

بِسْمِ اللَّهِ
الرَّحْمَنِ
الرَّحِيمِ



The mark of
responsible forestry
FSC® C009732

سرشناسه: راهنمای هویت دیجیتال/[گروه ویژه اقدام مالی]

عنوان: راهنمای هویت دیجیتال

مترجمان: سیده سیما آریایی منش، الهه امیرجان، اسمهان حکاک

مشخصات نشر: راه پرداخت

مشخصات ظاهری: ۱۸۴ ص.؛ ۲۱/۱۴×۵/۵ س.م.

شابک: ۹۷۸-۶۲۲-۷۷۰۲-۲۰۰

وضعیت فهرست نویسی: فیپا

یادداشت: عنوان اصلی: Guidance on digital identity, 2020.

یادداشت: چاپ قبلی: انتشارات گپ، ۱۴۰۰ (فیپا).

موضوع: هویت‌های برخط (Online identities)

موضوع: پول شویی - پیشگیری (Money laundering -- Prevention)

موضوع: تروریسم - پیشگیری (Terrorism -- Prevention)

شناسه افزوده: آریایی منش، سیده سیما، ۱۳۵۱-، مترجم

شناسه افزوده: امیرجان، الهه، ۱۳۶۱-، مترجم

شناسه افزوده: حکاک، اسمهان، ۱۳۵۲-، مترجم

شناسه افزوده: گروه ویژه اقدام مالی

رده بندی کنگره: HM۸۵۱

رده بندی دیویی: ۳۰۳/۴۸۳۳

شماره کتابشناسی ملی: ۸۷۷۸۵۷۴

مستند کارگروه ویژه اقدام مالی درباره هویت دیجیتال

راهنمای هویت دیجیتال

سیده سیمای آریایی منش، الهه امیرجان، اسمهان حکاک





عنوان: راهنمای هویت دیجیتال

ناشر: راه پرداخت

مترجمان: سیده سیما آریایی منش، الهه امیرجان، اسمهان حکاک

ویراستار ارشد: مینا والی

ویراستار محتوایی: قاسم سرافرازی

ویراستار فنی: یلدا شایسته‌فر

بازبینی نهایی متن: رضا قربانی

صفحه‌آرا: بهناز سعیدی

ناظر چاپ: قادر شهبازی

نوبت چاپ: اول ۱۴۰۱

شمارگان: ۱۰۰۰ نسخه

شابک: ۹۷۸-۶۲۲-۷۷۰۲-۲۰۰۰

تلفن: ۰۲۱-۴۴۴۴۳۹۶۶

دورنگار: ۸۹۷۸۴۹۰۲

ایمیل: publisher@way2pay.press

وبسایت: way2pay.press

لینتوگرافی: هنر اشکان

چاپ و صحافی: واژه

همه حقوق چاپ و نشر این اثر برای «انتشارات راه پرداخت» محفوظ است. هرگونه تکثیر، انتشار و بازنویسی این اثر یا قسمتی از آن به هر شکل و شیوه (چاپی، صوتی، ویدئویی، دیجیتال و ...) بدون اجازه کتبی ناشر ممنوع است.

فروشگاه انتشارات راه پرداخت نشانی: تهران، جنت آباد جنوبی، خیابان لاله غربی، روبه‌روی پاساژ سمرقند، خیابان حدیث، کوچه حدیث دوم، پلاک ۸

۱۳	پیشگفتار
۱۵	دیباچه
۲۰	سرواژه‌ها
۲۳	خلاصه مدیریتی

بخش اول

۳۶	معرفی
۳۷	مزایای بالقوه
۳۸	خطرات بالقوه
۴۰	هدف و مخاطب موردنظر
۴۰	محدوده

بخش دوم

۴۴	واژه‌شناسی هویت دیجیتال و ویژگی‌های کلیدی
۴۵	«هویت» در اهداف این راهنما چیست؟
۴۵	مفهوم هویت رسمی
۴۵	اثبات هویت رسمی
۴۷	سامانه هویت دیجیتال در اهداف این راهنما چیست؟
۴۸	اجزای کلیدی یک سامانه هویت دیجیتال چیست؟
۴۹	جزء اول: اثبات هویت و ثبت نام (با صحت اولی/اعتبارسنجی) - (ضروری)
۵۱	جزء دوم: احراز هویت و مدیریت چرخه هویت (ضروری)
۵۳	جزء سوم: سازوکار قابلیت‌های حمل و قابلیت تعامل (اختیاری)

۵۴ چهارچوب‌های تضمین هویت دیجیتال و استانداردهای فنی

بخش سوم

۵۶ استانداردهای FAFT در مورد شناسایی کامل مشتری

۵۷ الزامات شناسایی / صحه‌گذاری مشتری (هنگام پذیرش)

۵۷ فرم مستند یا دیجیتالی شواهد و فرایندهای هویت

۵۸ مدرک هویتی «قابل اعتماد و مستقل»

۵۹ رویکرد ریسک‌محور «شناسایی کامل مشتری»

۶۰ روابط تجاری و تراکنش‌های غیرحضوری

۶۱ شناسایی کامل مستمر در روابط تجاری

۶۲ الزامات اعتبار شخص ثالث

۶۳ اعتماد شخص ثالث در حوزه هویت دیجیتال

۶۴ نهادهای قانونی به‌عنوان ارائه‌دهندگان خدمات هویت دیجیتال خارج از توصیه ۱۷

بخش چهارم

۶۶ مزایا و ریسک‌های سامانه‌های هویت دیجیتال برای تطبیق با قانون AML/CFT

۶۸ مزایای بالقوه سامانه‌های هویت دیجیتال

۶۸ تقویت «شناسایی کامل مشتری»

۶۸ به حداقل رساندن ضعف‌ها در اقدامات کنترل انسانی

۶۹ بهبود تجربه مشتری و صرفه‌جویی در هزینه

۷۰ نظارت بر تراکنش

۷۰ شمول مالی

۷۲ ریسک‌ها و چالش‌های سامانه‌های هویت دیجیتال

۷۴ ریسک‌های اثبات هویت و ثبت نام

ریسک‌های جعل هویت و هویت‌های مصنوعی (شامل حملات سایبری، نقص‌های

۷۴ محافظت از داده یا امنیتی)

۷۶ ریسک‌های احراز هویت و مدیریت چرخه حیات هویت

موانع بالقوه برای دستیابی به اطلاعات هویت به‌منظور شناسایی کامل مستمر و نظارت بر

۸۱ تراکنش‌ها

مشکلات بزرگی که سامانه‌های هویت دیجیتال آشکار کرده‌اند و ممکن است بر تلاش‌ها

۸۱ در حوزه مبارزه با پول‌شویی / مقابله با تأمین مالی تروریسم تأثیر بگذارند

۸۲ چهارچوب‌های داخلی برای هویت رسمی

۸۲ چالش‌های حفظ حریم خصوصی و محافظت از داده

بخش پنجم

- ارزیابی اینکه سامانه‌های هویت دیجیتال، در یک رویکرد مبتنی بر ریسک برای شناسایی کامل مشتری به قدر کافی قابل اعتماد و مستقل هستند یا خیر ۸۵
- تقویت استانداردهای فنی و چهارچوب‌های تضمین هویت دیجیتال در اجرای رویکرد مبتنی بر ریسک ۹۱
- استفاده از استانداردها و چهارچوب‌های تضمین هویت دیجیتال ۹۳
- ملاحظات ویژه برای شمول مالی ۹۴
- رابطه مدیریت ریسک هویت دیجیتال با اقدامات کاهش ریسک پول شویی ۹۴
- استانداردها و چهارچوب‌های هویت دیجیتال می‌توانند از شمول مالی حمایت کنند ۹۹
- «داوران مورد اعتماد» ۹۹
- اثبات هویت از راه دور و پذیرش به صورت غیر حضوری ۱۰۰

پیوست‌ها

- پیوست ۱: تعریف یک سامانه هویت دیجیتال پایه و مشارکت کنندگان آن ۱۰۲
- خلاصه فرایند هویت دیجیتال ۱۰۲
- جزء اول: اثبات هویت و ثبت نام ۱۰۳
- جزء دوم: احراز هویت ۱۰۹
- جزء سوم: سازوکار قابلیت حمل و تعامل پذیری (اختیاری) ۱۱۷
- مشارکت کنندگان در سامانه هویت دیجیتال ۱۱۸
- پیوست ۲: مطالعات موردی ۱۲۳
- پیوست ۳: اصول مربوط به شناسایی در توسعه پایدار ۱۴۸
- هدف ۱. تضمین شمول ۱۴۹
- هدف ۲. طراحی سامانه‌های هویت قدرتمند، امن، پاسخ‌گو و پایدار ۱۴۹
- هدف ۳. ایجاد اعتماد از طریق محافظت از حریم خصوصی و حقوق کاربر ۱۵۲
- پیوست ۴: چهارچوب تضمین هویت دیجیتال و نهادهای تنظیم‌کننده استاندارد فنی ۱۵۴
- پیوست ۵: بررسی اجمالی استانداردهای فنی و چهارچوب‌های تضمین دیجیتالی آمریکا ۱۵۶
- و اتحادیه اروپا ۱۵۶
- واژه‌نامه ۱۶۸

[یادداشت حامی]

هوش مصنوعی امروزه به بخش جدایی ناپذیر از زندگی ما تبدیل شده است. این فناوری یک فرایند تکاملی است که با سرعتی بسیار زیاد تقریباً بر آینده تمام صنایع، خدمات و هر انسانی تأثیر می‌گذارد و جهان کنونی را بصورت غیر قابل باوری تغییر خواهد داد.

هوش مصنوعی پایه و اساس یادگیری ماشین است و فعالیت‌های ذهنی انسان را به صورت مصنوعی با توانایی‌های پردازش، یادگیری، استدلال و حل مسئله انجام می‌دهد. تلاش نهایی هوش مصنوعی ایجاد سیستم‌های مبتنی بر علم، فناوری و برنامه‌های رایانه‌ای است که بتوانند در حل مشکلات و دستیابی به اهداف در جهان مانند انسان‌ها عمل کنند. با بهره‌گیری از هوش مصنوعی، رایانه‌ها می‌توانند حجم عظیمی از داده‌ها را به کار گرفته و از هوش آموخته شده خود برای تصمیم‌گیری و نتیجه‌گیری بهینه در زمانی استفاده کنند که از انسان انتظار انجام این موارد می‌رود. هوش مصنوعی به عنوان محرک و مولد اصلی فناوری‌های نوظهور مانند کلان داده، رباتیک و اینترنت اشیاء عمل می‌کند، چراکه جمع‌آوری و تجزیه و تحلیل داده‌ها به میزان قابل توجهی افزایش یافته است.

از این رو، کشورهای پیشرو دنیا برنامه‌های راهبردی کاملی در زمینه توسعه هوش مصنوعی در صنایع مختلف، سطوح سازمانی و کشوری در چارچوب دولت هوشمند تدوین کرده و در دست اجرا دارند و تاکنون بیش از ۶۰ کشور نسبت به تدوین برنامه ملی خود در حوزه هوش مصنوعی اقدام کرده‌اند.

علی‌رغم نگاه توسعه دانش محور در تمامی اسناد بالادستی ابلاغی از جانب رهبر انقلاب و تأکید ایشان برای قرار گرفتن در جمع ۱۰ کشور برتر در زمینه هوش مصنوعی در دنیا، متأسفانه ایران در زمینه هوش مصنوعی در سطح ملی برنامه‌ای نداشته و تقسیم کار ملی برای توسعه هوش مصنوعی انجام نپذیرفته است و ضرورت تدوین برنامه‌ای ملی با داشتن نگاه آینده‌نگر با استفاده از توانمندی‌های شرکت‌های دانش بنیان و نخبگان داخلی، به منظور بهره‌گیری از فرصت‌های حاصل از توسعه فناوری برای توسعه هوش مصنوعی در کشورمان بیش از پیش احساس می‌شود. این برنامه می‌تواند نقش مهمی در جهت‌دهی به توسعه و پذیرش هوش مصنوعی در سراسر صنایع و خدمات در کشور داشته باشد.

در این برنامه راهبردی در سطح ملی لازم است به توسعه زیرساخت‌های ارتباطی و پردازشی لازم، حمایت مناسب از اکوسیستم هوش مصنوعی و محصولات شرکت‌های دانش بنیان فناوری بومی، سرمایه‌گذاری مناسب و ریسک‌پذیر، آسان‌سازی و توسعه فضای کسب و کار، توسعه بسترهای نوآوری، تدوین و اجرای قوانین و مقررات براساس ارزش‌های اخلاقی، توسعه دسترسی به داده‌های باز و توسعه فرهنگ استفاده شهروندان از محصولات هوش مصنوعی در سطح ملی توجه شود.

نقش کلیدی اکوسیستم هوش مصنوعی با محوریت شرکت‌های دانش بنیان متکی بر علم و فناوری هوش مصنوعی برای دسترسی به این اهداف واقعیتی انکارناپذیر است و یکی از مهم‌ترین انتظاراتی که می‌توان از اکوسیستم جدید مبتنی بر فناوری و نوآوری داشت، پرداختن به مسائل و اولویت‌های ملی کشور از جمله هویت دیجیتال است. در حال حاضر حفاظت از هویت دیجیتال بیش از هر زمان دیگری اهمیت پیدا کرده است. به نظر می‌رسد برای کاهش هزینه‌ها و همچنین از بین بردن خطاهای انسانی در این حوزه ما بیش از پیش به بررسی‌های هوشمند از طریق هوش مصنوعی نیازمند خواهیم بود و این فناوری، احتمالاً برای احراز هویت و نیز صیانت از هویت دیجیتال که موضوع کتاب حاضر است تلقی می‌شود. امید است انتشار چنین کتاب‌هایی بتواند به ارتقای گفتمان فناوری هوش مصنوعی در کشورمان منجر شود و مسیری نو در توسعه هوش مصنوعی ایجاد کند.

محمدحسین متقی‌زاده

رئیس هیئت مدیره آی‌تی‌ساز

[یادداشت ناشر]

چرا کتابی مانند «هویت دیجیتال» برای ما مهم است؟ واقعیت این است که ما در انتشارات راه پرداخت در همین مدت کوتاهی که نزدیک به ۱۰۰ کتاب منتشر کرده ایم پیوسته بر توسعه نوآوری و فناوری متمرکز بوده ایم. فناوری و نوآوری بر روی زیرساختی رشد می کنند که اگر نباشد شاهد رشد ناقص خواهیم بود. ما نمی توانیم انتظار داشته باشیم دستاوردهای فناوری و نوآوری را بچشمی ولی زیرساخت های آن را نداشته باشیم. سیستم های احراز و تأیید هویت یکی از همین زیرساخت هایی است که اگر نباشند به معنای عدم توسعه است. اکنون که جهان به سرعت دیجیتالی می شود هر آن چیزی که قابلیت دیجیتالی شدن دارد باید دیجیتالی شود. هویت از آن دست مفاهیمی است که سال ها است به سوی دیجیتالی شدن حرکت کرده است. بنابراین امروز مسئله ما این نیست که هویت دیجیتال خوب است و لازم؛ امروز کسی در اهمیت هویت دیجیتال شک و تردیدی ندارد و حتی آنهایی که به دلایلی با توسعه مخالف هستند کم تر جرئت مخالفت کردن پیدا می کنند. مسئله امروز مسئله دیگری است؛ امروز سؤال ما این است که چگونه سیستم های احراز و تأیید هویت دیجیتال را به درستی پیاده سازی کنیم. امروز هویت دیجیتال یک واقعیت پذیرفته شده است ولی چیزی که کیمیاست کسانی هستند که بتوانند آن را در عمل پیاده سازی کنند. علی رغم ظاهر ساده ای که مفاهیم مرتبط با هویت دیجیتال دارند در عمل پیاده سازی آنها طیف وسیعی از علوم و مهارت ها را نیاز دارد. به همین دلیل در سال های گذشته فعالان این حوزه رشد داشته اند و شاهد شکل گیری افراد

و کسب و کارهایی بوده ایم که در یک حوزه مشخص تخصص داشته اند. یکی از نهادهایی که به خوبی چارچوب های اجرایی پیاده سازی هویت دیجیتال را تدوین کرده FATF بوده است. متأسفانه نام FATF در ایران با مسائل سیاسی گره خورده است و همین موضوع دافعه بی موردی را در برخی علیه این چارچوب ها ایجاد کرده است.

ما برای توسعه اقتصادی چاره ای نداریم جز این که روی خوش به فناوری های انقلابی و به طور خاص دیجیتال نشان دهیم. با این حساب اگر بخواهیم در جهان تمام دیجیتال زندگی کنیم باز چاره ای نداریم جز این که ساختارهای اجرایی هویت دیجیتال را پیاده کنیم. در این زمینه ها بدترین کار اختراع دوباره چرخ است و انجام تجربه هایی که جهانیان قبلاً هزینه آن را پرداخته اند. آنچه امروز نیاز داریم بعد از تغییر مدل ذهنی راهنماهای عملی و کاربردی است؛ چارچوب هایی که به کار ذهن های تغییر یافته می آید.

ما در انتشارات راه پرداخت بر روی این کار می کنیم که ذهن ها را تغییر دهیم و برای جهان جدید آماده کنیم. زندگی در جهان جدید چارچوب های خودش را دارد و قاعدتاً نمی توان با مدل های ذهنی قدیمی در این جهان به شکل مطلوب زندگی کرد. زندگی مطلوب هم در برخی موارد نیازمند پیاده سازی چارچوب هایی است که تجربه های جهانی بهترین الگوها برای ما هستند. به عبارتی ما باید بر روی این زمان بگذاریم که ذهن ها را تغییر دهیم و چرایی تغییر را درک کنیم و بعد از آن کافی است بین روش های موجود گشته و بهترین روش اجرایی را پیاده کنیم. هر فرمانده ای در لشکرش برای پیاده کردن بهترین نقشه ها هم به سربازانی نیاز دارد که پای کار باشند. چارچوب ها و استانداردها حکم سربازهای این میدان را دارند. اگر به استانداردهای جهانی بی توجه باشیم خودمان را از منبعی رایگان محروم و هزینه ای بی دلیل بر خودمان تحمیل کرده ایم. چارچوب ها کمک می کنند در اجرا قطب نمایی مفید داشته باشیم. در پایان لازم می دانم از تمام همکاران خوبم در مجموعه راه پرداخت و همه آنهایی که به شکلی در تولید و آماده شدن این کتاب همکاری داشتند تشکر کنم. امیدوارم در راه پرداخت بتوانیم اثربخش تر از گذشته انتشار محتواهای کاربردی در زمینه فناوری و نوآوری را ادامه دهیم.

پیشگفتار

هویت دیجیتال مفهومی است که طی بیست سال گذشته و به دنبال رشد حیرت‌انگیز دستگاه‌های هوشمند شکل گرفته است. ضعف در حوزه شناسایی و احراز هویت حضوری و عدم امکان اثبات هویت معتبر در فرایند حضوری ایجاب می‌کرد از راه‌هایی معتبرتر و دقیق‌تر جهت احراز هویت استفاده شود. از طرف دیگر، جمعیت زیادی از اشخاص حقیقی در دنیا وجود دارند که مدرک هویتی ندارند و به همین دلیل از خدمات پایه انسانی محروم‌اند، این مسئله نشان‌دهنده ناکارآمدی مدارک فیزیکی هویتی است. مطابق با آمار شرکت مشاوره‌ای «مکنزی»، بیش از یک میلیارد نفر در دنیا وجود دارند که هیچ‌گونه مدرک هویتی ندارند. شمار زیادی از این اشخاص زنان و کودکان‌اند؛ این اشخاص از دریافت هرگونه خدمات به دلیل نبود مدارک هویتی معتبر محروم می‌شوند.

تعداد آوارگان و پناه‌جویان رو به افزایش است و به دلیل اینکه در شرایط بحرانی از منطقه خارج شده‌اند، هیچ مدرکی برای اثبات هویت خود ندارند.

از سوی دیگر، ظهور کسب‌وکارهای دیجیتال امکان عرضه خدمات غیرحضوری را فراهم کرده که لازمه آن شناسایی و احراز هویت اشخاص از طریق مدارک دیجیتال و غیرحضوری است.

تجربه همه‌گیری کووید ۱۹ نشان داد که عرضه خدمات غیرحضوری در سطح ملی و بین‌المللی نه تنها امری لازم، بلکه ضروری است. حتی در بخش سلامت، بسیاری از

متخصصان بر این باورند که به منظور پیشگیری از سرایت جهش‌های جدید ویروس کرونا بایستی در خصوص ردیابی مبتلایان به ویروس اقدامات لازم را انجام دهیم. در بسیاری از کشورها عرضه خدمات یارانه‌ای دولت به اقشار نیازمند جامعه، به بهبود عملکرد سامانه‌های مدیریت هویت نیاز دارد.

همه دلایل یادشده سبب می‌شوند به این نتیجه برسیم که در سطح ملی و بین‌المللی، اشخاص حقیقی باید دارای هویت ملی دیجیتال باشند و از طریق ابزارهای دیجیتال تعامل کنند.

کتابی که پیش رو دارید، کتاب راهنمای هویت دیجیتال است که توسط کارگروه ویژه اقدام مالی (FATF) و با کمک جمعی از متخصصان جهان تدوین شده است. این کتاب، به حق از بهترین و کامل‌ترین مستندات منتشرشده در این زمینه است که از تمام استانداردهای روز دنیا بهره گرفته است. متن تدوین شده کتاب نه فقط دید بسیار مناسبی از مفاهیم مدیریت هویت و فرایند احراز هویت به مخاطب می‌دهد، بلکه به مدیران ارشد، میانی و متخصصان مدیریت هویت، به عنوان مخاطبان اصلی این اثر، کمک می‌کند در چرخه حیات مدیریت هویت کشور حضور فعال داشته باشند.

تشکر می‌کنم از خانم‌ها لیلا یوسفی و نجمه نوذر و آقایان محمدمهدی اشجعی و محمدرضا جم که در ترجمه و نشر این کتاب با ما همکاری کردند.

این کتاب را شماری از اعضای کارگروه هویت دیجیتال «ساهر»، زیرمجموعه جامعه آزاد کسب و کار هوشمند خاورمیانه و شمال آفریقا (MSBC Group)، ترجمه کرده‌اند.

سیده سیما آریایی منش
اردیبهشت ماه ۱۴۰۱

دیباچه

جهان امروز با ادبیاتی متفاوت روبه‌روست و با کمک تحولات دهه اخیر در فناوری اطلاعات و توسعه کاربردهای آن، اکوسیستم‌هایی نوین در سطوح جهانی شکل گرفته و افق‌هایی گسترده پیش روی ما پدیدار شده‌اند. متخصصان فناوری اطلاعات، در هر رشته‌ای که فعال‌اند، با همکاری هم زیرساخت‌ها و ابزارهای جهانی جدید را فراهم می‌کنند، در بسیاری از فعالیت‌های ما مشکلات مسافت و بُعد مکان را از میان برداشته‌اند و مرزهای جغرافیایی را کمرنگ کرده‌اند. فراز اصلی این تحول شگرف در افزایش سرعت، انجام فعالیت از راه دور با افزایشی شگفت‌انگیز در حجم عملیات است.

کووید ۱۹ سرعت نوآوری را در فضای سایبری بیشتر کرده است و همه کاربران و سازمان‌ها در فاصله زمانی کوتاهی نیازمند تسلط دیجیتال در کار خود شده‌اند. متخصصان از جهان پساکرونا صحبت می‌کنند، فرهنگ کاری تغییر کرده است، دورکاری رواج پیدا کرده، کلاس‌های درسی، خرید و فروش و برگزاری جلسات کاری شکل‌شان را به قالب دیجیتال نزدیک کرده‌اند. در نتیجه این فرهنگ نوظهور، تولید داده و محتوا بیشتر شده است و همه این‌ها نیاز به توسعه فناوری اطلاعات و استفاده از آن را افزایش می‌دهد.

بسیاری از امور، ساده‌تر، سریع‌تر و صحیح‌تر انجام می‌شوند و هم‌زمان حجم عظیمی

از اطلاعات یکپارچه جمع‌آوری می‌شود و به عبارتی داده‌ها و دانش سازمان‌ها ثبت و نگهداری می‌شوند که مدیریت آن، امکان تعریف خدماتی جدید و مؤثر را فراهم می‌کند.

این بانک‌های اطلاعاتی عظیم اگر به یک نظام تعریف شده و استفاده از هویت دیجیتال متمرکز مجهز باشند، می‌توانند خدمات متعددی در اختیار مردم قرار دهند و به ایشان کمک کنند سریع‌تر و روان‌تر خدمات دریافت کنند و در عین حال این امکان را هم برای سازمان‌ها ایجاد می‌کنند که بتوانند در زمانی کوتاه‌تر با هزینه‌ای کمتر و نیروی انسانی محدودتر خدماتی با کیفیت بهتر و تنوع بیشتر عرضه کنند. هویت دیجیتال امکان دسترسی به خدمات را در بستری امن و قابل اعتماد فراهم می‌آورد و سازمان‌ها با کمک سامانه‌های مربوط و جمع‌آوری آمار و ارقام دقیق می‌توانند بهتر و کامل‌تر برنامه‌ریزی کنند.

مدیریت توسعه و به‌کارگیری سامانه‌ها در این اکوسیستم‌های جدید نیازمند ابزار و کارایی متفاوتی است. این ابزارها، هم از بُعد فناوری مهم‌اند و هم تعریف قوانین و ضوابط جدید و هم چهارچوب‌های مناسباتی دیگری می‌طلبند که با روش‌های گذشته بسیار متفاوت و در عین حال به‌صورت مداوم در حال تغییر و تحول‌اند.

این قوانین و ضوابط بایستی تبادلات حجیمی را در کسری از ثانیه ثبت و ضبط، صحت‌سنجی و مدیریت کنند و امنیت خاطر کاربران بابت مشکلاتی از قبیل خطا، تقلب، فساد و هک را فراهم سازند. گذر از بحرانی این‌چنینی روحیه‌ای نوآورانه و همکاری صاحبان فن و دانش را می‌طلبد.

در عین حال، توانایی استفاده از دستاوردهای متفکران و دانشمندان عرصه‌های مختلف نیز اهمیت بسیاری دارد.

یکی از ارکان استفاده از این تحول دیجیتال، تعریف و تعیین هویت دیجیتال و تشخیص یا احراز هویت دیجیتال است. مطالعه این کتاب برای همه دست‌اندرکاران، کاربران و توسعه‌دهندگان سامانه‌هایی که در سطح کلان تعریف می‌شوند، مفید خواهد بود.

این کتاب، ضمن معرفی الگوهایی متفاوت به‌منظور کاربردهایی مختلف،

استانداردهای بین‌المللی را بررسی کرده است و برای هرکسی که به دنبال استفاده از سامانه‌ای با قابلیت تعریف و احراز هویت دیجیتال باشد، قابل استفاده است.

امیرمسعود اسکوئیلر

اردیبهشت‌ماه ۱۴۰۱

این ترجمه غیر رسمی است و حق ترجمه و چاپ این سند به این گروه از طرف
گروه ویژه اقدام مالی (FATF) اعطا شده است.

سند با استناد به مرجع زیر ترجمه شده است:

FATF (2020), Guidance on Digital Identity, FATF, Paris, www.fatf-gafi.org/publications/documents/digital-identity-guidance.html

از گروه ویژه اقدام مالی (FATF) برای تهیه و تدوین این راهنما تشکر ویژه
به عمل می آید.
همچنین از جناب آقای علیرضا طلوع، جناب آقای احمد آهی و گروه
مشاوران هویت دیجیتال ساهر که در تهیه این مستند با ما همکاری
داشته اند، سپاسگزاری می شود.

سرواژه‌ها

<u>AAL</u> 1/2/3 Authentication Assurance Level (under NIST)	سطح تضمین احراز هویت (تحت NIST)
<u>AL</u> Assurance Level	سطح تضمین
<u>AML/ CFT</u> Anti-money laundering/Counteracting the financing of terrorism	مبارزه با پول‌شویی / مقابله با تأمین مالی تروریسم
<u>API</u> Application Programming Interface	رابط برنامه‌نویسی کاربردی
<u>ASP</u> Authentication Service Provider	ارائه‌دهنده خدمات احراز هویت
<u>CDD</u> Customer Due Diligence	شناسایی کامل مشتری
<u>CEN</u> European Committee for Standardization	کمیته اروپایی برای استانداردسازی
<u>CENELEC</u> European Committee for Electrotechnical Standardization	کمیته اروپایی برای استانداردسازی الکتروتکنیکی
<u>CSP</u> Credential Service Provider	ارائه‌دهنده خدمات اعتبارنامه
<u>DCS</u> Document Checking Service	خدمات بررسی اسناد
<u>DLT</u> Distributed Ledger Technology	فناوری دفترکل توزیع‌شده
<u>DNFBP</u> Designated Non-Financial Businesses and Professions	مشاغل و حرفه‌های غیرمالی تعیین‌شده
<u>ETSI</u> European Telecommunications Standards Institute	مؤسسه استاندارد ارتباطات از راه دور اروپا

eIDAS Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market	مقررات اتحادیه اروپا شماره ۹۱۰/۲۰۱۴ درمورد خدمات شناسایی و اعتماد الکترونیکی برای معاملات الکترونیکی در بازار داخلی
FAL 1/2/3 Federation Assurance Level (under NIST)	سطح تضمین هم‌پیمانی (تحت NIST)
FIDO Fast Identity Online	هویت سریع آنلاین
GDPR General Data Protection Regulation	مقررات عمومی حمایت از داده‌ها
GPS Global Position System	سامانه تعیین موقعیت جهانی
GSMA Global System for Mobile Communications	سامانه جهانی ارتباطات سیار
ICT Information and communications technology	فناوری اطلاعات و ارتباطات
IAL 1/2/3 Identity Assurance Level (under NIST)	سطح تضمین هویت (تحت NIST)
ID Identity	هویت
IDSP Identity Service Provider	ارائه‌دهنده خدمات هویت
IEC International Electrotechnical Commission	کمیسیون بین‌المللی الکتروتکنیکی
INR . Interpretive Note to Recommendation	یادداشت تفسیری برای توصیه
IP Internet Protocol	پروتکل اینترنت
ISO International Organization for Standardization	سازمان بین‌المللی استانداردسازی
ITU International Telecommunications Union	اتحادیه بین‌المللی ارتباطات از راه دور
IVSP Identity Verification Service Provider	ارائه‌دهنده خدمات صحت‌گذاری هویت
LoA Level of Assurance	سطح تضمین
MAC Media Access Control	کنترل دسترسی رسانه

<u>ML</u> Money laundering	پول‌شویی
<u>MFA</u> Multi-factor authentication	احراز هویت چندعاملی
<u>NGO</u> Non-governmental organisations	سازمان‌های مردم‌نهاد
<u>NIST</u> National Institute of Standards and Technology	انستیتوی ملی استانداردها و فناوری
<u>OIDF</u> OpenID Foundation	بنیاد OpenID
<u>PII</u> Personally Identifiable Information	اطلاعات شناسایی شخصی
<u>PIN</u> Personal Identification Number	شماره شناسایی شخصی
<u>R.</u> Recommendation	توصیه
<u>RBA</u> Risk-based approach	رویکرد مبتنی بر ریسک
<u>SAG</u> Standards Advisory Group	گروه مشاوره استاندارد
<u>SCA</u> Strong Customer Authentication	احراز هویت قوی مشتری
<u>TF</u> Terrorist financing	تأمین مالی تروریسم
<u>VASP</u> Virtual Asset Service Providers	ارائه‌دهندگان خدمات مجازی دارایی
<u>W3C</u> World Wide Web Consortium	کنسرسیوم وب جهانی
<u>UNHCR</u> United Nations High Commissioner for Refugees	کمیساریای عالی سازمان ملل در امور پناهندگان

خلاصه مدیریتی

۱. پرداخت‌های دیجیتالی، سالانه با ۱۲/۷ درصد تخمین، در حال رشدند و پیش‌بینی می‌شود تا سال ۲۰۲۰ میلادی به ۷۲۶ میلیارد تراکنش سالانه برسند.^۱ تا سال ۲۰۲۲ میلادی حدود ۶۰ درصد از تولید ناخالص داخلی جهان دیجیتالی می‌شود.^۲ از نگاه FATF، رشد تراکنش‌های مالی دیجیتالی نیازمند درک بهتر این موضوع است که چگونه اشخاص در دنیای خدمات مالی دیجیتالی، شناسایی و صحه‌گذاری می‌شوند. فناوری‌های هویت دیجیتال^۳ به سرعت در حال پیشرفت‌اند و باعث ایجاد انواع سامانه‌های هویت دیجیتال می‌شوند. این راهنما قصد دارد به دولت‌ها، نهادهای قانونی و دیگر ذی‌نفعان مرتبط کمک کند تا برای شان مشخص شود چگونه می‌توانند از سامانه‌های هویت دیجیتال به منظور هدایت عناصر خاصی از شناسایی کامل مشتری (CDD)^۴ مطابق با توصیه شماره ۱۰ مستند FATF^۵ استفاده کنند.^۶

۲. درک چگونگی عملکرد سامانه‌های هویت دیجیتال برای استفاده از رویکرد مبتنی بر ریسک توصیه شده در این راهنما ضروری است. در قسمت دوم راهنما، ویژگی‌های اصلی سامانه‌های هویت دیجیتال به طور خلاصه مطرح شده‌اند که مشروح آن در پیوست شماره یک آمده است.

۳. در بخش سوم، خلاصه‌ای از الزامات اصلی FATF، اشاره شده در این راهنما، از قبیل نیاز به شناسایی و تأیید هویت مشتریان با استفاده از اسناد منبع، داده‌ها یا اطلاعات «قابل اعتماد و مستقل» آورده شده است (توصیه^۷ 10(a)). در زمینه هویت دیجیتال، شرط اینکه اسناد منبع، داده‌ها یا اطلاعات دیجیتالی باید «قابل اعتماد و مستقل» باشند، به این معنی است که سامانه هویت دیجیتالی که به منظور شناسایی کامل مشتری از آن استفاده شده است، به فناوری، قانونمندی متناسب، فرایندها و روندهایی که سطح مناسبی از اطمینان را نسبت به تولید نتایج دقیق دارند، متکی است. این راهنما توضیح می‌دهد که شناسایی مشتری و معاملات

1. Capgemini & BNP Paribas (2018), World Payments Report 2018, accessed online at: <https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/World-Payments-Report-2018.pdf>

2. International Data Corporation (IDC), IDC Future Scape: Worldwide IT Industry 2019 Predictions

3. Digital Identity

4. Customer Due Diligence (CDD)

5. The Financial Action Task Force (FATF)

۶. مؤسسات مالی دست‌کم باید به مدت پنج سال کلیه سوابق لازم درمورد معاملات، اعم از داخلی یا بین‌المللی، را حفظ کنند تا بتوانند به سرعت آن‌ها را با درخواست‌های اطلاعاتی از سوی مراجع ذی‌صلاح مطابقت دهند.

7. Recommendation 10 (a)

غیرحضور که به سامانه‌های هویت دیجیتال قابل اعتماد و مستقل و با اقدامات مناسب جهت کاهش ریسک متکی اند، ممکن است یک سطح استاندارد از ریسک را ایجاد کند و حتی ممکن است کم‌خطر باشد.

۴. رویکرد مبتنی بر ریسک توصیه شده در این راهنما بر یک مجموعه متن باز، چهارچوب‌های تضمین اجماع محور^۱ و استانداردهای فنی برای سامانه‌های هویت دیجیتال (به آن به عنوان «استانداردها و چهارچوب‌های تضمین هویت دیجیتال»^۲ اشاره می‌شود) متکی است که در چند حوزه قضایی توسعه یافته است. سازمان بین‌المللی استانداردسازی^۳ به همراه کمیسیون بین‌المللی الکتروتکنیکی^۴ در حال استانداردسازی این چهارچوب‌های تضمین هویت دیجیتال و به روز کردن طیف وسیعی از استانداردهای فنی ISO/IEC از زمینه هویت، امنیت فناوری اطلاعات و حفظ حریم خصوصی است تا استاندارد جهانی جامعی را برای سامانه‌های هویت دیجیتال توسعه دهد. یک چهارچوب تضمین هویت، الزامات مربوط به «سطوح تضمین»^۵ مختلف را تعیین می‌کند. سطوح تضمین، پایایی و استقلال یک سامانه هویت دیجیتال و اجزایش را اندازه‌گیری می‌کند. اگرچه ممکن است سطح تضمینی که حوزه‌های قضایی مختلف ایجاد کرده‌اند، از جهات خاص متفاوت باشند، به منظور سهولت در ارجاع، این راهنما در درجه اول به چهارچوب و استانداردهای تضمین هویت دیجیتال از مؤسسه ملی استانداردها و فناوری ایالات متحده (NIST Digital ID Guidelines^۶) و مقررات eIDAS^۷ اروپا اشاره می‌کند. حوزه‌های قضایی باید رویکرد مندرج در این راهنما را متناسب با چهارچوب‌های تضمین هویت دیجیتال بومی‌سازی کنند و سایر استانداردهای فنی مربوطه را در نظر بگیرند.^۸

1. consensus-driven assurance frameworks

2. digital ID assurance frameworks and standards

3. International Organization for Standardization (ISO)

4. International Electrotechnical Commission (IEC)

5. assurance levels

۶. دستورالعمل هویت دیجیتال NIST 800-63 شامل مجموعه‌ای از مستندات است: 3-800-63 NIST SP دستورالعمل هویت دیجیتال (مرور کلی)؛ 800-63A NIST SP: دستورالعمل هویت دیجیتال شامل: ثبت نام و اثبات هویت؛ 800-63B NIST SP دستورالعمل هویت دیجیتال شامل: احراز هویت و مدیریت چرخه حیات و 800-63C NIST SP دستورالعمل هویت دیجیتال شامل: اظهارنامه‌ها (Assertions) و هم‌پیمانی (Federation).

۷. مقررات (اتحادیه اروپا) شماره ۲۰۱۴/۹۱۰ در مورد شناسایی الکترونیکی و خدمات اعتماد برای معاملات الکترونیکی در بازار داخلی.

۸. یک حوزه قضایی ممکن است یک چهارچوب تضمین هویت دیجیتال یا استانداردهای فنی ویژه برای سیستم‌های هویت دیجیتال نداشته باشد، اما ممکن است دارای معیارهای فنی دیگری (به عنوان مثال امنیت اطلاعات IT) باشد که بسیار مرتبط هستند.

۵. چهارچوب‌ها و استانداردهای تضمین هویت دیجیتال و مقررات مبارزه با پول شویی / مقابله با تأمین مالی تروریسم^۱ منشأهای مختلف و مخاطبان متفاوت دارند. این راهنما بین چهارچوب‌های تضمین هویت دیجیتال و استانداردها و الزامات شناسایی کامل مشتری مستند FATF پیوند ایجاد می‌کند. همان‌طور که در جدول صفحه بعد نشان داده شده، اجزای اصلی سامانه‌های هویت دیجیتال به الزامات شناسایی و صحه‌گذاری خاصی تحت توصیه (a)10 مربوط می‌شوند.

بر این اساس، چهارچوب‌های تضمین هویت دیجیتال و استانداردهای فنی که این اجزا را تعریف و الزامات هر سطح از تضمین را تنظیم می‌کنند، ابزاری بسیار پُرکاربرد جهت ارزیابی پایداری و استقلال سامانه‌های هویت دیجیتال با اهداف مبارزه با پول شویی / مقابله با تأمین مالی تروریسم، عرضه می‌کنند.

اجزای اصلی سامانه‌های هویت دیجیتال	نیازمندی‌های شناسایی کامل مشتری (مشتریان حقیقی)
ثبث نام و اثبات هویت (با اتصال): شما چه کسی هستید؟ به دست آوردن ویژگی‌ها (نام، تاریخ تولد، شماره ملی و غیره) و گواهی برای این ویژگی‌ها؛ اعتبارسنجی و صحه‌گذاری گواهی هویت و تصمیم‌گیری جهت اثبات هویت یکتای شخص؛ اتصال: صدور اعتبارنامه‌ها/ احرازکنندگان هویت که شخص را به اعتبارنامه‌هایی که مالک آن است و تحت کنترل دارد، برای اثبات هویت شخص متصل می‌کند. احراز هویت: آیا شما شخص شناسایی شده یا تأییدشده هستید؟ اثبات اینکه مدعی، مالکیت و کنترل اعتبارنامه‌های متصل شده را دارد. احراز هویت برای توصیه (a)10 به کار می‌رود، اگر نهاد قانونی با تأیید اعتبار هویت دیجیتال موجود که از قبل در اختیار مشتری است، شناسایی / صحه‌گذاری هویت را انجام دهد.	شناسایی / صحه‌گذاری - توصیه (a)10

۶. راهنما توضیح می‌دهد که: ۱. زمانی که نهاد قانونی برای یک مشتری، با اعتبارنامه‌های هویت دیجیتال از قبل موجود، یعنی یک راه‌کار هویت دیجیتال خارج از خانه، یک حساب باز می‌کند، احراز هویت با توصیه 10(a) مرتبط است و ۲. زمانی که در زمینه هویت دیجیتال و تأمین مالی دیجیتال، احراز هویت مؤثر مشتری برای صدور مجوز دسترسی به حساب کاربری می‌تواند از تلاش‌های مبارزه با پول‌شویی / مقابله با تأمین مالی تروریسم، پشتیبانی کند.

۷. اصل مطلب این راهنما بخش پنجم است و مقامات دولتی، نهادهای قانونی و دیگر طرف‌های مرتبط را درمورد چگونگی به‌کارگیری رویکرد مبتنی بر ریسک در استفاده از سامانه‌های هویت دیجیتال جهت شناسایی و صحه‌گذاری مشتریان مطابق با توصیه 10(a) و حمایت از شناسایی کامل مستمر^۱ در توصیه 10(a)، راهنمایی می‌کند. روش پیشنهادی به‌لحاظ فناوری، بی‌طرف^۲ است (و نوع خاصی از سامانه‌های هویت دیجیتال را توصیه نمی‌کند). دو جزء این رویکرد عبارت‌اند از:

الف. شناخت سطوح تضمین اجزای اصلی سامانه هویت دیجیتال (شامل فناوری‌ها، معماری و حاکمیت آن) برای تعیین آن به‌عنوان یک منبع قابل اعتماد و مستقل اطلاعات.

ب. تصمیم‌گیری مهم مبتنی بر ریسک درمورد اینکه آیا سامانه هویت دیجیتال خاص با توجه به سطوح تضمین آن، سطح مناسبی از اعتماد و استقلال را در برابر خطرهای بالقوه پول‌شویی، تأمین مالی تروریسم، تقلب^۳ و ریسک‌های تأمین مالی پُرخطر تأمین می‌کند.

۸. بخش پنجم این راهنما چگونگی استفاده از استانداردها و چهارچوب‌های تضمین هویت دیجیتال را به‌منظور ارزیابی قابلیت اعتماد و استقلال سامانه هویت دیجیتال تشریح می‌کند. این قسمت همچنین یک فرایند تصمیم‌گیری را برای نهادهای قانونی، به‌عنوان راهنمای تصمیم‌گیری درباره اینکه استفاده از

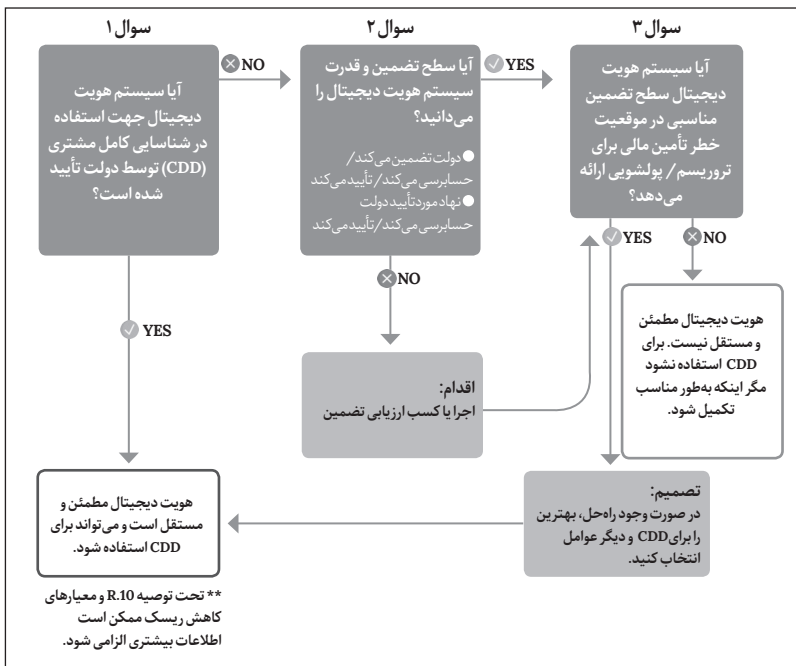
1. ongoing due diligence

2. technology-neutral

3. Fraud

هویت دیجیتال برای برآورده شدن برخی عناصر «شناسایی کامل مشتری» مطابق توصیه شماره ۱۰ مستند FATF مناسب است یا خیر، تعیین می‌کند. دولت‌ها و نهادهای قانونی باید این فرایند تصمیم‌گیری را با شرایط خاص حوزه قضایی و نهادهای شخصی تطبیق دهند. بسته به سامانه‌های هویت دیجیتال و چهارچوب نظارتی در یک حوزه قضایی خاص، دولت‌ها و نهادهای قانونی ممکن است نقش‌ها و مسئولیت‌های متفاوتی در ارزیابی سطوح تضمین یک سامانه هویت دیجیتال و تناسب آن به منظور «شناسایی کامل مشتری» داشته باشند. این موضوع در فلوچارت تصمیم‌گیری برای نهادهای قانونی در همین صفحه منعکس شده است.

۹. این راهنما غیرالزام‌آور است و تصریح می‌کند که استانداردهای کنونی FATF در برابر فناوری بی‌طرف‌اند.



شکل ۱- فرایند تصمیم‌گیری برای نهادهای قانونی

۱۰. بخش چهارم راهنما به برخی از منافع و خطرهای هویت دیجیتال اشاره می‌کند. بسیاری از خطرهای مرتبط با سامانه‌های هویت دیجیتال در اسناد هویتی نیز وجود دارند.

با این حال، اثبات هویت یا احراز هویت اشخاص از طریق شبکه ارتباطی باز (اینترنت) ریسک‌های ویژه‌ای را برای سامانه‌های هویت دیجیتال (خصوصاً در زمینه حملات سایبری و سرقت بالقوه هویت در مقیاس بزرگ) به همراه دارد. از سوی دیگر، سامانه‌های هویت دیجیتال که مطابق چهارچوب‌ها و استانداردهای تضمین هویت دیجیتال، این خطر را کاهش می‌دهند، در خصوص تقویت کنترل‌های «شناسایی کامل مشتری» و مبارزه با پول‌شویی / مقابله با تأمین مالی تروریسم، افزایش شمول مالی^۱، بهبود تجربه مشتری و کاهش هزینه برای نهادهای قانونی، وعده‌ای بزرگ می‌دهند.

۱۱. این راهنما به روش‌هایی می‌پردازد که با استفاده از آن‌ها سامانه‌های هویت دیجیتال برای «شناسایی کامل مشتری» می‌توانند از شمول مالی حمایت کنند. نخست، با استفاده از سامانه‌های هویت دیجیتال، دولت‌ها می‌توانند در ایجاد ویژگی‌ها، مدارک هویتی و فرایندهای اثبات هویت رسمی، از رویکرد انعطاف‌پذیرتر، با تفاوت‌های ظریف‌تر و رو به جلوتر استفاده کنند (از قبیل شناسایی و صحت‌گذاری مشتری پذیرش شده به صورتی که اهداف شمول مالی را تسهیل می‌کند).

دوم، چهارچوب‌ها و استانداردهای تضمین هویت دیجیتال، فرایند انعطاف‌پذیری را برای اثبات هویت و احراز هویت اشخاص ایجاد می‌کنند که این امر می‌تواند برای تحقق اهداف شمول مالی متناسب باشد.

سرانجام، ناظران و نهادهای قانونی، با استفاده از رویکرد مبتنی بر ریسک در مورد «شناسایی کامل مشتری»، با بهره‌گیری از سامانه‌های هویت دیجیتال، مطابق با رویکرد اشاره‌شده در مکمل FATF سال ۲۰۱۷ در مورد «شناسایی کامل مشتری و شمول مالی»، می‌توانند از شمول مالی حمایت کنند.

۱. شمول مالی به‌عنوان در دسترس بودن و برابری فرصت‌ها جهت دسترسی به خدمات مالی تعریف شده است.

توصیه‌هایی برای مقامات دولتی

۱۲. دستورالعمل‌ها و آیین‌نامه‌های واضحی را ایجاد کنید که امکان استفاده مناسب و مبتنی بر ریسک از سامانه‌های هویت دیجیتال مستقل و قابل اعتماد را، از طریق نهادهایی که برای اهداف مبارزه با پول‌شویی / مقابله با تأمین مالی تروریسم تنظیم شده‌اند، می‌دهد. به عنوان نقطه شروع، از سامانه‌های هویت دیجیتال موجود در حوزه قضایی و چگونگی تناسب آن‌ها با نیازهای موجود یا دستورالعمل شناسایی و صحه‌گذاری مشتری و شناسایی کامل مستمر (و نگهداری سوابق مرتبط و الزامات اعتبار شخص ثالث) اطلاع داشته باشید.

۱۳. ارزیابی کنید که آیا آیین‌نامه‌ها و دستورالعمل‌های موجود در مورد «شناسایی کامل مشتری» با تمامی مجوزهای مرتبط با سامانه‌های هویت دیجیتال مطابقت دارند و در صورت لزوم با توجه به حوزه قضایی زیست‌بوم هویت، آن‌ها را اصلاح کنید. برای مثال، مجوزها باید تصریح کنند که استفاده از پذیرش غیر حضوری، سطح استاندارد از ریسک را دربر دارد، یا اگر از سامانه‌های هویت دیجیتال با سطوح تضمین مناسب به منظور شناسایی / صحه‌گذاری و احراز هویت مشتری و شناسایی کامل مشتری استفاده شود، دربردارنده سطح ریسک پایین است.

۱۴. اصول، عملکرد و معیارهای مبتنی بر خروجی را هنگام ایجاد ویژگی‌ها، مدارک و فرایندها جهت اثبات هویت رسمی با اهداف شناسایی کامل مشتری، اتخاذ کنید. سرعت تکامل فناوری دیجیتال، به ارتقای مسئولانه و اثبات‌پذیر در آینده الزامات نظارتی کمک می‌کند.

۱۵. سیاست‌ها، مقررات و روش‌های نظارت و آزمون را اتخاذ کنید که از جریان داده‌ها، معماری فناوری و پردازش در تمام فعالیت‌های هویت دیجیتال، مبارزه با پول‌شویی / مقابله با تأمین مالی تروریسم، ضد تقلب و مدیریت ریسک عمومی جهت تقویت تمامی فعالیت‌های مرتبط با ریسک، استفاده می‌کند و برای نهادهای قانونی امکان توسعه رویکرد مؤثر و یکپارچه «ریسک‌پذیر» را فراهم می‌سازد.

توصیه‌هایی برای مقامات دولتی

۱۶. رویکردی یکپارچه، چندجانبه و با هدف کاهش ریسک به‌منظور درک فرصت‌ها و ریسک‌های مربوط به هویت دیجیتال و تدوین مقررات و دستورالعمل‌ها ایجاد کنید. در صورت لزوم، از چهارچوب‌های تضمین هویت دیجیتال و استانداردهای فنی تصویب‌شده توسط مقامات مسئول برای هویت، امنیت سایبری / محافظت از داده و حفظ حریم خصوصی (نظیر فناوری، امنیت، ملاحظات مربوط به حاکمیت و منابع)، به‌منظور ارزیابی سطوح تضمین سامانه‌های هویت دیجیتال جهت به‌کارگیری در شناسایی کامل مشتری استفاده کنید. در راستای توصیه شماره دو مستند FATF، به‌منظور تسهیل رویکردی جامع و هماهنگ برای درک و پرداختن به ریسک‌ها در اکوسیستم هویت دیجیتال و حصول اطمینان از سازگاری الزامات مبارزه با پول‌شویی / مقابله با تأمین مالی تروریسم در سامانه‌های هویت با قوانین محافظت از داده و حفظ حریم خصوصی، با مسئولان ذی‌ربط همکاری کنید و هماهنگ باشید.

۱۷. مسئولان مبارزه با پول‌شویی / مقابله با تأمین مالی تروریسم می‌توانند با اتخاذ سازوکارهایی جهت تقویت گفت‌وگو و همکاری با ذی‌نفعان بخش خصوصی، نظیر نهادهای قانونی و ارائه‌دهندگان خدمات هویت دیجیتال، به شناسایی فرصت‌های کلیدی مرتبط با هویت، ریسک‌ها و اقدامات کاهش این ریسک‌ها کمک کنند. سازوکارها می‌توانند به‌منظور ایجاد یک محیط نظارتی جهت بررسی ارتباط سامانه‌های هویت دیجیتال با قوانین و مقررات ملی مبارزه با پول‌شویی / مقابله با تأمین مالی تروریسم شامل رویکرد «سندباکس» نظارتی باشند. همچنین مسئولان ذی‌ربط می‌توانند سازوکارهایی را برای ارتقای همکاری میان صنعتی در حوزه شناسایی و رفع آسیب‌های سامانه‌های هویت دیجیتال موجود، ایجاد کنند.

۱۸. از توسعه و اجرای سامانه‌های هویت دیجیتال قابل اعتماد و مستقل حمایت کنید. این کار را از طریق حسابرسی و تصدیق این سامانه‌ها در مقایسه با چهارچوب‌های

توصیه‌هایی برای مقامات دولتی

تضمین هویت دیجیتال شفاف و استانداردهای فنی، یا با کمک نهادهای متخصص^۱ که این خدمات را ارائه می‌دهند، انجام دهید. وقتی مقامات مسئول، خودشان حسابرسی نمی‌کنند یا برای ارائه‌کنندگان خدمات هویت گواهی نامه صادر نمی‌کنند، از آن‌ها خواسته می‌شود از آزمایش تضمین و صدور گواهی نامه توسط نهادهای متخصص مناسب پشتیبانی کنند، به نحوی که صدور گواهی نامه معتبر در حوزه قضایی امکان‌پذیر باشد. از مسئولان خواسته می‌شود از تلاش‌ها جهت هماهنگی چهارچوب‌ها و استانداردهای تضمین هویت دیجیتال به منظور توسعه درک مشترک درباره آنچه یک سامانه هویت دیجیتال «قابل اعتماد و مستقل» را تشکیل می‌دهد، حمایت کنند.

۱۹. هنگام توسعه و اجرای هویت دیجیتال ارائه‌شده توسط دولت، چهارچوب‌های تضمین هویت دیجیتال مناسب و استانداردهای فنی را اعمال کنید. مقامات مسئول باید در مورد نحوه کار سامانه هویت دیجیتال حوزه قضایی و سطوح تضمین آن عملکردی شفاف داشته باشند.

۲۰. یک رویکرد انعطاف‌پذیر مبتنی بر ریسک را برای به کارگیری سامانه‌های هویت دیجیتال به منظور «شناسایی کامل مشتری» ترویج دهید که از شمول مالی پشتیبانی کند. دستورالعمل‌هایی در مورد نحوه استفاده از سامانه‌های هویت دیجیتال با سطوح مختلف تضمین برای اثبات هویت / ثبت نام و احراز هویت جهت «شناسایی کامل مشتری به صورت لایه‌ای» ایجاد کنید.

۲۱. بر تحولات فضای هویت دیجیتال با هدف به اشتراک گذاری دانش، به روش‌ها و ایجاد چهارچوب‌های قانونی در سطح داخلی و بین‌المللی که باعث ارتقای نوآوری مسئولانه می‌شود و انعطاف‌پذیری، کارایی و عملکرد بهتر سامانه‌های هویت دیجیتال، هم به صورت داخلی و هم در سرتاسر مرزها را امکان‌پذیر می‌کند، نظارت کنید.

۱. این نهادهای متخصص صدور گواهی نامه می‌توانند این خدمات را به حوزه قضایی خاص، در سطح منطقه‌ای یا در سطح بین‌المللی انجام دهند.

توصیه‌هایی برای مقامات قانونی

۲۲. اجزای اصلی سامانه‌های هویت دیجیتال، به‌ویژه اثبات و احراز هویت و نحوه اعمال آن‌ها در مورد عناصر الزامی «شناسایی کامل مشتری» را بشناسید (به بخش دوم و پیوست شماره یک مراجعه کنید).

۲۳. یک رویکرد مبتنی بر ریسک آگاهانه به‌منظور اتکا به سامانه‌های هویت دیجیتال برای «شناسایی کامل مشتری» اتخاذ کنید که شامل موارد زیر باشد:
الف. درک سطح / سطوح تضمین سامانه هویت دیجیتال برای اثبات و احراز هویت.

ب. حصول اطمینان از اینکه سطح / سطوح تضمین برای ریسک‌های پول‌شویی / تأمین مالی تروریسم در ارتباط با مشتری، محصول، حوزه قضایی، دسترسی جغرافیایی و مواردی از این دست، مناسب است.

۲۴. توجه کنید که سامانه‌های هویت دیجیتال با سطوح اطمینان پایین‌تر ممکن است در موارد کم‌خطر پول‌شویی / تأمین مالی تروریسم برای شناسایی کامل با پیچیدگی کمتر، از اعتباری مناسب برخوردار باشند. برای مثال، در صورت قانونی بودن، اتخاذ رویکرد «شناسایی کامل مشتری به‌صورت لایه‌ای» که از سامانه‌های هویت دیجیتال با سطوح مختلف تضمین، به‌منظور پشتیبانی از شمول مالی استفاده می‌کند.

۲۵. اگر به‌عنوان یک سیاست یا عملکرد داخلی، ارتباطات کسب‌وکاری یا معاملات غیرحضوری همیشه با ریسک بالا طبقه‌بندی می‌شوند، این سیاست‌ها را مرور و بازنگری کنید و در نظر داشته باشید که معیارهای شناسایی / صحت‌گذاری مشتری که به سامانه‌های هویت دیجیتال مستقل و قابل اعتماد متکی‌اند و اقدامات مناسبی جهت کاهش ریسک انجام می‌دهند، ممکن است ریسک استاندارد یا حتی ریسک پایین‌تری داشته باشند.

۲۶. در صورت لزوم، به‌منظور پشتیبانی از اثبات یا احراز هویت دیجیتال برای اقدامات مبارزه با پول‌شویی / مقابله با تأمین مالی تروریسم فرایندهای

توصیه‌هایی برای نهادهای قانونی

ضدتقلب و امنیت سایبری را به کار بگیرید (شناسایی / صحه‌گذاری مشتری در زمان پذیرش و شناسایی کامل و مستمر و نظارت بر معاملات). برای مثال، نهادهای قانونی می‌توانند به‌منظور جلوگیری از تقلب با استفاده از اقدامات محافظتی موجود در سامانه‌های هویت دیجیتال (به‌عنوان مثال نظارت بر رویدادهای احراز هویت جهت کشف سوءاستفاده سیستماتیک از هویت‌های دیجیتال برای دستیابی به حساب‌ها شامل مفقودی، افشا، دزدی یا فروش اعتبارنامه‌ها / احرازکنندگان هویت دیجیتال)، جهت راهبری دقیق و مستمر ارتباطات کسب‌وکار و همچنین نظارت، کشف و گزارش تراکنش‌های مشکوک به مسئولان، وارد سامانه‌ها شوند.

۲۷. نهادهای قانونی باید اطمینان حاصل کنند که به اطلاعات هویت قانونی و شواهد یا اطلاعات دیجیتالی موردنیاز جهت شناسایی و صحه‌گذاری اشخاص دسترسی دارند یا روندهایی برای امکان دستیابی مسئولان امور به این اطلاعات موجود است. از نهادهای قانونی خواسته می‌شود با سیاست‌گذاران و قانون‌گذاران و همچنین ارائه‌دهندگان خدمات هویت دیجیتال همکاری کنند تا بررسی کنند که چگونه دسترسی به اطلاعات می‌تواند در محیط هویت دیجیتال به‌صورت کارآمد و مؤثر صورت پذیرد.

توصیه‌هایی برای ارائه‌دهندگان خدمات هویت دیجیتال

۲۸. الزامات مبارزه با پول‌شویی / مقابله با تأمین مالی تروریسم برای «شناسایی کامل مشتری» (به‌ویژه شناسایی / صحه‌گذاری و شناسایی کامل و مستمر مشتری) و سایر مقررات مربوط از قبیل الزامات نهادهای قانونی جهت نگهداری گزارش‌های «شناسایی کامل مشتری» را درک کنید.

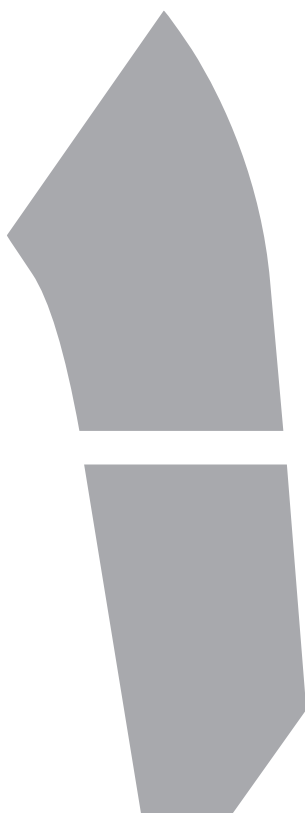
۲۹. به دنبال آزمون تضمین و دریافت گواهی‌نامه از دولت یا متخصص خبره، یا در صورت عدم دسترسی به این موارد، یک نهاد متخصص معتبر بین‌المللی باشید. در صورت وجود،

توصیه‌هایی برای ارائه‌دهندگان خدمات هویت دیجیتال

برای ارزیابی سطوح تضمین سامانه هویت دیجیتال^۱، در «سندباکس‌های» بخش دولتی (و سایر سازوکارهای مربوط) مشارکت کنید.

۳۰. اطلاعاتی شفاف درمورد سطح تضمین سامانه هویت دیجیتال برای اثبات، احراز هویت و در صورت لزوم هم‌پیمانی / قابلیت همکاری را در اختیار متصدیان مبارزه با پول‌شویی / مقابله با تأمین مالی تروریسم قرار دهید.

۱. استاندارد FATF برای نهادهای قانونی (نظیر مؤسسات مالی، ارائه‌دهندگان خدمات مجازی دارایی، مشاغل و حرفه‌های غیرمالی تعیین شده) کاربرد دارد. این راهنما برای برآوردن اهداف FATF به عنوان زمینه مرتبط با ارائه‌دهندگان خدمات احراز هویتی است که به نهادهای قانونی خدمات می‌دهند. در نهایت، این نهادهای قانونی اند که مسئولیت برآوردن الزامات FATF را بر عهده دارند.



بخش اول
معرفی



۳۱. کارگروه اقدام مالی (FATF) متعهد است تضمین کند استانداردهای جهانی مبارزه با پول شویی و مقابله با تأمین مالی تروریسم، نوآوری‌های مسئولانه مالی را ترغیب می‌کنند. در همین راستا، FATF کاملاً از به‌کارگیری فناوری‌های جدید در بخش مالی که با اجرای برنامه‌های استاندارد مبارزه با پول شویی، مقابله با تأمین مالی تروریسم و اهداف شمول مالی همراه است و موجب تقویت آن‌ها می‌شود، حمایت می‌کند.^۱

۳۲. سرعت نوآوری در فضای هویت دیجیتال به نقطه عطف خود رسیده است. فناوری، فرایندها و استانداردهای هویت دیجیتال، به جایگاهی رسیده‌اند که سامانه‌های هویت دیجیتال در دسترس‌اند یا به‌زودی در مقیاس واقعی در دسترس خواهند بود. برخی از این فناوری‌های مربوطه عبارت‌اند از طیف وسیعی از فناوری بیومتریک؛ فراگیری تقریبی اینترنت و تلفن همراه (مانند تکامل سریع و استفاده گسترده از «تلفن‌های همراه» دارای دوربین، میکروفن و دیگر فناوری‌های «تلفن‌های هوشمند»); شناسه‌های دستگاه دیجیتالی و اطلاعات مربوط به آن (برای مثال، نشانی MAC و IP^۲، شماره‌تلفن‌های همراه، سیم‌کارت‌ها، سامانه موقعیت مکانی جهانی^۳ منطقه جغرافیایی); اسکنرهایی با کیفیت بالا (برای اسکن گواهی‌نامه رانندگی، کارت‌های هویتی و سایر مستندات); انتقال ویدئو با وضوح بالا (امکان شناسایی و صحنه‌گذاری و اثبات «زنده بودن» از راه دور); هوش مصنوعی / یادگیری ماشین (برای مثال، برای تعیین اعتبار هویتی که دولت صادر کرده است) و فناوری دفترکل توزیع شده.^۴

مزایای بالقوه

۳۳. سامانه‌های هویت دیجیتال که از استانداردهای پیشرفته فناوری، سازمانی و دولتی برخوردارند، در خصوص پیشرفت قابلیت اعتماد، امنیت، حفظ حریم

۱. به مستند جایگاه FATF در فین‌تک و رگ‌تک (سوم نوامبر ۲۰۱۷) که در این لینک موجود است مراجعه کنید:

<http://www.fatf-gafi.org/publications/fatfgeneral/documents/fatf-position-fintech-regtech.html>

2. MAC addresses identify devices, IP addresses identify connections.

3. GPS

4. DLT

خصوصی و سهولت در شناسایی اشخاص حقیقی در طیف گسترده‌ای از زمینه‌ها، مانند خدمات مالی، بهداشت و درمان و دولت الکترونیکی در اقتصاد جهانی عصر دیجیتالی، نوید بزرگی می‌دهند. این هویت‌های دیجیتال به سامانه‌هایی گفته می‌شود که سطح تضمین بالاتری دارند.

۳۴. در خصوص استانداردهای FATF، سامانه‌های هویت دیجیتال مناسب قابل اعتماد و مستقل می‌توانند:

- شناسایی و صحه‌گذاری مشتری را هنگام پذیرش تسهیل کنند.
- از شناسایی کامل مستمر و بررسی موشکافانه معاملات در طول دوره روابط کسب‌وکار پشتیبانی کنند.
- دیگر اقدامات شناسایی کامل مشتری را تسهیل کنند.
- به نظارت بر معامله به منظور کشف و گزارش معاملات مشکوک و همچنین مدیریت ریسک عمومی و اقدامات ضدتقلب کمک کنند.

۳۵. آن‌ها همچنین ظرفیت کاهش هزینه‌ها و افزایش بهره‌وری برای نهادهای قانونی را دارند و امکان تخصیص مجدد منابع را به منظور سایر عملکردهای مبارزه با پول‌شویی / مقابله با تأمین مالی تروریسم، فراهم می‌کنند.

۳۶. سامانه‌های هویت دیجیتال مستقل و قابل اعتماد^۱ همچنین می‌توانند از طریق امکان اثبات هویت رسمی به اشخاص محروم و غیرمشمول در طیف گسترده‌ای از شرایط، مانند اثبات هویت از راه دور، به منظور دستیابی به خدمات مالی تحت نظارت، در شمول مالی شرکت کنند. آوردن تعداد بیشتری از اشخاص به بخش مالی تحت نظارت، حمایت از مبارزه با پول‌شویی / مقابله با تأمین مالی تروریسم را تقویت می‌کند.

خطرات بالقوه

۳۷. همچنین، سامانه‌های هویت دیجیتال ریسک‌هایی برای پول‌شویی / تأمین

1. reliable, independent

برای خوانش بهتر متن در برخی موارد به جای معادل «معتبر» (trustworthy) از واژه‌های مستقل و قابل اعتماد (reliable, independent) استفاده کرده‌ایم.

مالی تروریسم ایجاد می‌کنند که باید شناخته شوند و کاهش یابند. نهادهای قانونی‌ای که در انجام این کار شکست بخورند، در برآوردن الزامات مندرج در توصیه 10(a) و الزاماتی که تحت استانداردهای FATF است که لازم می‌داند نهادهای قانونی، ریسک پول‌شویی و تأمین مالی تروریسم را شناسایی، ارزیابی و کاهش دهند نیز شکست خواهند خورد. این ریسک‌ها ممکن است در زمینه استفاده از فناوری‌های جدید یا در حال توسعه برای هر دو دسته محصولات جدید و قدیمی ایجاد شوند.^۱

۳۸. این خطرها در بخش چهارم به تفصیل بیان شده‌اند. سامانه‌های هویت دیجیتال در مقیاس بزرگ که سطح تضمین مناسبی ندارند، خطرهای امنیت سایبری ایجاد می‌کنند. برای مثال، اجازه می‌دهند حملات سایبری با هدف غیرفعال کردن دامنه گسترده‌ای از بخش مالی، یا غیرفعال کردن خود سامانه‌های هویت دیجیتال، رخ دهند. آن‌ها همچنین خطرهای عمده‌ای در زمینه حفظ حریم خصوصی، تقلب یا دیگر خطرهای مرتبط با جرایم مالی ایجاد می‌کنند، چراکه نقص در امنیت سایبری ممکن است به سرقت گسترده هویت منجر شود که در این صورت اطلاعات شناسایی شخصی اشخاص^۲ را به خطر می‌اندازد. خطرهای مربوط به حاکمیت، امنیت داده و حریم خصوصی نیز بر معیارهای مبارزه با پول‌شویی / مقابله با تأمین مالی تروریسم تأثیرگذارند. این خطرها در رابطه با اجزای سامانه هویت دیجیتال متفاوت‌اند، اما به دلیل مقیاس احتمالی حملات می‌توانند مخرب‌تر از نقص‌های مرتبط با سامانه‌های هویت سنتی باشند. همان‌طور که در بخش چهارم بیان شده و در بخش پنجم بیشتر درباره‌اش بحث شده است، پیشرفت فناوری و طراحی مناسب فرایندهای اثبات و تأیید هویت می‌تواند به کاهش این خطرها کمک کند.

۳۹. FATF با شناخت مزایا و خطرهای بالقوه سامانه‌های هویت دیجیتال، این راهنما را برای روشن کردن چگونگی استفاده از سامانه‌های هویت دیجیتال به منظور مطابقت با الزامات خاص مبارزه با پول‌شویی / مقابله با تأمین مالی تروریسم تحت استانداردهای خود تهیه کرده است.

1. R.15 (for financial institutions and VASPs) and R.22 (for DNFBPs)

2. Personally Identifiable Information (PII)

هدف و مخاطب مورد نظر

۴۰. این راهنما در پی این است که به سازمان‌های دولتی برای داشتن درکی واضح از چگونگی عملکرد سامانه‌های هویت دیجیتال و روشن ساختن نحوه استفاده از آن‌ها تحت استانداردهای جهانی مبارزه با پول‌شویی / مقابله با تأمین مالی تروریسم کمک کند. این کار شامل سیاست‌گذاران، قانون‌گذاران، ناظران و بازرسان، نهادهای قانونی، مسئولان حریم خصوصی، محافظت از داده، امنیت سایبری (مطابق با موضوع) و دیگر مقامات دولتی مرتبط با اهداف خط‌مشی است (برای مثال، افزایش شمول مالی).

۴۱. این راهنما همچنین در پی کمک به ذی‌نفعان بخش خصوصی، مانند نهادهای قانونی و ارائه‌دهندگان خدمات هویت دیجیتال است. همچنین به سازمان‌های بین‌المللی، سازمان‌های غیردولتی^۱ و سایر اشخاصی مرتبط است که در حوزه تهیه و به‌کارگیری سامانه‌های هویت دیجیتال برای خدمات مالی و کمک‌های بشردوستانه مشارکت دارند.

محدوده

۴۲. این راهنما بر کاربرد توصیه ۱۰ (شناسایی کامل مشتری) در به‌کارگیری سامانه‌های هویت دیجیتال به‌منظور شناسایی / صحه‌گذاری هنگام پذیرش (افتتاح حساب) تحت توصیه 10(a) متمرکز است. همچنین به ظرفیت هویت دیجیتال برای پشتیبانی از شناسایی کامل مستمر (شامل نظارت بر تراکنش‌ها) تحت توصیه 10(d) نگاهی می‌اندازد. از سوی دیگر، به کاربرد توصیه ۱۷ (اعتماد شخص ثالث) در موقعیت‌هایی می‌پردازد که در آن‌ها نهادهای قانونی، سامانه‌های هویت دیجیتال را به‌منظور شناسایی / صحه‌گذاری مشتری به دیگر نهادهای قانونی ارائه می‌کنند.

۴۳. مطابق با اصل بی‌طرفی فناوری، الزامات توصیه ۱۱ (ثبت سوابق) به یک اندازه برای ثبت اسناد به‌صورت دیجیتالی و فیزیکی (مستند) اعمال می‌شود. به‌عنوان یک

1. NGO

موضوع عملی، سامانه‌های هویت دیجیتال ممکن است مسائل متمایزی مربوط به چگونگی نگهداری و دسترسی به اطلاعات مورد نیاز «شناسایی کامل مشتری» را ارائه دهند تا نهادهای قانونی را قادر سازند از الزامات توصیه ۱۱ پیروی کنند. رویکردهای ثبت سابقه در حوزه هویت دیجیتال، با توجه به نوع و طراحی سامانه‌های هویت دیجیتال، انواع و مسئولیت‌های ارائه‌دهندگان سازنده آن و چهارچوب‌های نظارتی و قراردادی مربوط در حوزه قضایی متفاوت خواهد بود. برای مثال، هنگامی که دولت‌ها سامانه‌های هویت دیجیتال را تهیه می‌کنند، مدارک هویتی بنیادی (اسناد منبع، اطلاعات و داده) را برای اثبات / ثبت نام هویت، جمع‌آوری یا ایجاد می‌کنند، بنابراین انتظار می‌رود برای اهداف اجرای قانون، یا نظارت، به این اطلاعات دسترسی داشته باشند و به این ترتیب مقاصد توصیه ۱۱ را برآورده می‌کنند. وقتی نهادهای قانونی از سامانه‌های هویت دیجیتالی استفاده می‌کنند که ارائه‌دهندگان غیردولتی تهیه کرده‌اند ممکن است ارائه‌دهندگان هویت دیجیتال، یا دیگر نهادها، کل یا جزئی از مدارک هویتی بنیادی را حفظ کنند. افزون بر این، ارائه‌دهندگان خدمات هویت دیجیتال بخش خصوصی ممکن است تمام یا بخشی از اطلاعات هویتی بنیادی را مستقیماً از منبع دیجیتالی (برای مثال، بانک اطلاعاتی دولتی یا سوابق مربوط به بخش خصوصی) به دست آورند یا تأیید کنند. در این حالت ممکن است سوابق دیجیتالی، انواع مدارک هویتی را که به‌منظور شواهد خاص از آن‌ها استفاده شده است، مشخص کنند، از قبیل منبع داده، تاریخ / زمان و روش دستیابی به آن، که ممکن است با توصیه ۱۱ مطابقت داشته باشد. این موارد به‌طور مناسب توسط مقامات در چهارچوب‌های نظارتی هویت دیجیتال و مبارزه با پول‌شویی / مقابله با تأمین مالی تروریسم خود و همچنین نهادهای قانونی از طریق نمایندگی استاندارد و روابط قراردادی ارائه‌دهنده خدمات مالی بررسی می‌شوند. بر این اساس، ثبت سوابق و چنین الزاماتی بیشتر از این در راهنما مورد توجه قرار نمی‌گیرند.

۴۴. این دستورالعمل بر شناسایی مشتریانی متمرکز است که شخص (اشخاص) حقیقی‌اند. این راهنما استفاده از سامانه‌های هویت دیجیتال را به‌منظور کمک به شناسایی و صحه‌گذاری هویت نماینده(های) شخص حقوقی به‌عنوان بخشی از عمل

شناسایی/ صحنه‌گذاری مشتریان حقوقی بررسی نمی‌کند، یا برای کمک به انجام دادن دیگر عناصر شناسایی کامل مشتری نیست، به‌ویژه شناسایی و صحنه‌گذاری هویت مالکان منافع تحت توصیه 10(b)، یا جهت درک و به دست آوردن اطلاعات بر اساس هدف و ماهیت تعیین‌شده رابطه تجاری تحت توصیه 10(c) نیست، گرچه سامانه‌های هویت دیجیتال مستقل و قابل اعتماد برای همه عملکردهای شناسایی کامل مشتری مهم‌اند.

۴۵. این راهنما سامانه‌های هویت دیجیتال ارائه‌شده توسط دولت یا به نمایندگی دولت^۱ و بخش خصوصی را دربر می‌گیرد. با توجه به سامانه‌های هویت دیجیتال ارائه‌شده توسط دولت، راهنما بر سامانه‌های هویت دیجیتال همه‌منظوره (هویت معتبر به منظور اثبات هویت قانونی برای همه یا بیشتر اهداف در حوزه قضایی) متمرکز است. اگرچه درباره هویت خاص منظوره (هویت معتبر برای یک هدف خاص) نیز بحث می‌کند، مثل ثبت نام تأمین اجتماعی یا دیگر پایگاه‌های داده، هنگامی که دولت به کارگیری آن‌ها را برای اهداف «شناسایی کامل مشتری» مجاز می‌کند و در اختیار نهادهای قانونی و ارائه‌دهندگان خدمات هویت دیجیتال قرار می‌دهد. اطلاعات بیشتر در مورد نوع سامانه‌های هویت دیجیتال تحت پوشش این راهنما، در بخش دوم آمده است.

۴۶. این راهنما برای ارزیابی استقلال یا قابلیت اطمینان سامانه‌های هویت دیجیتال از نظر فنی، فرایندها و معماری آن‌ها، چهارچوب‌های تضمین یا استانداردهای فنی ایجاد نمی‌کند. در عوض، بر چهارچوب‌های تضمین هویت دیجیتال و استانداردهای فنی (که به آن‌ها استانداردها و چهارچوب‌های تضمین هویت دیجیتال گفته می‌شود) متکی است که دیگر سازمان‌ها در حوزه‌های قضایی متفاوت توسعه داده‌اند یا در حال توسعه هستند. برای خواندن توضیحات در مورد استانداردهای فنی به بخش دوم و برای کسب اطلاعات بیشتر به بخش پنجم و

۱. سامانه هویت دیجیتال زمانی «به نمایندگی از دولت» اطلاق می‌شود که دولت با نهادهای غیردولتی، مانند کمیساریای عالی پناهندگان سازمان ملل متحد (UNHCR)، قرارداد یا تفاهم‌نامه‌ای منعقد کند، یا مجوز تأمین و عملیاتی کردن سامانه هویت دیجیتال را به آن بدهد. در این حالت باز یگر غیردولتی، با توجه به این عملیات هویتی، نمایندگی از دولت را بر عهده دارد.

پیوست شماره پنج مراجعه کنید.

۴۷. این راهنما شامل پنج پیوست و یک واژه‌نامه، همراه با فهرستی برای مطالعه بیشتر است.

- پیوست یک: تعریف یک سامانه هویت دیجیتال پایه و مشارکت‌کنندگان در آن: حاوی مرور کامل تر مفاهیم مطرح‌شده در بخش پنجم راجع به اجزای یک سامانه هویت دیجیتال است.
- پیوست دو: بررسی‌های موردی: حاوی مثال‌هایی درباره استفاده از هویت دیجیتال در حوزه‌های مختلف، شامل «شناسایی کامل مشتری» و دسترسی به سرویس‌های مالی است.
- پیوست سه: اصول مربوط به شناسایی در توسعه پایدار: حاکمیت/ پاسخ‌گویی، حفظ حریم خصوصی و سایر موارد عملیاتی را برجسته می‌کند که حوزه‌ها و سازمان‌های مختلف بررسی‌شان می‌کنند.^۱
- پیوست چهار: چهارچوب تضمین هویت دیجیتال و نهادهای تنظیم‌کننده استاندارد فنی: فهرستی از تعدادی سازمان تنظیم‌کننده استاندارد (شامل سازمان‌های ملی و منطقه‌ای) که چهارچوب‌ها و استانداردهای تضمین هویت دیجیتال را توسعه داده‌اند.
- پیوست پنج: بررسی اجمالی استانداردهای فنی و چهارچوب‌های تضمین هویت دیجیتال آمریکا و اتحادیه اروپا: جزئیات چهارچوب‌های ملی و منطقه‌ای تضمین هویت دیجیتال در آمریکا و اتحادیه اروپا را ارائه می‌دهد.
- واژه‌نامه: توضیح واژه‌های هویت دیجیتالی که در این راهنما از آن‌ها استفاده شده است.

۱. این اصول از طریق یک فرایند مشارکتی ایجاد شده و ۲۵ شریک توسعه، سازمان‌های بین‌المللی، سازمان‌های غیردولتی، انجمن‌های بخش خصوصی و نهادهای دولتی، آن را تأیید کرده‌اند.



بخش دوم

واژه‌شناسی هویت دیجیتال و

ویژگی‌های کلیدی

«هویت» در اهداف این راهنما چیست؟

مفهوم هویت رسمی

۴۸. هویت، مفهومی پیچیده با معانی بسیار است. هویت برای اهداف FATF و در ارتباط با توصیه 10(a) (برای مثال، «شناسایی مشتری و صحه‌گذاری هویت مشتری») به هویت رسمی^۱ اشاره می‌کند که مفهومی گسترده‌تر از هویت شخصی و اجتماعی دارد که ممکن است برای اهداف غیررسمی (به‌عنوان مثال، تعامل تجاری کنترل نشده یا اجتماعی و فردبه‌فرد با اشخاص یا از طریق اینترنت) مرتبط باشد. این راهنما کاربرد سامانه‌های هویت دیجیتال را برای اثبات «هویت رسمی» به‌منظور دسترسی به خدمات مالی پوشش می‌دهد.

۴۹. برای اهداف این راهنما هویت رسمی مشخصات یک شخص یکتای حقیقی است که:

- الف. مبتنی بر خصوصیات (ویژگی‌ها یا شناسه‌ها) شخصی است که یکتا بودن شخص را در جمعیت یا زمینه(های) خاص ایجاد می‌کند.
- ب. از جانب دولت برای اهداف نظارتی و سایر اهداف رسمی به رسمیت شناخته شده است.

اثبات هویت رسمی

۵۰. اثبات هویت رسمی به‌طور کلی به شکلی از ثبت نام، اسناد یا گواهی‌نامه‌های ارائه‌شده یا صادرشده توسط دولت بستگی دارد (برای مثال، شناسنامه یا کارت هویت یا اعتبارنامه هویت دیجیتال) که شواهدی از خصوصیات اصلی (برای مثال، نام و تاریخ و محل تولد) را برای اثبات و صحه‌گذاری هویت رسمی تشکیل می‌دهد.

۵۱. معیارهای اثبات «هویت رسمی» در حوزه قضایی می‌تواند متفاوت باشد. دولت‌ها در اعمال حق حاکمیت خود، ویژگی‌ها، شواهد و فرایندهای لازم را برای اثبات هویت رسمی تعیین می‌کنند. این عوامل می‌توانند با گذشت زمان تغییر کنند. با تکامل فناوری

1. official identity

و مفاهیم فرهنگی هویت، دولت‌ها ممکن است ویژگی‌های مختلفی را مجاز بدانند. در تعیین معیارهای اثبات هویت رسمی، دولت‌ها می‌توانند از رویکرد ثابت، تجویزی، مبتنی بر قواعد یا رویکرد دیگری بر اساس اصول، عملکرد یا مبتنی بر نتایج استفاده کنند. رویکرد دوم انعطاف‌پذیرتر است. پیشرفت سریع فناوری و استانداردها، حوزه‌های قضایی را برای ایجاد الزامات اثبات‌پذیر در آینده و پشتیبانی از نوآوری مسئولانه آماده می‌سازد.

۵۲. در اتحادیه اروپا، اتکا به چهارچوب‌های تضمین مشترک، اعضای اتحادیه اروپا را قادر می‌سازد ملزومات ملی متفاوتی را تطبیق دهند، مثل پذیرش انواع مختلف روش‌ها و اسناد هویت در دسترس ملی، به شرط آنکه نتیجه با ملزومات چهارچوب eIDAS مطابقت داشته باشد. بسته به زمینه‌ای که جنبه‌ای از مدارک هویتی باید در آن تأیید شود، منابع معتبر هویت می‌توانند از میان دیگر موارد، اشکال مختلفی مثل ثبت نام‌ها، مستندات و نهادهای مربوط را به خود اختصاص دهند. منابع معتبر می‌توانند حتی در یک زمینه مشابه در کشورهای مختلف اتحادیه اروپا متفاوت باشند، ولی چهارچوب eIDAS امکان هماهنگی و شناخت متقابل را فراهم می‌کند. هم‌اکنون سازمان بین‌المللی استاندارد (ISO)^۱ در حال تدوین استانداردهای جهانی به منظور شناسایی اشخاص حقیقی برای خدمات مالی، از جمله حوزه دیجیتالی، است.

۵۳. در اکثر کشورها اثبات هویت رسمی از طریق سامانه‌های هویت همه‌منظوره (بعضی اوقات به عنوان سامانه‌های هویت بنیادی شناخته می‌شوند)، مانند شناسه ملی و سامانه‌های ثبت احوال، فراهم می‌شود. این سامانه‌ها معمولاً اسناد یا اعتبارنامه‌های دیجیتالی ارائه می‌دهند که به طور گسترده توسط سازمان‌های دولتی و ارائه‌دهندگان خدمات بخش خصوصی به عنوان اثبات هویت رسمی برای اهداف مختلف، شناخته و پذیرفته می‌شوند. همه حوزه‌های قضایی سامانه‌های هویت همه‌منظوره ندارند.

۵۴. حوزه‌های قضایی همچنین به طور معمول انواع مختلفی از سامانه‌های هویت «خاص منظوره» (که به آن سامانه‌های هویت کاربردی نیز گفته می‌شود) دارند که برای ارائه شناسایی، احراز هویت و مجوز به منظور خدمات یا بخش‌های خاص، مانند اداره

۱. گروه مشاوران استاندارد ISO، کمیته فنی ۶۸، کارگروه ۷

امور مالیاتی، دسترسی به مزایا و خدمات خاص دولت، رأی دادن، اجازه کار با وسیله نقلیه موتوری و (در بعضی از حوزه‌های قضایی) دسترسی به خدمات مالی و غیره تهیه شده‌اند. نمونه‌هایی از مدارک هویتی خاص منظوره عبارت‌اند از (اما به آن‌ها محدود نمی‌شوند): شماره شناسایی مؤدیان مالیاتی، گواهی‌نامه رانندگی، گذرنامه‌ها، کارت‌های ثبت‌نام رأی‌دهندگان، شماره‌های تأمین اجتماعی و اسناد هویت پناهندگان. در برخی موارد نیز (به‌ویژه در کشورهای که سامانه هویت همه‌منظوره ندارند) می‌توان از این سامانه‌های کاربردی و اعتبارنامه‌ها برای اثبات هویت رسمی استفاده کرد.

۵۵. معمولاً اثبات هویت رسمی توسط دولت، یا از طرف دولت‌ها ارائه شده است. در عصر دیجیتالی، ما شاهد مدل‌های جدیدی هستیم که اعتبارنامه‌های دیجیتالی ارائه‌شده از طریق یا با همکاری بخش خصوصی، توسط دولت به‌عنوان اثبات رسمی هویت در یک محیط آنلاین (برای مثال، NemID در دانمارک)، در کنار اعتبارنامه‌های دیجیتالی سنتی صادرشده توسط دولت (برای مثال، هویت ملی الکترونیکی) شناخته می‌شوند.

۵۶. درمورد پناهندگان، اثبات هویت رسمی نیز ممکن است توسط یک سازمان بین‌المللی شناخته‌شده با چنین وظیفه‌ای ارائه شود.^۱ به کادر شماره ۸ مراجعه کنید.

سامانه هویت دیجیتال در اهداف این راهنما چیست؟

۵۷. سامانه‌های هویت دیجیتال از ابزارهای الکترونیکی برای ادعا و اثبات هویت رسمی یک شخص در محیط آنلاین (دیجیتالی) یا محیط‌های حضوری در سطوح مختلف تضمین استفاده می‌کنند.

۵۸. تمرکز این دستورالعمل بر سامانه‌های هویت دیجیتال سرتاسری^۲ است (سامانه‌هایی که فرایند اثبات هویت/ ثبت‌نام و احراز هویت را پوشش می‌دهند). سامانه‌های هویت دیجیتال می‌تواند شامل مدل‌های عملیاتی مختلفی باشد و ممکن است به نهادها و انواع فناوری، روندها و معماری‌های مختلف متکی باشد. در این راهنما

۱. به کنوانسیون ۱۹۵۱ درمورد وضعیت پناهندگان، ماده ۲۵ و ۲۷ و اساسنامه ۱۹۵۰ دفتر کمیساریای عالی سازمان ملل در امور پناهندگان مراجعه کنید.

2. end-to-end digital ID systems

منظور از سامانه‌های هویت دیجیتال، سامانه جامع هویت دیجیتال است، نه اجزای آن. ۵۹. همه عناصر یک سامانه هویت دیجیتال لزوماً دیجیتالی نیستند. برخی از عناصر اثبات هویت و مؤلفه ثبت نام می‌توانند به صورت دیجیتالی یا فیزیکی (مستند) یا ترکیبی باشند. ولی اتصال^۱، صدور اعتبارنامه^۲، احراز هویت^۳، قابلیت حمل / هم‌پیمانی^۴ (هرجا که عملی است) باید دیجیتالی باشد. این مفاهیم در بخش بعدی بیشتر توضیح داده شده‌اند.

۶۰. سامانه‌های هویت دیجیتال می‌تواند به روش‌های مختلفی از فناوری دیجیتال استفاده کند. مانند و نه محدود به مثال‌های زیر:

- بانک اطلاعاتی الکترونیکی شامل دفترکل توزیع شده به منظور به دست آوردن، تأیید، ذخیره یا مدیریت مدارک هویتی؛
- اعتبارنامه‌های دیجیتالی به منظور تصدیق هویت برای دسترسی به برنامه‌های تلفن همراه، آنلاین و آفلاین؛
- بیومتریک برای کمک به شناسایی یا تأیید هویت اشخاص؛
- رابط‌های برنامه کاربردی^۵ دیجیتال، پلتفرم‌ها و پروتکل‌هایی که شناسایی / صحه‌گذاری و احراز هویت آنلاین را سهولت می‌بخشند.

اجزای کلیدی یک سامانه هویت دیجیتال چیست؟

۶۱. همان‌طور که در دستورالعمل هویت دیجیتال NIST منعکس شده است، سامانه‌های هویت دیجیتال شامل دو جزء اصلی و یک جزء سوم اختیاری هستند که در زیر آمده است. اشخاص مختلف، مانند ترکیبی از نهادهای دولتی و بخش خصوصی، می‌توانند مسئول عملکرد اجزای فرعی باشند. اصطلاحات به کاررفته توسط حوزه قضایی و سازمان‌های مختلف ممکن است بسته به توصیف سامانه، کمی متفاوت باشند. توضیحات دقیق‌تر درباره هریک از مراحل در «پیوست شماره یک: تعریف یک

1. binding
 2. credentialing
 3. authentication
 4. portability/federation
 5. Application Programming Interfaces (APIs)

سامانه هویت دیجیتال پایه و مشارکت‌کنندگان آن» وجود دارد.

جزء اول: اثبات هویت و ثبت نام (با صحت اولی / اعتبارسنجی) - (ضروری)

۶۲. این جزء به این پرسش پاسخ می‌دهد: شما چه کسی هستید؟ و شامل جمع‌آوری، اعتبارسنجی و تأیید مدارک هویتی و اطلاعات مربوط به شخص است: ایجاد یک حساب هویتی (ثبت نام) و اتصال هویت یکتای شخص به احرازکنندگان هویت در مالکیت و کنترل شخص.

۶۳. این جزء مستقیم و آنی با الزامات شناسایی / صحه‌گذاری مطابق با بند 10(a) مرتبط است (بخش سوم را ببینید).



شکل ۲- اثبات هویت و ثبت نام

توجه: نمودار صفحه قبل فقط برای تصویرسازی است. مراحل اثبات هویت و ثبت نام می‌توانند با ترتیب دیگری انجام شوند. هدف، شناسایی و تأیید شخص و اتصال هویت به احرازکنندگان هویت است. برای توضیحات بیشتر درمورد اصطلاحات کلیدی به کاررفته در این نمودار، به پیوست شماره یک مراجعه کنید.

۶۴. فقط به منظور تصویرسازی، برخی از نمونه اقدامات انجام شده در جزء اول می‌تواند شامل موارد زیر باشد:

- **جمع‌آوری^۱:** ارائه و جمع‌آوری ویژگی‌ها و شواهد هویتی، چه به صورت حضوری چه آنلاین (برای مثال، با پرکردن یک فرم آنلاین، ارسال عکس شخصی، آپلود عکس‌های مستنداتی مثل گذرنامه یا گواهی نامه رانندگی و غیره).
- **اعتبارسنجی^۲:** بازرسی دیجیتالی یا فیزیکی به منظور حصول اطمینان از موثق بودن مستندات و صحیح بودن داده یا اطلاعات آن (برای مثال، بررسی ویژگی‌های امنیتی فیزیکی، تاریخ انقضا و صحت‌گذاری ویژگی‌ها از طریق سایر خدمات).
- **تکرارزدایی^۳:** مشخص کنید ویژگی‌ها و شواهد هویتی به یک شخص یکتا در سامانه هویت دیجیتال مربوط است (برای مثال، از طریق جست‌وجوی گزارش‌های تکراری، شناسایی بیومتریک یا الگوریتم‌های تکرارزدایی).
- **صحت‌گذاری^۴:** مرتبط‌سازی شخص به شواهد هویتی ارائه شده (برای مثال، استفاده از راهکارهای بیومتریک مثل تشخیص چهره و تشخیص زنده بودن).
- **ثبت نام در حساب هویتی و اتصال^۵:** یک حساب هویتی ایجاد و آن را منتشر کنید و یک یا چند احرازکننده هویت را به حساب هویتی متصل کنید (برای مثال، گذرواژه‌ها، ایجادکننده کد یک بار مصرف (OTC)^۶) روی تلفن‌های همراه، کارت‌های

1. Collection
 2. Validation
 3. De-duplication
 4. Verification
 5. Enrolment in identity account and binding
 6. one time code (OTC)

هوشمند زیرساخت کلید عمومی (PKI)^۱ گواهی‌نامه‌های FIDO و غیره). این فرایند، احراز هویت را امکان‌پذیر می‌کند (مطالب زیر را مشاهده کنید).

جزء دوم: احراز هویت و مدیریت چرخه هویت (ضروری)

۶۵. احراز هویت به این پرسش پاسخ می‌دهد: آیا شما شخصی هستید که شناسایی و صحه‌گذاری شده است؟ احراز هویت بر اساس تملک و کنترل احرازکنندگان هویت، این امر را تأیید می‌کند، شخصی که ادعای هویت می‌کند (مشتری پذیرش شده یا مدعی) همان شخصی است که اثبات هویت شده و ثبت نام کرده است.

۶۶. سه نوع عامل وجود دارند که می‌توان برای احراز هویت اشخاص از آن‌ها استفاده کرد (به شکل سه در صفحه بعد رجوع شود): ۱. عامل‌های مالکیتی (چیزی که در دست شماست مانند کلیدهای رمزنگاری)؛ ۲. عامل‌های دانشی (چیزی که شما می‌دانید مانند کلمه عبور)؛ ۳. عامل‌های ذاتی (چیزی که شما هستید مانند عوامل بیومتریک)^۲.

۶۷. احراز هویت می‌تواند به انواع مختلف عوامل و پروتکل‌ها یا فرایندهای احراز هویت تکیه کند. این عوامل احراز هویت دارای سطوح مختلف امنیتی است (به بحث ریسک‌های احراز هویت در بخش پنجم رجوع کنید). معمولاً فقط یک عامل احراز هویت، به تنهایی به اندازه کافی قابل اعتماد تلقی نمی‌شود. یک فرایند احراز هویت معمولاً هنگامی قابل اعتمادتر و قدرتمندتر تلقی می‌شود که گونه‌های متعددی از عوامل احراز هویت را در نظر بگیرد.^۳

1. Public Key Infrastructure (PKI)

۲. وقتی راهنمای اجزای احراز هویت را بیان می‌کند، این احراز همان «احراز هویت قوی مشتری (SCA)» تحت چهارچوب قانونی اتحادیه اروپا نیستند. اینکه چه چیزی یک عامل SCA معتبر را با توجه به بخش‌نامه PSD2 (2015/2366 (EU) تشکیل می‌دهد یا نمی‌دهد باید مطابق PSD2 و استانداردهای فنی رگولاتوری برای احراز هویت قوی مشتری و ارتباط امن تحت PSD2 (RTS on SCA & CSC) ارزیابی شود و نه راهنمای FATF.

۳. با تکامل سیستم‌های هویت دیجیتال، این درک ظریف‌تر می‌شود. جایی که احراز هویت فعال و مستمر است، قدرت احراز هویت گاهی نه با توجه به تعداد مختلف عوامل و انواع احراز هویت، بلکه با توجه به نیرومندی کلی ارزیابی می‌شود. نیرومندی کلی که به دلیل استفاده از چند منبع پویا و دیجیتال داده مشتری، شامل کانال‌های ورود به سامانه موردانتظار، منطقه جغرافیایی، فراوانی استفاده، نوع استفاده، آدرس‌های IP و الگوهای رفتاری بیومتریک مکانیکی حاصل می‌شود.

آنچه یک شخص



شکل ۳- عوامل متعارف احراز هویت

کادر ۱- نقش احراز هویت در شناسایی کامل مشتری و دیگر معیارهای مبارزه با پول شویی / مقابله با تأمین مالی تروریسم

- هنگامی که شخصی در سامانه هویت دیجیتال اثبات هویت می‌شود و ثبت‌نام می‌کند می‌تواند از اعتبارنامه و احرازکنندگان هویت متصل شده به هویت خود استفاده کند تا این هویت را به شخص ثالث، «طرف وابسته» (یک نهاد قانونی) «اظهار» کند. در حالی که قدرت فرایند اثبات هویت و ثبت‌نام، سطح اطمینانی را درمورد صحت اطلاعات هویت برای «طرف وابسته» فراهم می‌کند (برای مثال، ویژگی‌هایی مانند نام و سن صحیح است و مربوط به یک

شخص واقعی‌اند)، روند احراز هویت به «طرف وابسته» اطمینان می‌دهد که شخص ارائه‌دهنده اعتبار، واقعاً شخصی است که صاحب آن است، نه یک دزد یا جاعل. بنابراین، توانایی سامانه‌های هویت دیجیتال برای احراز هویت شخص، مؤلفه مهمی از عملکرد آن‌هاست و توسط نهادهای قانونی می‌تواند به‌عنوان بخشی از فرایند شناسایی / صحه‌گذاری «شناسایی کامل مشتری» در افتتاح حساب مورد استفاده قرار گیرد.

- توجه داشته باشید که «احراز هویت» مشتریان موجود نیز یک اقدام امنیتی مهم برای شناسایی مستمر و مجوز دسترسی به حساب است. در بعضی موارد، نهادهای قانونی ممکن است از همان اعتبارنامه‌های هویت دیجیتال و خدمات احراز هویت استفاده شده هنگام افتتاح حساب برای مجوز دسترسی به حساب استفاده کنند، اما لزوماً این‌گونه نیست. برای مثال، بسیاری از نهادهای قانونی، اعتبارنامه‌ها/ احرازکنندگان هویت خود را صادر می‌کنند (برای مثال، پین‌ها و توکن‌ها برای ورود به حساب‌های آنلاین) یا این‌ها را متصل می‌کنند به احرازکنندگان هویت روی دستگاه موجود در تلفن‌های همراه یا مرورگرها (برای مثال، استفاده از استانداردهای FIDO).

۶۸. مدیریت چرخه حیات هویت به اقداماتی گفته می‌شود که باید در واکنش به رویدادهایی که می‌توانند حین چرخه حیات هویت رخ دهند و بر استفاده، امنیت و اعتبار احرازکنندگان هویت تأثیرگذار باشند، انجام شود. برای مثال، مفقودی، دزدی، تکثیر غیرمجاز، انقضا و ابطال احرازکنندگان هویت یا اعتبارنامه‌ها.

جزء سوم: سازوکار قابلیت‌های حمل و قابلیت تعامل (اختیاری)

۶۹. سامانه‌های هویت دیجیتال می‌تواند شامل جزئی باشد که امکان قابلیت حمل اثبات هویت را فراهم کند. هویت قابل حمل به این معناست که می‌توان از اعتبارنامه‌های هویت دیجیتال شخص برای اثبات هویت رسمی ارتباطات جدید

مشتری در بخش‌های خصوصی نامرتبط یا اشخاص دولتی استفاده کرد، بدون اینکه آن‌ها مجبور باشند داده‌های شخصی را به دست آورند و صحت‌گذاری کنند و هر بار شناسایی / صحت‌گذاری مشتری را انجام دهند. داشتن قابلیت حمل می‌تواند از طریق معماری و پروتکل‌های مختلف هویت دیجیتال پشتیبانی شود. در اروپا، آیین‌نامه eIDAS، چهارچوبی برای شناسایی متقابل سامانه‌های هویت دیجیتال فراهم می‌کند.

۷۰. هم‌پیمانی یکی از راه‌هایی است که امکان قابل حمل بودن هویت رسمی را فراهم می‌کند. این روش به استفاده از معماری هم‌پیمان و پروتکل‌های ادعا برای حمل اطلاعات هویتی و احراز هویت از طریق مجموعه‌ای از سامانه‌های شبکه‌شده اشاره دارد. این روش، قابلیت همکاری و تعامل در شبکه‌های مجزا را فراهم می‌کند. در انگلستان، GOV.UK Verify نمونه‌ای از هویت دیجیتال هم‌پیمان شده است (به کادر ۱۶ مراجعه کنید).

چهارچوب‌های تضمین هویت دیجیتال و استانداردهای فنی

۷۱. چهارچوب‌های تضمین و استانداردهای فنی برای قابلیت اطمینان فناوری هویت دیجیتال، فرایندها و معماری توسعه‌یافته‌اند یا در حال توسعه‌اند:

- حوزه‌های قضایی یا حوزه‌های قضایی فراملی (برای مثال، اتحادیه اروپا، کانادا و استرالیا).

- سازمان‌های استاندارد بین‌المللی یا سازمان‌های خاص صنعتی مثل سازمان بین‌المللی استاندارد (ISO)، کمیسیون بین‌المللی الکترونیک (IEC)، اتحاد هویت سریع آنلاین (FIDO)، بنیاد (OpenID (OIDF)، اتحادیه بین‌المللی ارتباطات از راه دور (ITU) و GSMA.

۷۲. برای مطالعه خلاصه سطح بالای این سازمان‌ها به پیوست شماره چهار: چهارچوب تضمین هویت دیجیتال و نهادهای تنظیم‌کننده استاندارد فنی مراجعه کنید.

۷۳. چهارچوب‌ها و استانداردهای تضمین هویت دیجیتال که در سطح قضایی

تهیه شده‌اند در حال حاضر شماره‌ها/ نام‌های مختلفی را برای سطوح تضمین به کار می‌برند، اما عمدتاً از نظر محتوایی مطابقت دارند. در حال حاضر حوزه‌های قضایی برای برطرف کردن هرگونه اختلاف، استانداردهای فنی هویت دیجیتال مربوط را به یکدیگر نگاشت می‌کنند. در سال ۲۰۱۸، ISO و IEC بین‌المللی، استاندارد بین‌المللی را برای اثبات هویت و ثبت نام اشخاص حقیقی با نام ISO/IEC 29003:2018 منتشر کردند. در حال حاضر ایزو در حال بازنگری در چهارچوب تضمین احراز هویت خود (ISO/IEC 29115:2013) است و به‌کارگیری دستورالعمل‌های مدیریت ریسک (ISO 3100:2018) را برای شناسایی خطرهای مربوط، مورد توجه قرار داده است. علاوه بر این، ایزو در تلاش است که تمامی استانداردهای دیگر ایزو را به منظور ایجاد یک چهارچوب جامع بین‌المللی تضمین هویت دیجیتال به‌روزرسانی و هم‌راستا کند.

۷۴. با توجه به استانداردهای در حال رشد، این راهنما بارها به دستورالعمل‌های هویت دیجیتال NIST و چهارچوب eIDAS اشاره می‌کند. متخصصان مبارزه با پول‌شویی / مقابله با تأمین مالی تروریسم باید با هم‌تایان خود در هویت دیجیتال، امنیت سایبری و دیگر آژانس‌های مرتبط به‌منظور شناسایی چهارچوب‌ها و استانداردهای کاربردی تضمین هویت دیجیتال همکاری کنند.

۷۵. با پیشرفت فناوری، معماری و فرایندهای هویت دیجیتال، چهارچوب‌ها و استانداردهای فنی تضمین سامانه‌های هویت دیجیتال نیز به رشد و پیشرفت نیاز دارند و احتمالاً از پیشرفت سامانه‌های هویت عقب خواهند ماند. از دولت‌ها و بخش خصوصی خواسته می‌شود که فناوری / فرایندهای رو به رشد هویت دیجیتال را که اثبات یا احراز هویت قوی‌تری را ارائه می‌دهند، به‌دقت ردیابی و به‌جای به‌کارگیری سطوح تضمین بالاتر موجود، برای محدود کردن آن، چهارچوب‌ها و استانداردها را یک ابزار ارزیابی مفید تلقی کنند.