنند. برای مثال، یک دامنه ممکن است مدل چهار سطحی را به کار بگیرد و یک دامنه دیگری می‌تواند مدل پنج سطحی را بپذیرد. معیارهای مختلف برای مدل‌های اصالت‌سنجی متفاوت باید به صورت مجزا تعریف و به طور گسترده ابلاغ شوند.

به منظور دستیابی به قابلیت همکاری متقابل میان مدل‌های LoA مختلف، هر دامنه باید نحوه ارتباط طرح نگاشت خود با LoAهای تعریف شده در این استاندارد را به صورت زیر توضیح دهد:

1- Uptake
2 - Class
3 - Interoperability

الف- ایجاد روشگان تضمین اصالت‌سنجی خوش تعریف که شامل طبقه‌بندی خوش تعریف برای LoAها می‌شود.

ب- انتشار وسیع این روشگان به نحوی که سازمان‌هایی که مایل به ورود در این پیمان‌های اتحادیه گونه با آن‌ها هستند بتوانند فرآیندها و اصطلاح‌شناسی یکدیگر را به وضوح درک کنند.

روشگان LoA باید LoAها را از لحاظ ارزیابی مخاطره به صورت شفاف تعریف کنند و موارد زیر را برای آن معین و کیفی کنند:

الف- تهدیدهای پیش‌بینی شده؛

ب- اثرات (یعنی کمینه، متوسط) در صورتی که تهدید به واقعیت تبدیل شود؛

پ- شناسایی تهدیدهایی که باید در هر LoA کنترل شوند؛

ت- فناوری‌ها و فرآیندهای امنیتی پیشنهادی برای استفاده در پیاده‌سازی کنترل‌ها در هر LoA، مانند معین کردن اجرای اعتبارنامه بر روی افزاره‌های سخت‌افزاری (مانند کارت هوشمند) یا مشخص کردن الزامات برای تولید و ذخیره‌سازی اعتبارنامه‌ها؛

ث- معیارهای معین کردن هم‌ارزی ترکیبات مختلف عامل‌های اصالت‌سنجی با در نظر داشتن اثبات هویت و اعتبارنامه‌های نسبت داده شده.

یک رویکرد برای پرداختن به مسئله نگاشت/ارتباط بین مدل‌های LoA مختلف می‌تواند استفاده از مدل چهار سطح تعریف شده در این مستند و نگاشت سایر مدل‌های n سطحی به آن باشد. این روش به اتحادیه هویت[1] که از مدل‌های متفاوتی برای تضمین اصالت‌سنجی استفاده می‌کنند امکان می‌دهد خود را با مدل چهار سطحی نگاشت کنند. نگاشت‌ها باید نحوه کنترل LoAهای نگاشت نشده را تعریف کنند، که نادیده گرفتن آن‌ها یا نگاشت موثر آن‌ها به پایین‌ترین سطح بعدی (زیرا اگر از قبل به صورت مشخصی معین نشده بود هیچ مبنایی برای فرض اینکه LoA سطح بالاتری دارد نمی‌توانست وجود داشته باشد) می‌تواند یک راه حل باشد.

۷-۶ تبادل نتایج اصالت‌سنجی بر مبنای LoA4

اشخاص درگیر در تراکنش اصالت‌سنجی (به عنوان مثال CSPها، RPها) ممکن است برای تکمیل تراکنش یا فعالیت نیاز به تبادل اطلاعات داشته باشند.

حیطه این فعالیت‌ها شامل موارد زیر می‌شود، هر چند به این‌ها محدود نیست:

1- Identity federation

الف- اجازه دادن به یک RP برای بیان انتظاراتش از LoAای که یک هستار باید در آن اصالت‌سنجی شود؛

ب- اجازه دادن به یک هستار یا CSP برای نشان داده LoA واقعی در پاسخ‌های خود؛

پ- اجازه دادن به یک هستار یا CSP برای تبلیغ LoAهایی که از نظر داشتن الزامات مرتبط با آن LoA واجد صلاحیت شناخته شده است.

اشخاص درگیر در یک تراکنش اصالت‌سنجی باید بر روی قرارداد، معناشناسی[1]، قالب و ساختار اطلاعاتی که باید تبادل شوند، توافق کنند. ممکن است نیاز باشد RP مشخص کند که پاسخ‌های اصالت‌سنجی غیر از آنچه را که به طور دقیق خواسته شده می‌پذیرد یا خیر.

در حالی که گواهینامه‌های رقمی روشی محرز برای انتقال اطلاعات در خصوص تضمین اعتبارنامه‌های مرتبط هستند، فراداده به طور فزاینده‌ای به عنوان روش ابلاغ الزامات تضمینی طرفین تبادل مورد استفاده قرار می‌گیرد. یک رده زمینه[2]، مانند رده زمینه اصالت‌سنجی[3] زبان نشانه‌گذاری اظهارنامه امنیتی (SAML) در قالب URI، سازوکار شناخته شده‌ای برای طرفین است تا رده‌های مرتبط با تضمین اصالت‌سنجی در اظهارنامه یا درخواست اصالت‌سنجی را بیان کنند. برای مثال، یک اظهارنامه معمول از طرف یک ارائه کننده هویت ممکن است شامل اطلاعاتی مانند «این کاربر «جان داو» است؛ آدرس رایانامه او john.doe@example.com است؛ او با استفاده از سازوکار اسم رمز در این سامانه اصالت‌سنجی شده است» باشد.

باقی این چارچوب به ساختاری که فرآیندها و الزامات خدمات در آن ساخته می‌شوند و تهدیدها و اثرات مرتبط با اصالت‌سنجی هستار می‌پردازد. در خاتمه مرور کلی بر نیاز به معیارهای تضمین خدمات ارائه می‌شود که خدمات باید در برابر آن ارزیابی شوند تا تضمین شود که LoA مقتضی برای دستیابی به خدمات اعتباردهی مناسب اختصاص یافته است.

۷ اشخاص

اشخاص درگیر در EAAF شامل هستارها، CSPها، RAها، RPها، درستی‌سنج‌ها و TTPها می‌شود. این اشخاص ممکن است متعلق به یک سازمان یا سازمان‌های مجزا باشند. ممکن است تنوعی از روابط و قابلیت‌ها توسط تعدادی از سازمان‌ها ارائه شود، از جمله مولفه‌ها، سامانه‌ها و خدمات مشترک یا تعاملی.

۷-۱ هستار

یک هستار می‌تواند اصالت‌سنجی شود. قابلیت اصالت‌سنجی یک هستار به چند عامل وابسته است. در زمینه این چارچوب، قابلیت اصالت‌سنجی یک هستار به این معنا است که هستار توسط یک CSP ثبت شده و

1- Semantic
2 - Context class
3 - Authentication context class

اعتبارنامه‌های مناسب را دریافت کرده است و یک قرارداد اصالت‌سنجی برای آن معین شده است. در حین اصالت‌سنجی، هستار می‌تواند برای هویت خود گواهی دهد. همچنین امکان دارد که یک طرف مستقل از طرف هستار برای اهداف اصالت‌سنجی ایفای نقش کند.

۲-۷ ارائه کننده خدمات اعتبارنامه

یک ارائه کننده خدمات اعتبارنامه (CSP)، اعتبارنامه‌ها یا سخت‌افزار، نرم‌افزار و داده‌های وابسته را که می‌توانند برای تولید اعتبارنامه‌ها استفاده شوند، صادر یا مدیریت می‌کند. اسم رمز یا خصیصه‌های زیست‌سنجی نمونه‌هایی از یک اعتبارنامه هستند که توسط یک CSP می‌تواند صادر و مدیریت شود. کارت‌های هوشمند در بر گیرنده کلیدهای محرمانه نمونه‌ای از سخت‌افزار و داده‌های وابسته (که می‌توانند برای تولید اعتبارنامه‌ها استفاده شوند) هستند که می‌تواند توسط یک CSP صادر و مدیریت شود. یک CSP همچنین می‌تواند داده‌هایی را صادر و مدیریت کند که می‌توانند برای اصالت‌سنجی اعتبارنامه‌ها استفاده شوند. اگر اسم رمزها به عنوان اعتبارنامه استفاده شوند، این داده‌ها می‌تواند مقادیر کارکردهای یک طرفه[1] آن‌ها باشند. اگر اعتبارنامه‌ها بر پایه اطلاعات دارای امضای رقمی باشند، CSPها می‌توانند گواهینامه‌های کلید عمومی تولید کنند که توسط درستی‌سنج‌ها استفاده شوند. اعتبارنامه‌هایی که صادر و پشتیبانی می‌شوند و همچنین حفاظ‌های پیاده‌سازی شده توسط CSP، عامل‌های کلیدی در معین کردن LoA در یک تراکنش اصالت‌سنجی خاص هستند (به بند ۱۰-۳ نیز مراجعه شود).

برای هر هستار باید یک یا چند اعتبارنامه، یا ابزاری برای صدور اعتبارنامه، صادر شود تا اصالت‌سنجی در آینده را ممکن سازد. اعتبارنامه‌ها، یا ابزار تولید اعتبارنامه‌ها، به طور معمول تنها بعد از تکمیل موفقیت‌آمیز فرآیند نام‌نویسی، که هستار در پایان آن ثبت می‌شود، صادر می‌شوند.

۳-۷ مرجع ثبت

یک مرجع ثبت (RA) هویت یک هستار را احراز می‌کند و برای آن نزد یک CSP تضمین می‌دهد. CSP باید به RA اطمینان کند که فرآیندهای مرتبط با مرحله نام‌نویسی و ثبت هستارها را به نحوی اجرا کند که امکان تخصیص اعتبارنامه‌ها توسط CSP در آینده فراهم باشد.

هر RA باید نوعی اثبات هویت و درستی‌سنجی اطلاعات هویت را بر طبق فرآیندهای معین شده انجام دهد. به منظور تمایز بین هستار و سایر هستارها، به طور معمول به هستار یک یا چند شناسانه اختصاص داده می‌شود، که امکان شناسایی هستار در زمینه کاربردی در آینده را فراهم می‌کند.

۴-۷ طرف اعتماد کننده

طرف اعتماد کننده (RP) شخصی است که به یک اظهارنامه یا ادعا هویت اعتماد می‌کند. طرف اعتماد کننده ممکن است یک هویت اصالت‌سنجی شده را برای اهداف متنوعی درخواست کند، مانند مدیریت حساب

1 - One-way functions

کاربری، کنترل دسترسی، تصمیمات صدور مجوز و غیره. طرف اعتماد کننده می‌تواند خود عملیات لازم برای اصالت‌سنجی هستار را انجام دهد، یا می‌تواند عملیات را به یک طرف سوم واگذار کند.

۵-۷ درستی‌سنج

درستی‌سنج شخصی است که اطلاعات هویت را تایید می‌کند. درستی‌سنج می‌تواند در چندین مرحله از EAA شرکت کند و می‌تواند درستی‌سنجی اعتبارنامه یا درستی‌سنجی اطلاعات هویت را انجام دهد.

۶-۷ طرف سوم مورد اعتماد

یک TTP مسؤول یا عامل آن است که مورد اعتماد سایر اشخاص در ارتباط با انجام فعالیت‌های خاصی (به عنوان مثال، فعالیت‌های مرتبط با امنیت) است. در این چارچوب، یک TTP برای اهداف اصالت‌سنجی مورد اعتماد یک هستار یا درستی‌سنج است. نمونه‌هایی از TTP برای اهداف اصالت‌سنجی هستار شامل مراجع صدور گواهی(CA) و مرجع صدور مُهر زمانی هستند.

۸ مراحل چارچوب تضمین اصالت‌سنجی هستار

در این بند توضیح مرحله‌ها و فرآیندهای EAA ارائه می‌شود. با این که برخی مدل‌های EAA ممکن است متفاوت از ساختار این مدل باشند، تطابق با این مدل مستلزم این است که قابلیت‌های کارکردی به طور کامل الزاماتی مشخص شده در این چارچوب را پوشش دهند. این چارچوب به هیچ فناوری وابسته نیست.

سازمان‌هایی که این چارچوب را می‌پذیرند باید خط‌مشی‌ها، رویه‌ها و قابلیت‌هایی را دایر کنند که فرآیندهای پشتیبانی لازم را فراهم می‌کنند و الزامات مشخص شده در این چارچوب را برآورده می‌کنند. این موارد بسته به نقش انتخاب شده توسط هر سازمان و، به عنوان مثال، LoA که سازمان در آن اعتبارنامه ارائه می‌کند متفاوت خواهند بود. برای مثال، یک سازمان ممکن است لازم باشد موارد زیر را معین کند:
الف- الزاماتی برای اقدامات خاصی از طرف سازمان یا نمایندگان آن در ارتباط با LoAهای خاص؛

ب- الزاماتی برای ارزیابی قابلیت اجرایی سازمان در حیطه EAAF توسط طرف سوم یا خارجی؛

پ- خط‌مشی‌ها، اقدامات و قابلیت‌های لازم جهت تصدیق قابلیت اعتماد فرآیندها، خدمات و قابلیت‌های ارائه شده توسط سازمان‌هایی که چارچوب را پذیرفته‌اند.

۱-۸ مرحله نام‌نویسی

مرحله نام‌نویسی شامل چهار فرآیند می‌شود: درخواست و شروع، اثبات هویت، درستی‌سنجی اطلاعات هویت، نگهداری رکورد/ثبت. این فرآیندها ممکن است به طور کامل توسط یک سازمان انجام شود یا ممکن است از تنوعی از روابط و قابلیت‌های ارائه شده توسط شماری از سازمان‌ها تشکیل شده باشد که شامل مولفه‌ها، سامانه‌ها و خدمات مشترک و تعاملی می‌شوند.

فرآیندهای مورد نیاز بسته به دقت خواسته شده توسط LoA کاربردپذیر متفاوت خواهند بود. در مورد هستاری که تحت LoA1 نام‌نویسی می‌کند، این فرآیندها کمینه هستند (به عنوان مثال، یک نفر می‌تواند بر روی دکمه «کاربر جدید» در یک وبگاه کلیک کند و شناسانه کاربری و اسم رمز ایجاد کند). در موارد دیگر، فرآیندهای نام‌نویسی ممکن است گسترده باشد. برای مثال، نام‌نویسی در LoA4 علاوه بر اثبات هویت گسترده، نیازمند نشست حضوری میان هستار و RA است.

۸-۱-۱ درخواست و شروع

فرآیند نام‌نویسی به روش‌های مختلفی شروع می‌شود. به طور مثال، ممکن است در پی درخواست هستارهایی که به دنبال دریافت اعتبارنامه‌های خاصی برای خود هستند، شروع شود (به عنوان مثال، هنگامی که کاربر جدید یک وبگاه می‌خواهد شناسانه کاربری و اسم رمز به دست آورد). همچنین احتمال دارد که فرآیند نام‌نویسی توسط یک طرف سوم از طرف هستار یا توسط خود CSP (به عنوان مثال کارت شناسایی صادر شده توسط دولت، نشان کارمندی) شروع شود. برای مثال، در LoAهای بالاتر درخواست‌ها ممکن است تنها در صورتی پذیرفته شوند که توسط یک طرف سوم حمایت شوند.

در هر صورت، فرآیند شروع مرحله نام‌نویسی برای انسان‌ها ممکن است شامل پر کردن کل فرم درخواست‌نامه شود. توصیه می‌شود این فرم اطلاعات کافی جهت تضمین شناسایی منحصر به فرد هستار در یک زمینه را ثبت کند (به عنوان مثال، از طریق ثبت اسم کامل، تاریخ و محل تولد). برای NPEها، مانند افزاره‌های تلفن همراه، نام‌نویسی ممکن است مستلزم آغاز از طریق دایر کردن اعتبارنامه‌ها در افزاره باشد که امکان شناسایی افزاره به صورت منحصر به فرد و دریافت تنظیمات ویژه افزاره از طریق یک رُخ‌نما پیکربندی رمزبندی شده را فراهم می‌سازد.

CSPها باید شرایطی را که ارائه نام‌نویسی و استفاده از خدمات مرتبط با نام‌نویسی تحت آن ارائه می‌شوند، مشخص کند. شرایط خدمات مرتبط با نام‌نویسی ممکن است مطابق یک چارچوب اعتماد برقرار شوند. در مواردی که مناسب باشد، پیش از ادامه فرآیند نام‌نویسی ادعاهای سلب مسؤولیت[1] یا سایر شرایط[2] حقوقی توسط هستار، یا از طرف آن، پذیرفته می‌شوند.

۸-۱-۲ اثبات هویت و درستی‌سنجی اطلاعات هویت

اثبات هویت فرآیند جمع‌آوری و بررسی اطلاعات کافی جهت شناسایی یک هستار در یک سطح تضمین معین یا قابل درک است. درستی‌سنجی اطلاعات هویت فرآیندی بررسی اطلاعات هویت و اعتبارنامه‌ها در مقابل صادر کنندگان، منابع داده و سایر منابع داخلی و خارجی از حیث اصالت‌سنجی، اعتبار، صحت و ارتباط با هستار است. بسته به زمینه، طیف وسیعی از اطلاعات هویت (به عنوان مثال کارت‌های شناسایی دولتی، گواهینامه رانندگی، اطلاعات زیستی، گواهی‌های مبتنی بر افزاره[3]، گواهی تولد) از منابع معتبر می-

1 - Liability disclaimer
2 - Provision
3 - Machine-based certificate

توانند الزامات اثبات هویت را برآورده سازند. اطلاعات هویت اصلی که برای برآورده کردن الزامات اثبات هویت ارائه می‌شوند بسته به LoA متفاوت خواهد بود.

اثبات هویت ممکن است به منظور کشف تقلب، دستکاری یا جعل مستندات شامل بررسی فیزیکی مستندات هویت ارائه شده، شود. همچنین ممکن است اثبات هویت شامل انجام بررسی‌هایی شود تا اطمینان به دست آید که هویت در زمینه‌های دیگر نیز استفاده می‌شود (یعنی توسط RAهای دیگری تایید شده است). هر چه LoA بالاتر باشد الزامات اثبات هویت باید دقیق‌تر باشند. علاوه بر این، فرآیند اثبات هویت باید برای هستارهایی که از راه دور اظهارنامه یا ادعای هویت می‌کنند (به عنوان مثال از طریق کانال‌های بر خط) دقیق‌تر از هستارهای محلی (به عنوان مثال به صورت شخصی با RA) باشد.

دقت الزامات اثبات هویت بر مبنای اهدافی که باید برای هر LoA برآورده شوند، مشخص می‌شود. در LoA1 تنها هدف تضمین منحصر به فرد بودن هویت در زمینه مورد نظر است. به عبارت دیگر، هویت نباید به دو هستار مختلف نسبت داده شده باشد. در LoA2 دو هدف وجود دارد. اول، هویت باید در زمینه منحصر به فرد باشد. دوم، هستاری که هویت متعلق به آن است باید وجود عینی[1] داشته باشد، که به این معنا است که هویت ساختگی نیست یا از روی عمد برای اهداف جعلی ایجاد نشده است[2]. برای مثال، اثبات هویت انسان‌ها در LoA2 می‌تواند شامل بررسی تاریخ تولد و وفات شود تا نوعی اصالت تضمین شود (اگر چه این ثابت نمی‌کند که هستاری که گواهی تولد را در اختیار دارد همان هستاری است که گواهی تولد برای آن صادر شده است). به طور مشابه، اثبات هویت برای NPEها در LoA2 می‌تواند شامل بررسی شماره ردیف با تولید کننده شود.

LoA3 علاوه بر اهداف LoA1 و LoA2، شامل هدف وارسی اطلاعات هویت از طریق یک یا چند منبع معتبر، مانند پایگاه‌داده‌های خارجی، می‌شود. درستی‌سنجی اطلاعات هویت نشان می‌دهد که هویت در حال استفاده است و به هستار پیوند می‌خورد. با این وجود، تضمینی وجود ندارد که اطلاعات هویت در تملک صاحب واقعی و مشروع هویت است. در مورد انسان‌ها، LoA4 یک هدف دیگر به LoA3 اضافه می‌کند و آن این است که از هستارها می‌خواهد به صورت حضوری شهادت دهند تا به مقابله با جعل هویت کمک شود.

فرآیندهای اثبات هویت در LoA بالاتر باید شامل فرآیندهای LoAهای پایین‌تر شود. برای مثال، اثبات هویت LoA3 فرض می‌کند که کنترل‌های اثبات هویت LoA1 و LoA2 برآورده شده‌اند.

1- Objectively

۲- این هدف مانع استفاده از اسم‌های مستعار نمی‌شود.

جدول۳- اعمال اهداف اثبات هویت به LoAها

LoA	توصیف	هدف	کنترل‌ها	روش پردازش[a]
LoA1- پایین	اطمینان در مورد هویت اظهارنامه یا ادعا شده ناچیز است یا اصلا وجود ندارد	هویت در زمینه منحصر به فرد است	خود ادعا[b]، خود اظهارنامه[c]	محلی یا راه دور
LoA2– متوسط	تا حدودی در مورد هویت اظهارنامه یا ادعا شده اطمینان وجود دارد	هویت در زمینه منحصر به فرد است و هستاری که هویت متعلق به آن است وجود عینی دارد	اثبات هویت از طریق استفاده از اطلاعات هویت از یک منبع معتبر	محلی یا راه دور
LoA3– بالا	اطمینان بالایی در مورد هویت اظهارنامه یا ادعا شده وجود دارد.	هویت در زمینه منحصر به فرد است، هستاری که هویت متعلق به آن است وجود عینی دارد، هویت تایید می‌شود و هویت در زمینه‌های دیگر استفاده می‌شود	اثبات هویت از طریق استفاده از اطلاعات هویت از یک منبع معتبر + درستی‌سنجی اطلاعات هویت	محلی یا راه دور
LoA4– خیلی بالا	اطمینان بسیار بالایی در مورد هویت اظهارنامه یا ادعا شده وجود دارد.	هویت در زمینه منحصر به فرد است، هستاری که هویت متعلق به آن است وجود عینی دارد، هویت تایید می‌شود و هویت در زمینه‌های دیگر استفاده می‌شود	اثبات هویت از طریق استفاده از اطلاعات هویت از یک منبع معتبر + درستی‌سنجی اطلاعات هویت + شهادت هستار به صورت حضوری[d]	فقط محلی

[a] اثبات هویت راه دور بر روی شبکه انجام می‌شود و در نتیجه امکان دیدن هستار به صورت فیزیکی میسر نیست در حالیکه اثبات هویت محلی به نحوی انجام می‌شود که مستلزم دیدن هستار به صورت فیزیکی است.

[b] Self-claimed

[c] Self-asserted

[d] کنترل شهادت حضوری فقط در مورد هستارهای انسانی اعمال می‌شود.

اثر مرحله نام‌نویسی بر LoA باید با استفاده از کنترل‌های فهرست شده در بند ۱۰-۱-۲ معین شود.

هر گونه پیاده‌سازی EAAF به (زیرمجموعه‌ای) اطلاعات هویت و منابعی که در اختیار RA یا هستارهای احتمالی قرار دارند، وابسته است.

قابلیت اطمینان و دقت این اعتبارنامه‌ها، اطلاعات هویت و منابع تضمین واقعی فراهم شده از طریق مرحله نام‌نویسی را مشخص می‌کنند. در نتیجه، پیاده‌سازان EAAF باید هنگام تصمیم‌گیری در مورد اعتبارنامه‌ها، اطلاعات هویت و منابعی که برای اهداف اثبات هویت و درستی‌سنجی اطلاعات هویت به آن‌ها اعتماد می‌کنند، با دقت تضمین فراهم شده توسط زیرساخت‌های (مدیریت) هویت که توسط منابع و صادرکنندگان استفاده می‌شوند را در نظر بگیرند. هر گونه پیاده‌سازیEAAF باید شامل انتشار مستندات (به عنوان مثال خط‌مشی اثبات هویت که در بند ۱۰-۱-۲-۱ توصیف می‌شود) باشد که دید اجمالی از اطلاعات هویت، منابع و صادرکنندگانی که برای پشتیبانی از مرحله نام‌نویسی به آن‌ها اعتماد شده است ارائه می‌کند.

۸-۱-۳ نگهداری رکورد/ثبت

این فرآیند پایانی نام‌نویسی یک هستار است. فرآیند نگهداری رکورد از مرحله نام‌نویسی است که در آن، رکورد از نام‌نویسی ایجاد می‌شود. این رکورد باید شامل اطلاعات و مستنداتی که جمع‌آوری شده‌اند (و می‌توانند نگهداری شوند)، اطلاعات مربوط به فرآیند درستی‌سنجی اطلاعات هویت، نتایج این گام‌ها و سایر داده‌های مرتبط شود. سپس در مورد قبول کردن، رد کردن یا ارجاع نام‌نویسی برای بررسی‌های بیشتر یا سایر پیگیری‌ها تصمیم گرفته شده و ثبت می‌شود.

۸-۱-۴ ثبت‌نام

ثبت‌نام فرآیندی است که در آن یک هویت برای استفاده از خدمات یا منابع درخواست ارائه می‌کند. با وجود اینکه فرآیند ثبت‌نام به طور عمومی به عنوان بخشی از فرآیند نام‌نویسی در نظر گرفته می‌شود، به طوری که در پایان مرحله نام‌نویسی انجام می‌شود، ممکن است در زمانی دیگر نیز اجرا شود. برخلاف سایر فرآیندها در نام‌نویسی که به طور احتمالی تنها یک بار لازم خواهند بود، ثبت‌نام ممکن است هر بار که هستاری برای اولین بار درخواست دسترسی به خدمت یا منبعی را ارائه می‌کند لازم باشد.

۸-۲ مرحله مدیریت اعتبارنامه

مرحله مدیریت اعتبارنامه شامل تمامی فرآیندهای مرتبط با چرخه عمر مدیریت یک اعتبارنامه، یا ابزار تولید اعتبارنامه، است که به کاربر امکان مشارکت در یک فعالیت یا زمینه را می‌دهد. مرحله مدیریت اعتبارنامه ممکن است شامل برخی یا تمامی فرآیندهای زیر شود: تولید اعتبارنامه‌ها، صدور اعتبارنامه‌ها یا ابزار تولید اعتبارنامه‌ها، فعال‌سازی اعتبارنامه‌ها یا ابزار تولید اعتبارنامه‌ها، ذخیره‌سازی اعتبارنامه‌ها، ابطال[1] و انهدام اعتبارنامه‌ها یا ابزار تولید اعتبارنامه‌ها، تجدید و جایگزینی اعتبارنامه‌ها یا ابزار تولید اعتبارنامه‌ها و نگهداری رکورد. برخی از این فرآیندها به این بستگی دارند که اعتبارنامه برای یک افزاره سخت‌افزاری یا هستار دیگری صادر شده باشد.

1 - Revocation

۸-۲-۱ ایجاد اعتبارنامه

فرآیند ایجاد اعتبارنامه، تمامی فرآیندهای لازم برای ایجاد یک اعتبارنامه، یا ابزار تولید اعتبارنامه را، برای اولین بار شامل می‌شود. این فرآیندها ممکن است شامل پیش-پردازش، مقداردهی اولیه و انقیاد شود.

۸-۲-۲ پیش-پردازش اعتبارنامه

برخی اعتبارنامه‌ها، یا ابزار تولید اعتبارنامه‌ها، قبل از صدور به پیش پردازش نیاز دارند، مانند شخصی‌سازی[1] که در آن یک اعتبارنامه مطابق با هویت هستار سفارشی‌سازی می‌شود. شخصی‌سازی بسته به اعتبارنامه می‌تواند اشکال مختلفی بگیرد. به عنوان نمونه، شخصی‌سازی یک کارت هوشمند که اعتبارنامه‌ها در آن ذخیره شده‌اند می تواند شامل چاپ (بر روی سطح خارجی کارت) و نوشتن (بر روی تراشه کارت) نام هستاری که کارت برای آن صادر می‌شود باشد. اعتبارنامه‌هایی نیز وجود دارند که به شخصی‌سازی نیاز ندارند، مانند اسم رمزها.

۸-۲-۲-۱ مقداردهی اولیه اعتبارنامه[2]

مقداردهی اولیه شامل تمامی مراحلی است که تضمین می‌کنند یک روش تولید اعتبارنامه در ادامه قادر به پشتیبانی کارکردهای مورد انتظار از اعتبارنامه است. به عنوان نمونه، یک کارت هوشمند ممکن است لازم باشد جفت کلید رمزنگاشتی لازم برای پشتیبانی تولید امضای رقمی در آینده را محاسبه کند. به طور مشابه، کارت هوشمند ممکن است در حالت «قفل شده» صادر شود و در حین فرآیند فعال‌سازی به یک PIN نیاز داشته باشد.

۸-۲-۲-۲ انقیاد اعتبارنامه

انقیاد، فرآیند برقراری همبستگی میان یک اعتبارنامه، یا ابزار تهیه اعتبارنامه و هستاری که برای آن صادر می‌شود، است. نحوه انجام انقیاد و اعتماد به همبستگی انقیاد با توجه به LoA متفاوت خواهد بود. به عنوان نمونه، در یک فرانامه‌ی بر خط جهت انقیاد شناسانه مستعار ماندگار هستار به رکورد مشتری هستار، «کد فعال‌سازی» مراجعه اول می‌تواند در فرآیند انقیاد از طریق یک کوکی[3] رمزبندی شده ویژه نشست بر روی یک کانال امن حمل شود. ممکن است به طور متناوب، در پایان فرآیند هنگامی که مرحله انقیاد هستار به شناسانه مداوم کامل شده است، کد فعال‌سازی به منظور انقیاد شناسانه ماندگار به رکورد مشتری خواسته شود.

۸-۲-۳ صدور اعتبارنامه

صدور اعتبارنامه فرآیند ارائه یا به عبارتی دیگر ارتباط یک هستار با یک اعتبارنامه خاص، یا ابزار تولید اعتبارنامه، است. پیچیدگی این فرآیند بسته به LoA مورد نیاز متفاوت است. برای LoAهای بالاتر، این

1- Personalization
2 - Credential initialization
3 - Cookie

ممکن است شامل تحویل حضوری یک افزاره سخت‌افزاری (به عنوان مثال کارت هوشمند) دارای اعتبارنامه شود. در مورد LoAهای پایین‌تر فرآیند تضمین ممکن است به سادگی ارسال یک اسم رمز یا PIN به آدرس پست فیزیکی یا الکترونیکی هستار باشد.

برای NPEها، مانند افزاره‌ها، فرآیندهای صدور در LoAهای بالاتر به طور معمول هنگامی آغاز می‌شوند که تولید کننده افزاره با ارائه فهرستی از شماره‌های شناسایی منحصر به فرد افزاره‌ها به یک ارائه کننده خدمات اعتبارنامه (CSP) برای هر افزاره به صورت یکجا سفارش گواهینامه رقمی می‌دهد. CSP با آماده کردن گواهینامه و کلیدهای خصوصی در قالب رمزبندی شده، به تولید کننده پاسخ می‌دهد. تولید کننده ممکن است در حین فرآیند تولید، یک گواهینامه رقمی در هر افزاره تعبیه کند که یک شناسانه افزاره منحصر به فرد ایجاد می‌کند.

۸-۲-۴ فعال‌سازی اعتبارنامه

فعال‌سازی اعتبارنامه فرآیندی است که در آن یک اعتبارنامه، یا ابزار تولید اعتبارنامه، آماده استفاده می‌شود. بسته به اعتبارنامه، فرآیند فعال سازی ممکن است شامل اقدامات متنوعی شود. به عنوان نمونه، یک اعتبارنامه، یا ابزار تولید اعتبارنامه، ممکن است بعد از مقداردهی اولیه جهت جلوگیری از سوء استفاده موقتی تا زمان صدور برای هستار «قفل» شده باشد. در چنین مواردی، فعال‌سازی می‌تواند شامل «باز کردن» اعتبارنامه شود (به عنوان مثال استفاده از یک اسم رمز). یک اعتبارنامه، یا ابزار تولید اعتبارنامه، همچنین می‌تواند بعد از تعلیق شدن، که اعتبار آن به صورت موقت متوقف می‌شود، فعال‌سازی شود.

۸-۲-۵ ذخیره‌سازی اعتبارنامه

ذخیره‌سازی اعتبارنامه فرآیندی است که در آن اعتبارنامه‌ها، یا ابزار تولید اعتبارنامه‌ها، به صورت امن ذخیره می شوند به نحوی که در برابر دسترسی غیرمجاز، انتشار، استفاده، تغییر، یا انهدام محافظت شوند. ذخیره‌سازی اعتبارنامه شامل هستار مرتبط با یک اعتبارنامه و اقدامات لازم برای جلوگیری از استفاده غیرمجاز از اعتبارنامه می‌شود.

اگر اطلاعات استفاده شده برای بررسی درست بودن اعتبارنامه بخشی از خود اعتبارنامه نباشند، ذخیره‌سازی اعتبارنامه به طور الزامی شامل محافظت از آن اطلاعات نمی‌شود. محافظت از اطلاعات، مانند جدول‌های اسم رمزهای درهم‌سازی شده مورد نیاز برای اصالت‌سنجی، در LoAهای بالاتر الزامی هستند.

۸-۲-۶ تعلیق، ابطال و / یا انهدام[1] اعتبارنامه

ابطال فرآیندی است که در آن اعتبار یک اعتبارنامه به صورت دائم خاتمه می‌یابد. تعلیق یک فرآیند وابسته است که در آن اعتبار یک اعتبارنامه به صورت موقت خاتمه می‌یابد. ابطال در موارد مختلفی ممکن است مناسب باشد. ابطال در موارد زیر باید صورت گیرد:

1- Destruction

الف- اعلام شود که یک اعتبارنامه، یا ابزار تولید اعتبارنامه، مفقود یا دزدیده شده است یا به هر نحو دیگری در معرض خطر است؛

ب-اعتبار یک اعتبارنامه به پایان رسیده باشد؛

پ- مبنای اعتبارنامه دیگر وجود نداشته باشد (به عنوان مثال هنگامی که کارمندی کارفرمای خود را ترک می‌کند)؛

ت-یک اعتبارنامه برای اهداف غیرمجاز استفاده شده باشد؛

ث-یک اعتبارنامه دیگر برای جایگزین کردن اعتبارنامه مورد بحث صادر شده باشد.

چارچوب زمانی میان اطلاع از رویدادی که نیازمند ابطال است و پایان یافتن فرآیند ابطال توسط خط‌مشی سازمانی معین می‌شود. در LoAهای بالاتر، چارچوب زمانی مجاز برای ابطال به طور معمول کوتاه‌تر است. برخی اعتبارنامه‌ها، مانند آن‌هایی که بر روی کارت‌های هوشمند نگهداری می‌شوند، می‌توانند هنگام ابطال به صورت فیزیکی منهدم شوند. با این وجود، اطلاعات مرتبط با اعتبارنامه همیشه قابل انهدام نیست.

۸-۲-۷ تجدید و / یا جایگزینی اعتبارنامه

تجدید فرآیندی است که در آن عمر یک اعتبارنامه موجود تمدید می‌شود. جایگزینی فرآیندی است که در آن برای یک هستار اعتبارنامه، یا ابزار تولید اعتبارنامه، جدید صادر می‌شود تا جایگزین اعتبارنامه‌ای باشد که در قبل صادر شده بوده و ابطال شده است. مثالی از جایگزینی اعتبارنامه هنگامی است که یک CSP یک اسم رمز موقت برای آدرس رایانامه هستار ارسال می‌کند که به هستار امکان می‌دهد بعد از ارائه اسم رمز موقت یک اسم رمز جدید تعریف کند. مثالی دیگر کد فعال‌سازی PIN است که توصیه می‌شود همانند یک PIN با آن برخورد شود. سخت‌گیری فرآیندهای تجدید و جایگزینی اعتبارنامه‌ها بسته به LoA متفاوت خواهد بود.

۸-۲-۸ نگهداری رکورد

در چرخه عمر اعتبارنامه باید رکوردهای مناسب از آن را نگهداری کرد. در حالت کمینه، باید رکوردهایی را برای مستندسازی اطلاعات زیر نگهداری کرد:

الف. این حقیقت که یک اعتبارنامه ایجاد شده است؛

ب-شناسانه اعتبارنامه (هر جا که ممکن باشد)؛

پ- هستاری که اعتبارنامه برای آن صادر شده است (هر جا که ممکن باشد)؛ و

ت-وضعیت اعتبارنامه (هر جا که ممکن باشد).

باید برای هر یک از فرآیندهای درگیر در مرحله مدیریت اعتبارنامه رکوردی نگهداری کـرد. در مـواردی کـه اعتبارنامه‌ها برای انسان‌ها صادر می‌شوند، نگهداری رکورد به طور احتمالی شامل پردازش PII خواهد شد. بـه پیوست الف مراجعه شود.

۸-۳ مرحله اصالت‌سنجی هستار

در مرحله اصالت‌سنجی هستار، هستار از اعتبارنامه‌هایش برای شهادت دادن در مورد هویت خود نزد یک RP استفاده می‌کند. فرآیند اصالت‌سنجی تنها به برپایی (یا عدم برپایی) اعتماد به ادعا یا اظهارنامه هویـت مـی-پردازد و با اقداماتی که طرف اعتماد کننده ممکن است بر اساس ادعا یـا اظهارنامـه انجـام دهـد هـیچ گونـه جهت‌گیری یا ارتباطی ندارد.

۸-۳-۱ اصالت‌سنجی

فرآیند اصالت‌سنجی شامل استفاده از یک قرارداد برای نمایش در اختیار داشتن یا کنترل بر یـک اعتبارنامـه به منظور برپایی اعتماد به هویت، است. الزامات قرارداد اصالت‌سنجی بسته به LoA مناسـب متفـاوت اسـت. برای مثال، برای LoA پایین اصـالت‌سـنجی مـی‌توانـد شـامل اسـتفاده از اسـم رمـز باشـد. در LoA بـالاتر اصالت‌سنجی می‌تواند شامل استفاده از قرارداد چالش-پاسخ مبتنی بر رمزنگاشتی باشد. اصالت‌سـنجی چنـد عامله در LoAهای بالا الزامی است. همه عامل‌های اصالت‌سنجی قدرت یکسانی فراهم نمی‌کنند و از چندین عامل استفاده می‌شود تا تضمین را افزایش دهد. به بند ۱۰ مراجعه شود.

۸-۳-۲ نگهداری رکورد

پایش و نگهداری رکورد رویدادهای مرحله اصالت‌سنجی ممکن است برای اهداف متنـوعی لازم باشـد ماننـد تدارک خدمت، انطباق، پاسخ‌گویی و الزامات قانونی.

در موارد مربوط به هستارهای انسانی، اطلاعات نگهداری شده در این رکوردها می‌تواند شامل اطلاعات حساس باشد. این رکوردها باید به نحوی مدیریت شوند که نیاز به محافظت از PII و به کمینه کردن آن در نظر گرفته شده باشد.

۹ ملاحظات مدیریتی و سازمانی

EAA تنها از عوامل فنی نشات نگرفته است بلکه شامل مقررات، توافق‌های قـراردادی و ملاحظـات در مـورد نحوه مدیریت و سازمان‌دهی تدارک خدمت نیز می‌شود. یک راه‌حـل فنـی سـخت بـدون مـدیریت و اجـرای شایسته می‌تواند در هدف بالقوه خود برای فراهم کردن امنیت در تدارک EAA ناکام بماند.

این بند حاوی اطلاعات مفیدی است که ملاحظات سازمانی و مدیریتی که بر EAA اثر می‌گذارنـد، توصـیف می‌کند. در اینجا معیارهای خاص برای هر LoA ارائه نمی‌شود. معیـارهـای خـاص و ارزیـابی متابعـت بـرای ملاحظات مدیریتی و سازمانی خارج از محدوده این اسـتاندارد ملـی هسـتند، امـا توصـیه مـی‌شـود در یـک چارچوب اعتماد ارائه شوند.

۹-۱ استقرار خدمت

استقرار خدمت وضعیت قانونی ارائه دهنده خدمت و وضعیت تدارک خدمت کارکردی را مورد بررسی قرار می‌دهد. به عنوان نمونه، آگاهی از این موضوع که ارائه کننده خدمات مدیریت هویت و اصالت‌سنجی یک هستار ثبت شده قانونی است این اطمینان را به وجود می‌آورد که CSP در حوزه‌ای که فعالیت می‌کند سازمان صالحی است. این موضوع زمانی اهمیت بیشتری پیدا می‌کند که مولفه‌های خدمت توسط هستارهای قانونی متفاوت اجرا می‌شوند (به عنوان مثال، ثبت نام به عنوان کارکردی مجزا صورت می‌گیرد).

هر چند الزامات پایه برای تمامی LoAها یکسان هستند، توصیه می‌شود LoAهای بالاتر به کامل و قابل اعتماد بودن تدارک خدمت وابستگی بیشتری داشته باشند. به عنوان نمونه، در LoA3 و بالاتر، توصیه می‌شود از دانش در مورد روابط شرکتی خدمت و درک میزان استقلال در انجام عملیات برای رسیدن به تضمین بالاتر در تدارک خدمت استفاده شود.

۹-۲ انطباق قانونی و قراردادی

توصیه می‌شود تمامی اشخاص EAAF هر گونه الزام قانونی را که در ارتباط با اجرا و تحویل خدمت بر عهده آن‌ها قرار داده شده است، درک کرده و آن‌ها را برآورده کنند. این توصیه بر نوع اطلاعاتی که ممکن است جستجو شوند، نحوه انجام اثبات هویت و اطلاعاتی که ممکن است نگهداری شوند دلالت دارد، اما به این ها محدود نیست. ساماندهی PII یک نگرانی قانونی خاص است (به پیوست الف مراجعه شود). توصیه می‌شود به تمامی حوزه‌های اختیاراتی که اشخاص در آن فعالیت می‌کنند، توجه شود. در LoA2 و بالاتر، توصیه می‌شود الزامات قراردادی و خط‌مشی خاص شناسایی شوند.

۹-۳ شرایط مالی

در مواردی که دسترس‌پذیری طولانی مدت خدمات، یک ملاحظه در انتظارات هستار و طرف اعتماد کننده است توصیه می‌شود نشان داده شود که ثبات مالی برای تضمین اجرای پیوسته خدمت و پذیرش درجه مسؤولیت در قبال افشا خدمت وجود دارد. بعید است برای خدمات و اعتماد LoA1، چنین شرایطی در نظر گرفته شوند، در حالی که توصیه می‌شود خدماتی که تراکنش‌های با اهمیت‌تری در LoA2 و بالاتر را پشتیبانی می‌کنند چنین نیازهایی را در نظر بگیرند.

۹-۴ مدیریت و ممیزی امنیت اطلاعات

در LoA2 و بالاتر، توصیه می‌شود اشخاص EAAF در جایگاه خود شیوه‌های مدیریت امنیت اطلاعات، خط‌مشی‌ها، رویکردهای مدیریت مخاطره و سایر کنترل‌های شناخته شده را مستند کرده باشند تا تضمین کند که شیوه‌ها در جایگاه خود اثربخشی دارند. برای LoA3 و بالاتر توصیه می‌شود از یک سامانه مدیریت امنیت اطلاعات رسمی (به عنوان مثال مجموعه استانداردهای ISO/IEC 27000) استفاده شود.

بسته به توافقات در مورد انطباق قانونی، قراردادی و فنی توصیه می‌شود اشخاص تضمین کنند که طرفین به تعهدات خود پایبند هستند و در صورتی که پایبند نباشند می‌توانند راهی برای جبران خسارت فراهم کنند.

در LoA2 و بالاتر، توصیه می‌شود این تضمین با ممیزی‌های امنیتی، هم داخلی و هم خارجی و نگهداری امن رکوردهایی از رویدادهای مهم، از جمله ممیزی‌های امنیتی، پشتیبانی شود. ممیزی می‌تواند برای بررسی اینکه رویه‌های طرفین در محدوده توافقات انجام شده قرار دارند استفاده شود. در مورد اختلاف نظر می‌توان از خدمات حل اختلاف[1] استفاده کرد.

۹-۵ مولفه‌های خدمات خارجی

هنگامی که یک سازمان برای بخشی از خدمات خود به طرف‌های سوم وابسته است، نحوه مدیریت و نظارت بر اقدامات آن‌ها، در تضمین کلی تدارک خدمت نقش دارد. توصیه می‌شود ماهیت و حوزه توافقات متناسب با LoA مورد نیاز و سامانه مدیریت امنیت اطلاعات اعمال شده باشد. در LoA1، توصیه می‌شود چنین تضمینی اثر کمینه داشته باشد، اما از LoA2 به بالا این اقدامات در تضمین کلی داده شده نقش دارند.

۹-۶ زیرساخت عملیاتی

برای فراهم کردن شبکه‌های اعتماد مقیاس وسیع می‌توان از چارچوب اعتماد استفاده کرد. در چارچوب اعتماد، اشخاص جریان اطلاعات میان یکدیگر را پشتیبانی می‌کنند. بسته به توافقات، برای تضمین اینکه همه اشخاص به تعهدات پایبند هستند می‌توان از اشخاص اضافی استفاده کرد و آن‌ها می‌توانند راهی برای جبران خسارت در صورت عدم پایبندی به تعهدات فراهم کنند.

۹-۷ سنجش قابلیت‌های عملیاتی

تعیین کنندگان خط‌مشی، الزامات فنی و قراردادی برای چارچوب‌های اعتماد را مشخص می‌کنند. الزامات فنی ممکن است شامل سطح نسخه محصولات[2]، پیکربندی، تنظیمات و قراردادهای سامانه شود در حالی که الزامات قراردادی ممکن است به سمت رویه‌های اطلاعات منصفانه[3] جهت‌گیری داشته باشند. همزمان با استقرار این الزامات، توصیه می‌شود خط‌مشی سازان معیارهایی برای سنجش هستارهای احتمالی چارچوب اعتماد در نظر بگیرند. خط‌مشی سازان ممکن است به جای ایجاد معیارها، تمایل داشته باشند از معیارهای استاندارد که متخصصین ساخته‌اند، مانند این استاندارد ملی، استفاده کنند. هر چه خط‌مشی سازان از معیارهای استاندارد در چارچوب‌های اعتماد مختلف بیشتر استفاده کنند درک و اعمال بدون تناقض معیارها برای هستارها آسان‌تر خواهد بود. علاوه بر این، مجموعه‌های مشخصی از معیارها می‌توانند به عنوان مختصر نویسی برای نشان دادن درجات یا انواع مختلفی از سختگیری در الزامات یا قابلیت‌ها در LoAهای مختلف به کار روند.

۱۰ تهدیدها و کنترل‌ها

این بند تهدیدهای مرتبط با هر یک از مرحله‌های EAAF را توصیف و کنترل‌های لازم برای هر LoA را ارائه می‌کند.

---

1 - Dispute resolution services
2 - Product version levels
3 - Fair information practices

۱۰-۱ تهدیدها و کنترل‌های مرحله نام‌نویسی

۱۰-۱-۱ تهدیدهای مرحله نام‌نویسی

جدول ۴ تهدیدهای مرتبط با مرحله نام‌نویسی را شناسایی و توصیف می‌کند.

جدول ۴- تهدیدها در مرحله نام‌نویسی

تهدید	مثال
جعل هویت	جعل هویت زمانی است که یک هستار به صورت غیرقانونی از اطلاعات هویت هستار دیگری استفاده می‌کند، به عنوان مثال استفاده از گواهینامه رانندگی جعلی توصیف کننده فردی که وجود ندارد یا هنگامی که یک افزاره با استفاده از یک آدرس کنترل دسترسی رسانه (MAC) جعلی در یک شبکه ثبت نام می‌کند.

۱۰-۱-۲ کنترل‌های LoA مورد نیاز برای محافظت در برابر تهدیدهای مرحله نام‌نویسی

جدول ۵ کنترل‌های مورد نیاز برای مرحله نام‌نویسی را مطابق با LoA شناسایی می‌کند.

جدول۵-کنترل‌های مرحله نام‌نویسی برای هر LoA

تهدیدها	کنترل‌ها	کنترل‌های مورد نیاز			
		LoA1	LoA2	LoA3	LoA4
جعل هویت	اثبات هویت: تبعیت از خط‌مشی	#1	#1	#1	#1
	اثبات هویت: حضور شخصی	#2	-	-	-
	اثبات هویت: اطلاعات معتبر	#6	#5	#4	#3

یادآوری –در جدول بالا، شناسانه‌های #1-#6به کنترل‌های خاص مورد نیاز جهت فراهم کردن محافظت در هر LoA اشاره می‌کنند. هر یک از این کنترل‌ها به صورت دقیق در ۱۰-۱-۲-۱ توصیف می‌شوند. خانه‌هایی از جدول که علامت «–» در آن‌ها درج شده است نشان می‌دهند که کنترل مربوطه در LoA نشان داده شده کاربرد پذیر نیست.

۱۰-۱-۲-۱ کنترل‌های محافظت در برابر تهدیدهای مرحله نام‌نویسی

کنترل‌های زیر در برابر تهدیدهای مرحله نام‌نویسی متناظر با #1-#6 در جدول ۵ هستند.

IdentityProofing: PolicyAdherence

#1. خط‌مشی اثبات هویت را منتشر کنید و تمامی اثبات هویت را بر طبق خط‌مشی اثبات هویت منتشر شده انجام دهید.

IdentityProofing: InPerson

#2. باید برای انسان‌ها از اثبات هویت شخصی استفاده شود.

IdentityProofing: AuthoritativeInformation

#3. اطلاعات هویت می‌تواند توسط خود هستار ادعا یا اظهارنامه شده باشد.

#4. کنترل‌های زیر قابل اجرا هستند:

- تمامی کنترل‌ها از #3

علاوه بر آن:

- هستار باید اطلاعات هویت را حداقل از یک منبع معتبر اطلاعات هویت مطیع خط‌مشی ارائه کند.

الف- برای انسان‌ها:

۱- حضوری:

- تضمین شود که هستار یک مستند شناسایی از حداقل یک منبع معتبر مطیع خط‌مشی در اختیار دارد که شامل عکسی از مالک مستند است که با ظاهر هستار مطابقت دارد؛
- تضمین شود که مستند شناسایی ارائه شده مستند اصل است که به درستی صادر شده و در زمان درخواست معتبر است.

۲- غیر حضوری:

- هستار باید مدارکی ارائه کند که او اطلاعت هویت فردی مطیع خط‌مشی را در اختیار دارد. (نمونه-هایی از اطلاعات هویت قابل قبول می‌توانند شامل گواهینامه رانندگی و گذرنامه باشند)؛
- وجود و اعتبار مدارک ارائه شده باید از نظر مطابقت با الزامات خط‌مشی تایید شوند.

ب- برای NPEها:

- اطلاعات رکورد ارائه شده، مانند توصیف اسم مشترک، شماره ردیف، آدرس MAC، مالک، مکان، سازنده و غیره، از یک منبع معتبر اطلاعات هویت.

#5. کنترل‌های زیر قابل اجرا هستند:

- تمامی کنترل‌ها از #4.

علاوه بر آن:

الف. برای انسان‌ها:

۱- حضوری:

- از اطلاعات تماس لیست شده در مستند شناسایی برای تماس با هستار به منظور وارسی صحت آن‌ها استفاده شود؛
- حداقل یکی از مستندات شناسایی (به عنوان مثال مستند گواهی تولد، ازدواج، یا مهاجرت) در برابر دفاتر منابع معتبر مربوط وارسی شود؛
- اطلاعات شخصی در برابر منابع اطلاعات معتبر کاربرد پذیر و (در صورت امکان) منابعی از سایر زمینه‌ها تایید شوند به نحوی که برای تضمین هویت منحصر به فرد کافی باشد؛
- اطلاعاتی که هستار پیشتر ارائه کرده است یا به طور احتمالی فقط او از آن‌ها مطلع است وارسی شوند.

۲- غیر حضوری:

- بررسی ادعا/اظهارنامه هستار در مورد در اختیار داشتن یک اعتبارنامه LoA3 (یا بالاتر) از یک منبع معتبر توسط یک طرف سوم مورد اعتماد تضمین شود؛
- اطلاعاتی که هستار پیشتر ارائه کرده است یا به طور احتمالی فقط او از آن‌ها مطلع است وارسی شوند.

برای NPEها:

- در LoA3 باید از سخت‌افزارهای مورد اعتماد (به عنوان مثال TPM) استفاده شود؛
- در مورد NPEهایی که استفاده می‌شوند، NPE باید به صورت فیزیکی با استفاده از یک اعتبارنامه LoA3 صادر شده توسط انسان نزد یک افزاره RA نام‌نویسی شود.
- NPEهایی که هنوز تدارک دیده نشده‌اند باید با استفاده از اصالت‌سنجی انسان LoA3 یا امضای رقمی LoA3 سفارش داده شوند تا تایید شود که هستار مجاز به سفارش NPE است. RA سازنده باید NPE را ثبت نام کند، هر گونه سخت‌افزار مورد اعتماد را فعال سازد و صدور و شخصی‌سازی NPE را کنترل کند. سخت‌افزارهای مورد اعتماد هنگام اتصال
- به شبکه مقداردهی اولیه می‌شوند؛
- در مورد NPEهایی غیر از رایانه‌ها، اتصال میان افزاره، مالک، شبکه یا حامل ارتباط و RA باید به صورتی مشابه سخت‌افزار رایانه مورد اعتماد از طریق رمزنگاشتی ایمن سازی شوند؛

- در مواردی که از نرم‌افزار استفاده می‌شود، کد باید به صورت رقمی پیش از صدور به وسیله یک اعتبارنامه LoA3 صادر شده توسط انسان امضا شود و باید قبل از استفاده توسط RA به عنوان پذیرش اثبات مجددا امضا شود.

#6. کنترل‌های زیر قابل اجرا هستند:

- تمامی کنترل‌ها از #5.

علاوه بر آن:

الف. برای انسان‌ها:

- هستار باید حداقل از یک منبع معتبر مطیع خط‌مشی اضافی اطلاعات هویت ارائه کند.

ب- برای NPEها:

- افزاره‌های اضافی متصل به رایانه، تلفن هوشمند، یا پردازنده‌های مشابه باید هنگام صدور ضبط شوند و به صورت رمزنگاشتی شده به افزاره لنگر[1] (به عنوان مثال افزاره سخت‌افزار مورد اعتماد فعال شده، خواننده زیست‌سنجی[2]، کارت‌های هوشمند، تعیین کننده زمینی GPS[3]) متصل شوند.

- هر گونه تغییر در تنظیمات انقیاد بین افزاره‌ها باید از طریق RA مدیریت شود. در صورت امکان، توصیه می‌شود قابلیت مدیریت شبکه، RA یا مدیریت شبکه را از هر گونه تغییر در روابط افزاره‌ها مطلع سازد و اقدام اصلاحی انجام گیرد؛

- باید قابلیتی برای جلوگیری از کار کردن روابط تغییر داده شده افزاره‌ها وجود داشته باشد؛

- کد نرم‌افزار LoA4 باید به صورت رقمی توسط اعتبارنامه LoA4 صادر شده توسط انسان امضا شود و باید پیش از استفاده به عنوان اثبات پذیرش مجددا توسط RA امضا شود.

۱۰-۲ تهدیدها و کنترل‌های مرحله مدیریت اعتبارنامه

۱۰-۲-۱ تهدیدهای مدیریت اعتبارنامه

تهدیدهای مرتبط با مرحله مدیریت اعتبارنامه در جدول ۶ فهرست شده‌اند.

1- Anchor device
2- Biometric reader
3- GPS geo-authenticator

جدول۶- تهدیدهای مدیریت اعتبارنامه

تهدید	مثال
CredentialCreation: Tampering	مهاجم اطلاعات را هنگام گذر از فرآیند نام‌نویسی به فرآیند ایجاد اعتبارنامه دستکاری می‌کند.
CredentialCreation: UnauthorizedCreation	مهاجم باعث می‌شود CSP اعتبارنامه را بر اساس یک هستار جعلی ایجاد کند.
CredentialIssuance: Disclosure	اعتبارنامه تولید شده توسط CSP برای یک هستار هنگام انتقال از CSP به هستار در حین استقرار اعتبارنامه مورد حمله مهاجم قرار می‌گیرد.
CredentialActivation: Unauthorized Possession	مهاجم به اعتبارنامه‌ای دست پیدا می‌کند که متعلق به او نیست و از طریق جا زدن خود به عنوان هستار مشروع سبب می‌شود که CSP اعتبارنامه را فعال کند.
CredentialActivation: Unavailability	۱- هستار نسبت داده شده به اعتبارنامه، یا ابزار تولید اعتبارنامه، در مکان معمول خود نیست و قادر به اصالت‌سنجی خود به CSP به صورت مناسب نیست. ۲- تحویل اعتبارنامه، یا ابزار تولید اعتبارنامه، به تعویق افتاده است و فعالسازی در بازه زمانی از پیش تعیین شده امکان پذیر نیست.
CredentialStorage: Disclosure	اعتبارنامه‌های ذخیره شده در سامانه پرونده آشکار شده‌اند. به عنوان مثال، مهاجم به رکورد ذخیره شده از شناسانه کاربری و اسم رمزها دسترسی پیدا کرده است.
CredentialStorage: Tampering	به پرونده‌ای که شناسانه‌های کاربری را به اعتبارنامه‌ها نگاشت می‌دهد نفوذ شده است به صورتی که نگاشت‌ها تغییر داده شده‌اند و اعتبارنامه‌های موجود با اعتبارنامه‌هایی که مهاجم به آن‌ها دسترسی دارد جایگزین شده‌اند.
CredentialStorage: Duplication	مهاجم از اطلاعات ذخیره شده برای ایجاد اعتبارنامه تکراری استفاده می‌کند (به عنوان مثال، از طریق تکثیر کارت هوشمندی که می‌تواند اعتبارنامه تولید کند) که می‌توانند توسط هستار غیرمجاز استفاده شوند.
CredentialStorage: DisclosureByEntity	هستار یک رکورد نوشتاری از شناسانه کاربری و اسم رمز را در جایی که توسط دیگران قابل دسترس است نگه می‌دارد.
CredentialRevocation: DelayedRevocation	انتشار اطلاعات ابطال به موقع نیست که منجر به این تهدید می‌شود که هستارهایی که اعتبارنامه آن‌ها ابطال شده است تا هنگامیکه درستی‌سنج اعتبارنامه آخرین اطلاعات ابطال را دریافت نکرده است همچنان قادر به اصالت‌سنجی هستند.
CredentialRevocation: UseAfterDecommissioning	حساب‌های کاربری هنگامی که کارمند شرکت را ترک می‌کند حذف نمی‌شوند که منجر به سوء استفاده احتمالی افراد غیرمجاز از حساب‌های قدیمی می‌شود.
CredentialRenewal: Disclosure	اعتبارنامه تجدید شده توسط CSP برای یک هستار هنگام انتقال توسط مهاجم کپی برداری می‌شود.
CredentialRenewal: Tampering	اعتبارنامه جدید تولید شده توسط هستار هنگام ارسال به CSP جهت جایگزینی با اعتبارنامه منقضی شده توسط مهاجم تغییر داده می‌شود.
CredentialRenewal: UnauthorizedRenew	مهاجم قادر به سوء استفاده از یک قرارداد تجدید اعتبارنامه ضعیف برای تمدید مدت اعتبار اعتبارنامه برای یک هستار فعلی است. مهاجم CSP را به صدور اعتبارنامه جدید برای یک هستار فعلی فریب می‌دهد و اعتبارنامه جدید هویت هستار فعلی را به اعتبارنامه ارائه شده توسط مهاجم متصل

تهدید	مثال
	می‌سازد. برای هستارهای NPE، یک مثال می‌تواند برچسب‌زنی مجدد (صدور مجدد) یک مولفه سامانه (به عنوان مثال RAM) به عنوان مولفه جدید بعد از استفاده از آن باشد.
CredentialRecordkeeping: Repudiation	هستار به منظور اینکه به دروغ استفاده از اعتبارنامه را رد کند ادعا یا اظهارنامه می‌کند که یک اعتبارنامه مشروع جعلی است یا شامل اطلاعات غیر صحیحی می‌شود.

۱۰-۲-۲ کنترل‌های LoA لازم برای محافظت در برابر تهدیدهای مرحله مدیریت اعتبارنامه

کنترل‌های مورد نیاز در برابر تهدیدهای مدیریت اعتبارنامه بر طبق LoA در جدول ۷ مشخص شده‌اند.

جدول۷- کنترل‌های مدیریت اعتبارنامه برای هر LoA

تهدیدها	کنترل‌ها	کنترل‌های مورد نیاز			
		LoA1	**LoA2**	**LoA3**	**LoA4**
CredentialCreation: Tampering	AppropriateCredentialCreation	#1	#1	#2	#2
	HardwareOnly	-	-	-	-#3
	StateLocked	-	-	-	#4
CredentialCreation: UnauthorizedCreation	TrackedInventory	#5	#5	#5	#5
CredentialIssuance: Disclosure	AppropriateCredentialIssuance	#6	#7	#7	#8
CredentialActivation: UnauthorizedPossession CredentialActivation: Unavailability	ActivatedByEntity	#9	#9	#10	#11
CredentialStorage: Disclosure CredentialStorage: Tampering CredentialStorage: Duplication CredentialStorage: DisclosureByEntity	CredentialSecureStorage	#12	#13	#14	#15
CredentialRevocation: DelayedRevocation	CredentialSecureRevocation &Destruction	#16	#16	#16	#16

تهدیدها	کنترل‌ها	کنترل‌های مورد نیاز			
		LoA1	LoA2	LoA3	LoA4
CredentialRevocation: UseAfterDecommissioning					
CredentialRenewal: Disclosure CredentialRenewal: Tampering CredentialRenewal: UnauthorizedRenewal	CredentialSecureRenewal	#17	#17	#18	#19
CredentialRecordkeeping: Repudiation	RecordRetention	#20	#20	#21	#21

یادآوری – در جدول بالا، شناسانه‌های #1-#21 به کنترل‌های خاص مورد نیاز جهت فراهم کردن محافظت در هر **LoA** اشاره می‌کنند. هر یک از این کنترل‌ها به صورت دقیق در ۱۰-۲-۲-۱ توصیف می‌شوند. خانه‌هایی از جدول که علامت «–» در آن‌ها درج شده است نشان می‌دهند که کنترل مربوطه در LoA نشان داده شده کاربرد پذیر نیست.

۱۰-۲-۲-۱ کنترل‌ها در برابر تهدیدهای مرحله مدیریت اعتبارنامه

کنترل‌های زیر برای مقابله با تهدیدهای مرحله مدیریت اعتبارنامه با شماره‌های #1-#21 در جدول ۷ متناظر هستند.

AppropriateCredentialCreation

#1. کنترل‌های زیر قابل اجرا هستند:

- برای ایجاد اعتبارنامه‌ها باید از فرآیندهای رسمی و مستند شده استفاده کرد.
- پیش از نهایی کردن انقیاد اعتبارنامه به هستار، CSP باید تضمین کافی داشته باشد که اعتبارنامه به هستار درست متصل شده است و به همین هستار متصل باقی می‌ماند.

#2. کنترل‌های زیر قابل اجرا هستند:

- تمامی کنترل‌ها از #1.

علاوه بر آن:

- انقیاد اعتبارنامه باید با استفاده از یکی از رویکردهای زیر در برابر دستکاری محافظت شود:

الف- امضای رقمی

ب- سازوکار توصیف شده برای «وضعیت قفل شده» در مورد اعتبارنامه‌هایی که روی افزاره‌های سخت‌افزاری نگهداری می‌شوند.

HardwareOnly

#3. اعتبارنامه‌ها باید روی پودمان امنیت سخت‌افزاری[1] نگهداری شوند[2].

StateLocked

#4. اعتبارنامه‌هایی که روی افزاره سخت‌افزاری نگهداری می‌شوند باید در پایان فرآیند ایجاد در وضعیت قفل شده قرار داده شوند.

TrackedInventory

#5. اگر اعتبارنامه، یا ابزار ایجاد اعتبارنامه، روی افزاره سخت‌افزاری نگهداری می‌شود، افزاره سخت‌افزاری باید از لحاظ فیزیکی در محلی امن نگهداری شود و مخزن ردیابی شود. به عنوان مثال، توصیه می‌شود کارت‌های هوشمند غیرشخصی در محلی امن ذخیره شوند و شماره ردیف آن‌ها ضبط شود تا در برابر سرقت و تلاش-های متعاقب آن جهت ایجاد اعتبارنامه‌های غیرمجاز محافظت شود.

AppropriateCredentialIssuance

#6. برای صدور اعتبارنامه‌ها باید از فرآیندهای رسمی و مستند شده استفاده کرد.

#7. کنترل‌های زیر قابل اجرا هستند:

- تمامی کنترل‌ها از #6.

علاوه بر آن:

- فرآیند صدور باید شامل سازوکاری شود که تضمین کند اعتبارنامه به هستار درست یا یک نماینده مجاز ارائه شده است. اگر اعتبارنامه به صورت حضوری تحویل داده نشود، باید از سازوکاری برای بررسی وجود آدرس تحویل و ارتباط مشروع آن با هستار استفاده شود.

#8. کنترل‌های زیر قابل اجرا هستند:

- تمامی کنترل‌ها از #7.

علاوه بر آن:

1- Hardware security module

۲- حدود پودمان امنیت سخت‌افزاری در ISO/IEC 19790:2012 تعریف شده است.

- اگر اعتبارنامه به صورت حضوری تحویل داده نشود، آنگاه باید از طریق یک کانال امن تحویل داده شود و هستار یا نماینده مجاز آن باید رسید اعلام وصول اعتبارنامه را امضا کنند.

ActivatedByEntity

#9. رویه‌ای باید وجود داشته باشد که تضمین کند اعتبارنامه، یا ابزار تولید اعتبارنامه، تنها در صورتی فعال می‌شود که تحت کنترل هستار مورد نظر است. هیچ الزام خاصی برای این رویه وجود ندارد.

#10. رویه‌ای باید وجود داشته باشد که تضمین کند اعتبارنامه، یا ابزار تولید اعتبارنامه تنها در صورتی فعال می‌شود که تحت کنترل هستار مورد نظر است. این رویه باید ثابت کند که هستار به فعال‌سازی اعتبارنامه وصل است (به عنوان مثال، قرارداد چالش-پاسخ).

#11. رویه‌ای باید وجود داشته باشد که تضمین کند اعتبارنامه، یا ابزار تولید اعتبارنامه تنها در صورتی فعال می‌شود که تحت کنترل هستار مورد نظر است. این رویه باید:

الف- ثابت کند که هستار به فعال‌سازی اعتبارنامه وصل است (به عنوان مثال، قرارداد چالش-پاسخ)

ب- فعال‌سازی را فقط در یک بازه زمانی معین شده در خط‌مشی ممکن سازد.

CredentialSecureStorage

#12. کنترل‌های زیر قابل اجرا هستند:

- اعتبارنامه‌های مبتنی بر رازهای به اشتراک گذاشته شده باید توسط کنترل‌های دسترسی محافظت شوند که دسترسی را به مدیران و برنامه‌های کاربردی که به دسترسی نیاز دارند محدود می‌کنند.
- خط‌مشی محافظت برای اعتبارنامه‌های ذخیره شده باید در مستند مرتبط با استفاده از این اعتبارنامه‌ها که در اختیار هستارها قرار داده می‌شود مستند شود.

#13. کنترل‌های زیر قابل اجرا هستند:

- تمامی کنترل‌ها از #12.

علاوه بر آن:

- چنین پرونده‌های رازهای به اشتراک گذاشته شده‌ای نباید حاوی اسم رمز یا رازها به صورت متن ساده شوند؛ می‌توان از روش جایگزینی برای محافظت رازهای به اشتراک گذاشته شده استفاده کرد.

#14. کنترل‌های زیر قابل اجرا هستند:

- تمامی کنترل‌ها از 13#.

علاوه بر آن:

- رازهای به اشتراک گذاشته شده باید با کنترل‌های دسترسی محافظت شوند که دسترسی را به مدیران و برنامه‌های کاربردی که نیاز به دسترسی دارند، محدود می‌کنند. چنین رازهای به اشتراک گذاشته شده‌ای باید رمزنگاشتی شوند. کلید رمزبندی برای راز به اشتراک گذاشته شده، باید در یک پودمان رمزنگاشتی[1] (سخت‌افزار یا نرم‌افزار) رمزبندی و ذخیره‌سازی شوند. کلید رمزبندی راز به اشتراک گذاشته باید فقط برای عمل اصالت‌سنجی از رمز خارج شوند؛

- هستارها یا نماینده‌های مجاز آن‌ها باید تایید کنند که این الزامات را درک می‌کنند و موافقت کنند که مطابق با این الزامات از اعتبارنامه‌ها محافظت می‌کنند.

15#. کنترل‌های زیر قابل اجرا هستند:

- تمامی کنترل‌ها از 14#.

علاوه بر آن:

- هستارها یا نماینده مجاز آن‌ها باید مستندی را امضا کنند که اعلام می‌کند الزامات برای ذخیره اعتبارنامه‌ها را درک می‌کنند و می‌پذیرند که مطابق آن‌ها از اعتبارنامه‌ها محافظت کنند.

CredentialSecureRevocation&Destruction

16#. CSPها باید اعتبارنامه‌ها (از جمله آن‌هایی که بر اساس رازهای به اشتراک گذاشته شده هستند) را برای هر LoA در یک بازه زمانی معین که توسط خط‌مشی سازمان تعریف شده است باطال و (در صورت امکان) منهدم کنند.

CredentialSecureRenewal

17#. کنترل‌های زیر قابل اجرا هستند:

- CSP باید خط‌مشی‌های مناسبی برای تجدید و جایگزینی اعتبارنامه‌ها برقرار کند؛

- اثبات مالکیت اعتبارنامه فعلی منقضی نشده باید توسط هستار قبل از دادن اجازه تجدید یا جایگزینی از طرف CSP، ارائه شود؛

1- Cryptographic module

- اسم رمزها باید کمینه الزامات خط‌مشی CSP در مورد قدرت اسم رمز و استفاده مجدد از اسم رمز را برآورده کند؛
- بعد از منقضی شدن اعتبارنامه فعلی، تجدید نباید اجازه داده شود؛
- تمامی تعاملات باید بر روی یک کانال امن مانند SSL/TLS انجام شود.

#18. کنترل‌های زیر قابل اجرا هستند:

- تمامی کنترل‌ها از #17.

علاوه بر آن:

- انجام اثبات هویت LoA2 مطابق با ۱۰-۱-۲-۱ (اثبات هویت: تبعیت از خط‌مشی، اثبات هویت: اطلاعات معتبر).

#19. کنترل‌های زیر قابل اجرا هستند:

- تمامی کنترل‌ها از #17.

علاوه بر آن:

- انجام اثبات هویت LoA3 مطابق با ۱۰-۱-۲-۱ (اثبات هویت: تبعیت از خط‌مشی، اثبات هویت: اطلاعات معتبر).

RecordRetention

#20. باید رکوردی از ثبت نام، تاریخچه و وضعیت (از جمله ابطال) هر اعتبارنامه توسط CSP نگهداری شود. مدت نگهداری باید در خط‌مشی CSP معین شود.

#21. کنترل‌های زیر قابل اجرا هستند:

- تمامی کنترل‌ها از #20؛
- باید فرآیندهای رسمی و مستند شده برای زنجیره نگهداری هر رکورد تولید شود.

۱۰-۳ تهدیدها و کنترل‌های مرحله اصالت‌سنجی

۱۰-۳-۱ تهدیدهای مرحله اصالت‌سنجی

تهدیدهای مرحله اصالت‌سنجی شامل تهدیدهای مرتبط با استفاده از اعتبارنامه‌ها در حین اصالت‌سنجی و تهدیدهای عمومی اصالت‌سنجی می‌شود. تهدیدهای عمومی اصالت‌سنجی شامل نرم‌افزارهای مخرب[1] (به عنوان مثال ویروس‌ها، اسب تراوا[2]، رویداد نگارهای صفحه کلید[3])؛ مهندسی اجتماعی[4] (به عنوان مثال، نگاه دزدکی[5]، سرقت افزاره‌های سخت‌افزاری و شماره‌های شناسایی شخصی)؛ خطاهای کاربری (به عنوان مثال، اسم رمزهای ضعیف، ناتوانی در محافظت از اطلاعات اصالت‌سنجی)؛ انکار نادرست؛ استراق سمع یا تغییر داده‌های اصالت‌سنجی هنگام انتقال؛ منع خدمت[6]؛ و ضعف رویه‌ای می‌شود، هر چند به این موارد محدود نیست. کنترل‌ها برای تهدیدهای عمومی اصالت‌سنجی فراتر از محدوده این استاندارد هستند، به استثنای استفاده از اصالت‌سنجی چند عامله. این بند روی تهدیدهای مرتبط با استفاده از اعتبارنامه‌ها برای اصالت‌سنجی تمرکز می‌کند، آن‌ها را توصیف کرده و کنترل‌هایی را برای هر نوع تهدید مشخص می‌کند.

مشخص کردن کنترل‌های خاص در قالب LoA برای مرحله اصالت‌سنجی، به جز در مورد الزام استفاده از اصالت‌سنجی چندعامله در LoA3 و LoA4، درست نیست. برخی کنترل‌ها ممکن است برای تمامی زمینه‌ها مناسب نباشند. به عنوان مثال، کنترل‌های اصالت‌سنجی کاربرانی که به مجلات برخط دسترسی پیدا می‌کنند به طور احتمالی از کنترل‌های پزشکانی که به رکوردهای بیمار دسترسی پیدا می‌کنند متفاوت خواهد بود. از این رو، توصیه می‌شود با حادتر شدن مخاطره و پی‌آمد سوء استفاده، CSP امنیت را عمیق‌تر بررسی کند (یعنی، کنترل‌ها مناسب با محیط عملیاتی، برنامه کاربردی و LoA لایه‌بندی شوند). این موضوع بر عهده طراح سامانه است که بر اساس تحلیل مخاطره در مورد نحوه، زمان و ترکیب استفاده از این کنترل-ها تصمیم بگیرد.

خطرهای بسیاری اعتبارنامه‌هایی را که برای اصالت‌سنجی استفاده می‌شوند تهدید می‌کنند. در جدول ۸ برخی طبقه‌بندی‌های عمومی از تهدیدهای مطرح در خصوص استفاده از اعتبارنامه‌ها فهرست شده و مثال-های ویژه‌ای جهت نمایش این تهدیدها ارائه شده‌اند.

جدول ۸- خلاصه تهدیدها علیه استفاده از اعتبارنامه‌ها در مرحله اصالت‌سنجی

تهدید	توصیف و مثال
تهدیدهای عمومی	تهدیدهای عمومی اصالت‌سنجی شامل طبقه‌بندی‌های بسیاری از تهدیدهای امنیتی رایج برای هر نوع ICT می‌شوند. برخی مثال‌ها شامل ثبت کننده صفحه کلید، مهندسی اجتماعی و خطای کاربری می-شوند. کنترل‌های مقابله با این تهدیدها در خارج از محدوده این استاندارد هستند، به استثنای

1- Malicious software
2- Trojan
3- Keystroke loggers
4- Social engineering
5- Shoulder surfing
6- Denial of service

تهدید	توصیف و مثال
	اصالت‌سنجی چندعامله. توجه داشته باشید که اصالت‌سنجی چندعامله در برابر همه تهدیدهای عمومی احتمالی محافظت نمی‌کند.
حدس زدن برخط	مهاجم با حدس زدن مقادیر احتمالی اعتبارنامه تلاش‌های تکراری جهت ورود می‌کند.
حدس زدن برون‌خط	رازهای مرتبط با تولید اعتبارنامه با استفاده از روش‌های تحلیلی در خارج از تراکنش اصالت‌سنجی افشا می‌شوند. شکست اسم رمز اغلب بر روش‌های جستجوی فراگیر[a]، مانند استفاده از حمله‌های واژه-نامه[b]، متکی هستند. در حملات واژه‌نامه مهاجم از برنامه‌ای برای چرخیدن در تمامی لغات یک واژه-نامه (یا چند واژه‌نامه زبان‌های مختلف)، محاسبه مقدار درهم‌سازی برای هر لغت و بررسی مقدار درهم‌سازی به دست آمده با پایگاه‌داده استفاده می‌کند. استفاده از جدول‌های رنگین کمان[c] روش دیگری برای شکستن اسم رمز است. جدول‌های رنگین کمان جدول‌های از پیش محاسبه شده جفت متن ساده/مقدار درهم‌سازی هستند. جدول‌های رنگین کمان از حمله‌های جستجوی فراگیر سریع‌تر هستند زیرا از توابع کاهشی برای کوچک کردن فضای جستجو استفاده می‌کنند. هنگامی که یک جدول رنگین کمان تولید شد می‌توانند به طور مکرر توسط مهاجم استفاده شود.
تکثیر اعتبارنامه	اعتبارنامه هستار، یا ابزار تولید اعتبارنامه، به صورت غیر مشروع تکثیر شده است. یک مثال می‌تواند تکثیر غیرمجاز کلید خصوصی باشد.
حمله صیادی	هستار فریب داده می‌شود تا با یک درستی‌سنج جعلی تعامل داشته باشد و اسم رمز یا داده‌های شخصی حساس را آشکار سازد که مهاجم می‌توانند برای جا زدن خود به عنوان هستار استفاده شوند.
استراق سمع	مهاجم به تراکنش اصالت‌سنجی گوش می‌دهد تا اطلاعاتی را به دست آورد که می‌توانند در یک حمله فعالانه بعدی جهت جا زدن خود به عنوان هستار استفاده شوند.
حمله تکرار	مهاجم قادر است پیام‌های از پیش ربوده شده (بین یک هستار مشروع و یک RP) را تکرار کند تا به عنوان آن هستار نزد RP اصالت‌سنجی شود.
دزدی نشست	مهاجم قادر است بعد از تبادل اصالت‌سنجی موفقیت‌آمیز بین یک هستار و درستی‌سنج، خود را بین آن‌ها قرار دهد. مهاجم می‌تواند خود را نزد طرف اعتماد کننده به عنوان هستار معرفی کند، یا برعکس، تا تبادل داده نشست را کنترل کند. یک مثال هنگامی است که مهاجم قادر است از طریق استراق سمع یا حدس زدن مقدار کوکی‌های[d] اصالت‌سنجی استفاده شده جهت علامت زدن درخواست‌های HTTP ارسال شده توسط هستار کنترل نشست اصالت‌سنجی شده را در دست گیرد.
فرد در میان	مهاجم خود را میان هستار و طرف اعتماد کننده قرار می‌دهد به نحوی که بتواند محتوای پیام‌های قرارداد اصالت‌سنجی را قطع کند و تغییر دهد. مهاجم به طور معمول نزد هستار خود را به عنوان طرف اعتماد کننده و نزد درستی‌سنج خود را به عنوان هستار جا می‌زند. انجام تبادل فعال با هر دو طرف به صورت همزمان می‌تواند به مهاجم امکان دهد از پیام‌های اصالت‌سنجی فرستاده شده توسط یک طرف مشروع برای اصالت‌سنجی موفقیت‌آمیز نزد طرف دیگر استفاده کند.
دزدی اعتبارنامه	افزاره‌ای که اعتبارنامه‌ها را تولید یا نگهداری می‌کند توسط یک مهاجم به سرقت می‌رود.
جعل هویت	جعل هویت[e] و جا زدن خود به موقعیت‌هایی اشاره می‌کنند که در آن مهاجم خود را به جای یک هستار دیگر معرفی می‌کند تا امکان اجرای عملی را به دست آورد که در غیر این صورت قادر به انجام آن نبود (به عنوان مثال دسترسی به یک دارایی که در غیر این صورت غیر قابل دسترسی است). این کار می‌تواند از طریق استفاده از اعتبارنامه(های) یک هستار یا معرفی خود به عنوان هستار (به عنوان مثال با جعل اعتبارنامه) صورت گیرد. برخی مثال‌ها هنگامی هستند که مهاجمی که خود را به عنوان

تهدید	توصیف و مثال
	یک هستار جا می‌زند با ایجاد یک اثر انگشت چسبنده[f] که با الگو هستار تطبیق دارد یک یا چند خصیصه زیست‌سنجی آن هستار را جعل می‌کند؛ مهاجم از طریق انتشار آدرس MAC متعلق به افزاره‌ای دیگر که در شبکه دارای مجوز است توسط افزاره خود آن آدرس MAC را جعل می‌کند؛ یا مهاجم خود را به عنوان ناشر نرم‌افزار مشروع جا می‌زند که مسؤول بارگیری نرم‌افزارها یا به روزرسانی-هایی برخط است.

[a] Brute force

[b] Dictionary attack

[c] Rainbow table

[d] Coockie

[e] Spoofing

[f] Gummy finger

۲-۳-۱۰ کنترل‌های LoA مورد نیاز برای محافظت در برابر تهدیدها علیه استفاده از اعتبارنامه‌ها

کنترل‌های مورد نیاز جهت مقابله با تهدیدهای استفاده از اعتبارنامه بر طبق LoA در جدول ۹ مشخص شده‌اند.

جدول ۹- خلاصه کنترل‌ها برای تهدیدهای علیه استفاده از اعتبارنامه‌ها بر طبق LoA

تهدیدها	کنترل‌ها	کنترل‌های مورد نیاز				
		LoA*	LoA1	LoA2	LoA3	LoA4
عمومی**	MultiFactorAuthentication	-	-	-	#1	#1
حدس زدن برخط	StrongPassword	#2	-	-	-	-
	CredentialLockOut	#3	-	-	-	-
	DefaultAccountUse	#4	-	-	-	-
	AuditAndAnalyze	#5	-	-	-	-
حدس زدن برون‌خط	HashedPasswordWithSalt	#6	-	-	-	-
تکثیر اعتبارنامه	AntiCounterfeiting	#7	-	-	-	-
حمله صیادی	DetectPhishingFromMessages	#8	-	-	-	-
	AdoptAntiPhishingPractice	#9	-	-	-	-
	MutualAuthentication	#10	-	-	-	-
استراق سمع	NoTransmitPassword	#11	-	-	-	-
	EncryptedAuthentication	#12	-	-	-	-
	DifferentAuthenticationParameter	#13	-	-	-	-
حمله تکرار	DifferentAuthenticationParameter	#13	-	-	-	-
	Timestamp	#14	-	-	-	-

تهدیدها	کنترل‌ها	کنترل‌های مورد نیاز				
		LoA*	LoA1	LoA2	LoA3	LoA4
	PhysicalSecurity	#15	-	-	-	-
دزدی نشست	EncryptedSession	#16	-	-	-	-
	FixProtocolVulnerabilities	#17	-	-	-	-
	CryptographicMutualHandshake	#18	-	-	-	-
فرد در میان	MutualAuthentication	#10	-	-	-	-
	EncryptedSession	#16	-	-	-	-
دزدی اعتبارنامه	CredentialActivation	#19	-	-	-	-
جعل هویت	CodeDigitalSignature	#20	-	-	-	-
	LivenessDetection	#21	-	-	-	-

* - توصیه می‌شود این کنترل‌ها بر طبق نیاز مشخص شده توسط ارزیابی مخاطره به کار گرفته شوند.

** - اصالت‌سنجی چندعامله با تمامی تهدیدهای عمومی نمی‌تواند مقابله کند.

یادآوری–در جدول بالا، شناسانه‌های #1-#21به کنترل‌های خاص مورد نیاز جهت فراهم کردن محافظت در هر LoA اشاره می‌کنند. هر یک از این کنترل‌ها به صورت دقیق در ۱۰-۳-۲-۱ توصیف می‌شوند.

۱۰-۳-۲-۱ کنترل‌ها در برابر تهدیدها علیه استفاده از اعتبارنامه‌ها در مرحله اصالت‌سنجی

کنترل‌های زیر در برابر تهدیدها علیه استفاده از اعتبارنامه در حین مرحله اصالت‌سنجی متناظر با شماره‌های #1 -#21 فهرست شده در جدول ۹ هستند.

MultiFactorAuthentication

#1. دو یا چند اعتبارنامه که عامل‌های اصالت‌سنجی متفاوتی را پیاده‌سازی می‌کنند باید استفاده شوند (به عنوان مثال، ترکیب چیزی که در اختیار دارید با چیزی که از آن مطلع هستید).

StrongPassword

#2. استفاده از اسم رمزهای قوی (به عنوان مثال، رشته‌های پیچیده و خارج از واژه‌نامه که شامل ترکیبی از حروف بزرگ، حروف کوچک، اعداد و نویسه خاص هستند) باید اجبار شود.

CredentialLockout

#3. بعد از تعداد معینی تلاش ناموفق برای وارد کردن اسم رمز باید سازوکار تحریم یا کندسازی استفاده شود.

DefaultAccountUse

#4. اسم و اسم رمزهای حساب کاربری پیش فرض (به عنوان مثال، تنظیمات سازنده) نباید استفاده شوند.

AuditAndAnalyze

#5. باید از سلسله ممیزی[1] ورودهای ناموفق جهت تحلیل الگوهای حدس زدن برخط اسم رمز استفاده شود.

HashedPasswordWithSalt

#6. باید از اسم رمزهای درهم‌سازی شده با سالت استفاده شود تا مانع از حملات جستجوی فراگیر و جدول رنگین کمان شود.

Anticounterfeiting

#7. تدابیر مقابله با جعل (به عنوان مثال تمام‌نگاشت[2]، ریزنوشته[3]) باید بر روی افزاره‌هایی که اعتبارنامه‌ها را نگه می‌دارند استفاده شود.

DetectPhishingFromMessages

#8. کنترل‌هایی باید پیاده‌سازی شوند که به طور خاص برای تشخیص حملات حمله صیادی طراحی شده‌اند (به عنوان مثال، پالایه‌های بِیزین[4]، لیست سیاه IP، پالایه‌های مبتنی بر URL، طرح‌های اثر انگشت و اکتشافی).

AdoptAntiPhishingPractice

#9. رویکردهایی مانند غیرفعال‌سازی تصاویر، غیرفعال‌سازی اَبَرپیوند[5] از منابعی که مورد اعتماد نیستند و ارائه نشانه‌های تصویری در رایانامه مشتریان باید برای محافظت از هستارها در برابر حملات حمله صیادی استفاده شوند.

MutualAuthentication

#10. اصالت‌سنجی متقابل باید استفاده شود.

NoTransmitPassword

#11. باید از سازوکارهای اصالت‌سنجی استفاده شود که اسم رمزها را بر روی شبکه ارسال نمی‌کنند (به عنوان مثال قرارداد کربروس[6]).

1- Audit trail
2- Hologram
3- Microprint
4- Bayesian Filter
5- Hyperlink
6- Kerberos Protocol

EncryptedAuthentication

#12. اگر تبادل اصالت‌سنجی بر روی شبکه لازم باشد، داده‌ها باید قبل از ارسال رمزبندی شوند.

DifferentAuthenticationParameter

#13. برای هر تراکنش اصالت‌سنجی باید از پارامتر اصالت‌سنجی متفاوت استفاده شود (به عنوان مثال، اسم رمز یک بار مصرف، اعتبارنامه نشست).

Timestamp

#14. هر پیام باید به وسیله یک مُهر زمانی غیرقابل جعل مُهر زمانی بخورد.

PhysicalSecurity

#15. باید از سازوکارهای امنیت فیزیکی استفاده شود (یعنی، مدارک دستکاری، تشخیص و واکنش).

EncryptedSession

#16. باید از نشست‌های رمزبندی شده استفاده شود.

FixProtocolVulnerabilities

#17. باید از وصله‌های بستر[1] جهت رفع آسیب‌پذیری‌های قرارداد (به عنوان مثال، TCP/IP) استفاده شود.

CryptographicMutualHandshake

#18. باید از دست دادن متقابل مبتنی بر رمزنگاری (به عنوان مثال، SSL/TLS) استفاده شود.

CredentialActivation

#19. برای استفاده از اعتبارنامه یک مشخصه فعال‌سازی باید لازم باشد (به عنوان مثال، وارد کردن یک PIN یا اطلاعات زیست‌سنجی در افزاره سخت‌افزاری که اعتبارنامه را نگه می‌دارد).

CodeDigitalSignature

#20. امضاهای رقمی باید در برابر یک منبع مورد اعتماد بررسی شوند تا با دانلود نرم‌افزارهایی که توسط طرفین غیرمجاز تغییر داده شده‌اند مقابله شود.

LivenessDetection

#21. فنون تشخیص زنده بودن باید جهت شناسایی استفاده از مشخصه‌های زیست‌سنجی (به عنوان مثال، اثر انگشت‌های جعل شده) استفاده شوند.

1- Platform Patch

۱۱ معیارهای تضمین خدمت

متصدیان چارچوب اعتماد که به دنبال مطابقت با این چارچوب هستند باید معیارهای معینی را دایر کنند که الزامات هر LoA را که قصد پشتیبانی از آن را دارند برآورده می‌کنند و باید CSPهایی را که ادعای انطباق با چارچوب می‌کنند بر اساس آن معیارها ارزیابی کنند. به طور مشابه، CSPها باید LoAای را که خدمات آن‌ها در آن با این چارچوب مطابقت دارد از طریق ارزیابی فرآیندهای کلی کسب و کار خود و سازوکارهای فنی در برابر معیارهای معین، مشخص کنند.

پیوست الف
(اطلاعاتی)
حریم خصوصی و محافظت از PII

شایستگی یک رویکرد اصالت‌سنجی خاص برای کاربردی خاص نه تنها به ارزیابی اثربخشی اصالت‌سنجی بستگی دارد، بلکه به مخاطرات و رواداری مخاطره[1] سازمان درگیر نیز وابسته است. سوء استفاده یا فقدان محافظت مناسب PII هستارها مخاطرات قابل توجهی را برای سازمان، از آسیب به اعتبار سازمانی تا افشای آسیب‌پذیری[2]، به همراه خواهد داشت. از این رو، استفاده از PII برای اهداف اصالت‌سنجی و محافظت از آن لازم است به دقت سنجیده و بررسی شود. این بخش در ارتباط با برخی از ملاحظات حریم خصوصی[3] که به سازمان‌ها توصیه می‌شود هنگام تصمیم‌گیری در مورد استفاده و پیاده‌سازی رویکرد خاص اصالت‌سنجی در نظر بگیرند راهنمای اطلاعاتی ارائه می‌کند.

در مواردی که هستارها افراد باشند، اکثر رویکردهای اصالت‌سنجی شامل پردازش PII در حین یک یا چند مورد زیر می‌شوند:

الف-در حین مرحله نام‌نویسی هنگام جمع‌آوری، اثبات و وارسی هویت و سایر اطلاعات مرتبط با هستارها؛

ب-در حین ایجاد، صدور و مدیریت اعتبارنامه هستارها

پ-در حین استفاده از اعتبارنامه‌ها توسط هستار و وارسی آن‌ها توسط طرفین اعتماد کننده و درستی‌سنج‌ها.

داشتن اصالت‌سنجی قوی و حریم خصوصی قوی امکان‌پذیر است. رویکردهای اصالت‌سنجی زیادی وجود دارند که از نظر رمزنگاشتی قوی هستند ولی اثرات منفی محدودی روی حریم خصوصی دارند (به عنوان مثال، اعتبارنامه‌های بی‌نام[4]، امضاهای گروهی). علاوه بر این، باید توجه شود که افزایش قدرت سطح تضمین (به عنوان مثال، LoA4 در مقابل LoA2) می‌تواند اثر منفی بر حریم خصوصی فرد داشته باشد، اما به طور الزامی این چنین نیست. این مساله تا حدود زیادی به رویکرد اصالت‌سنجی انتخاب شده و نحوه پیاده‌سازی آن بستگی دارد. هنگام تصمیم‌گیری در مورد این موضوعات، توصیه می‌شود سازمان‌ها علاوه بر نیازهای محافظت از منابع خود و مسؤول دانستن هستارها در صورت فعالیت‌های غیرمجاز، به نیاز محافظت از PII هستارها نیز به دقت توجه کنند.

اکثر رویکردهای اصالت‌سنجی شامل استفاده از شناسانه‌های تمایز دهنده جهت تشخیص بدون ابهام یک هستار از سایر هستارهای احتمالی در زمینه اصالت‌سنجی می‌شوند. استفاده از شناسانه‌های تمایز دهنده

1- Risk tolerance
2- Liability Exposure
3- Privacy
4- Anonymous credentials

اغلب برای اهداف متنوع دیگری، مانند مدیریت حساب کاربری و نگهداری سلسله ممیزی مناسب، نیز لازم است. نگرانی اصلی از لحاظ حریم خصوصی در ارتباط با استفاده از شناسانه‌های تمایز دهنده به استفاده از خود شناسانه تمایز دهنده بر نمی‌گردد، بلکه استفاده مجدد از یک شناسانه در چندین زمینه متفاوت است. برای مثال، شماره حساب کاربری اختصاص داده شده برای یک منظور منفرد در مقابل کد مرجع اداری دولتی که برای چندین منظور (به عنوان مثال، مالیات، بیمه، حقوق بازنشستگی) استفاده می‌شود به طور عمومی دارای حساسیت پایین‌تری در نظر گرفته می‌شود. در برخی حوزه‌های خاص، ممکن است قوانینی وجود داشته باشند که استفاده از شناسانه‌های معینی را محدود می‌سازند.

با توجه به ملاحظات عنوان شده در بالا، توصیه می‌شود سازمان‌ها حفاظت‌های اثربخش جهت محافظت از PII هستارها در مرحله‌ها و فرآیندهای توصیف شده در این EAAF پیاده‌سازی کنند. به طور خاص، توصیه می‌شود رویکرد اصالت‌سنجی انتخاب شده به نحوی طراحی و پیاده‌سازی شود که به طور کلی پردازش PII را به حداقل برساند. علاوه بر این، توصیه می‌شود استفاده از شناسانه‌های تمایز دهنده که در زمینه‌ها یا دامنه‌های دیگر نیز استفاده می‌شوند به مواردی محدود شود که استفاده از آن‌ها الزامی است و قوانین آن حوزه استفاده از آن‌ها را مجاز می‌شمارند.

استانداردهای راهنمای اضافی برای محافظت از PII در دو منبع زیر یافت می‌شوند:

الف- ISO/IEC 29100 الزامات حریم خصوصی پایه را در قالب سه عامل اصلی توصیف می‌کند: (۱) الزامات قانونی و مقرارتی جهت حفاظت از حریم خصوصی فرد و محافظت از PII او، (۲) الزامات خاص کسب و کار و مورد کاری، (۳) اولویت‌های حریم خصوصی انفرادی هستار PII. ISO/IEC 29100 اصول حریم خصوصی پایه زیر را توصیف می‌کند: توافق و انتخاب، معیارهای هدف، محدودیت جمع‌آوری، استفاده، محدودیت نگهداری و افشا، کمینه‌سازی داده، آشکاری دقت و کیفیت، شفافیت و اعلان، مشارکت و دسترسی فرد، مسؤولیت، کنترل‌های امنیتی، انطباق. توصیه می‌شود سازمان‌ها علاوه بر انجام ارزیابی مخاطره جهت تحلیل تهدیدها، اثر رویکرد اصالت‌سنجی خود بر حریم خصوصی را مورد ارزیابی قرار دهند تا مشخص شود کدامیک از مولفه‌های سامانه‌های آن‌ها از لحاظ تدابیر محافظت از حریم خصوصی به توجه ویژه نیاز دارد.

ب-ISO/IEC 29101 یک چارچوب معماری برای سامانه‌های ICT که PII را پردازش می‌کنند ارائه می‌کند. این چارچوب معماری به صورت نگرانی‌ها و چندین دید معماری بیان شده است. مجموعه‌ای از مولفه‌ها برای پیاده‌سازی سامانه‌های ICT که PII را پردازش می‌کنند ارائه شده است. این چارچوب جهت ساخت معماری سامانه‌هایی که از اصول حریم خصوصی مطرح شده در ISO/IEC 29100 پیروی می‌کنند ارائه شده است.

برای راهنمایی دقیق در مورد الزامات، اصول و طراحی سامانه در ارتباط با محافظت از PII، به استانداردهای فوق مراجعه شود.

پیوست ب
(اطلاعاتی)
مشخصات یک اعتبارنامه

الف- اعتبارنامه از نوع داده است.

اعتبارنامه شامل محفظه یا افزاره فیزیکی که داده را نگه می‌دارد نمی‌شود. همچنین شامل یک تولید کننده برای داده‌هایی که اعتبارنامه را تشکیل می‌دهند نمی‌شود. از این رو، تولید کننده کد عبور هرگز بخشی از اعتبارنامه نیست و کارت هوشمندی که قادر به امضای داده است، نرم‌افزاری که امضای رقمی تولید می‌کند، یا کاغذی که می‌توان روی آن چیزی نوشت نیز شامل این موضوع می‌شوند.

ب-اعتبارنامه باید حاوی داده‌ای باشد که مدرک یک هویت یا حق است.

موارد زیر مثال‌هایی از چنین مدارکی هستند:
۱- نوعی اطلاعات (به عنوان مثال، اسم رمز ایستا)؛

۲- یک مشخصه زیست‌سنجی یا نمایشی از این نوع؛

۳- داده تولید شده توسط یک دارایی (به عنوان مثال، کدهای عبور یک بار مصرف که توسط تولید کننده کد عبور ایجاد شده‌اند، یا داده‌ای که با استفاده از کلید محرمانه‌ای که پنداشته می‌شود در اختیار هستار است به صورت رقمی توسط سخت‌افزار یا نرم‌افزار امضا شده است).

پ-اعتبارنامه می‌تواند با سایر داده‌هایی همراه باشد که در فرآیند اصالت‌سنجی و شناسایی می‌توانند مفید واقع شوند، اما بخشی از اعتبارنامه به حساب نمی‌آیند.

مثال‌هایی از این نوع داده شامل نام هستار و گواهی کلید عمومی می‌شوند. هیچ یک از این دو به عنوان مدرک هویت یا حق الزامی نیستند، اما در قراردادهای اصالت‌سنجی مفید هستند. ایجاد ارتباط میان نام هستار و اعتبارنامه، هویت را تایید می‌کند. ایجاد ارتباط میان گواهی کلید عمومی و اعتبارنامه اطلاعاتی را فراهم می‌کند که به آزمایش مدارک کمک می‌کند و همچنین به طور احتمالی می‌تواند اطلاعاتی در مورد هویت یا حق هستار فراهم کند.

ت-یک اعتبارنامه می‌تواند اعتبارنامه اشتقاقی[1] نیز باشد. در این حالت، چنین اعتبارنامه اشتقاقی می‌تواند اجتماع اطلاعات مشتق شده از مجموعه‌ای از اعتبارنامه‌ها باشد، که به طور معمول توسط یک هستار ایجاد می‌شوند و جهت اصالت‌سنجی نزد یک درستی‌سنج اعتبارنامه فرستاده می‌شوند. برای مثال، در برخی انواع

1- Derived credential

اصالت‌سنجی بی‌نام، هستار اعتبارنامه‌های صادر شده توسط CSP را به اعتبارنامه اشتقاقی تبدیل می‌کند که برای اصالت‌سنجی استفاده می‌شود.

ث-لازم نیست همه داده‌هایی که اعتبارنامه را تشکیل می‌دهند محرمانه باشند.

ج-اعتبارنامه می‌تواند برای اصالت‌سنجی، شناسایی یا صدور مجوز هستار یا ترکیبی از این سه مورد استفاده شود.

چ- اعتبارنامه باید پیش از آنکه برای اهداف خاصش (به عنوان مثال، اصالت‌سنجی، شناسایی، صدور مجوز) معتبر و قابل اعتماد پذیرفته شود مورد بررسی قرار گیرد.

ح-اعتبارنامه باید جهت بررسی چند مرحله را طی کند. مثال‌هایی از این مراحل شامل موارد زیر می‌شود:
۱- برررسی معتبر بودن اعتبارنامه جهت تضمین اینکه از صادر کننده ادعا شده نشات گرفته است؛

۲- تایید صحت و قابل اعتماد بودن اعتبارنامه (به عنوان مثال، مشخص کردن اینکه پیوند مستقیمی از صادر کننده اعتبارنامه به یک ریشه مورد اعتماد[1] وجود دارد یا خیر)؛

۳- تایید درستی محاسبات ریاضیات و رمزنگاری.

خ-اعتبارنامه می‌تواند صحیح باشد اما در تمامی زمینه‌ها معتبر نباشد (به عنوان مثال، اعتبارنامه نگهداری شده روی یک کارت هوشمند، مانند کارت‌های تلفن، می‌تواند صحیح باشد ولی فقط برای تماس‌هایی معتبر باشد که از طریق تجهیزات صادر کننده کارت صورت می‌گیرند).

1- Trusted root

کتاب‌نامه

[۱] استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷، فن آوری اطلاعات - فنـون امنیتـی -سیسـتم هـای مدیریت امنیت اطلاعات-الزامات

[2] The National e-Authentication Framework http://www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html

[3] Australian Government Gatekeeper Public Key Infrastructure http://www.gatekeeper.gov.au/

[4] ITU-T Focus Group on Identity Management Report 5 Report on Requirements for Global Interoperable Identity Management http://www.itu.int/ITU-T/studygroups/com17/fgidm/

[5] ITU-T Focus Group: Report on Identity Management Report 6 Framework for Global Interoperability http://www.itu.int/ITUT/studygroup/com*17/fgidm/*

[6] ITU-T Report on the Definition of the Term "Identity", April, 2008 http://www.itu.int/ITU-T/jca/idm/

[7] Kantara Initiative Identity Assurance Framework v2.0, http://kantarainitiative.org/confluence/display/GI/Identity+Assurance+Framework+v2.0

[8] New Zealand Standard: *Evidence of Identity (EOI)* June 2006 http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Evidence-of-Identity-Standard-Evidence-of-Identity-Standard-(html-version)?Open Document

[9] NIST Special Pub 800-36 Guide to Selecting Information Technology Security Products, October 2003, http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf

[10] NIST Special Pub 800-63 Electronic Authentication Guideline Version 1.0.2, April 2006 http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

[11] "OECD Recommendation for Electronic Authentication and OECD Guidelines for Electronic Authentication" http://www.oecd.org/dataoecd/32/45/38921342.pdf

[12] OMB M-04-04, *e-Authentication Guidance for Federal Organization* http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

[13] Principles for Electronic Authentication: A Canadian Framework, http://strategis.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00240e.html

[14] B. VAN ALSENOY and D. DE COCK, 'Due processing of personal data in eGovernment? A Case Study of the Belgian electronic identity card', Datenschutz und Datensicherheit, March 2008, p. 180

[15] A. Menezes, P. van Oorschot, S. Vanstone, 'Handbook of Applied Cryptography', 1997, p. 3-4. http://www.cacr.math.uwaterloo.ca/hac

[16] ENISA, Mapping (Interoperable Delivery of European e-government services to public Administrations, Businesses and Citizens) IDABC Authentication Assurance Levels to SAML v2.0

[17] ITU-T Recommendation X.1252 (2010), Baseline identity management terms and definitions

[18] ITU-T Recommendation Y.2702 (2010), Next generation network authentication and authorization requirements

[19] ITU-T Recommendation Y.2720 (2010), Next generation network identity management framework

[20] ITU-T Recommendation Y.2721 (2010), NGN identity management requirements and use cases

[21] ITU-T Recommendation Y.2722 (2010), *NGN identity management mechanisms*

[22] ISO/IEC 9798:2010, Information technology – Security techniques – Entity authentication

[23] ISO/IEC 19792:2009, Information technology – Security techniques – Security evaluation of biometrics

[24] ISO/IEC 29100:2011, Information technology – Security techniques – Privacy framework

[25] ISO/IEC 29101, Information technology – Security techniques – Privacy architecture framework

[26] ISO/IEC 24760-1:2011, Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts

[27] ISO/IEC 19790: 2012, Information technology – Security techniques – Security requirements for cryptographic modules