دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۳، جلد ۲۲، شماره ۱ (۶۱-۷۳)
https://monadi.isc.org.ir

مروری بر کاربردهای متعدد استاندارد احراز اصالت فایدو در امنیت فضای تولید و تبادل اطلاعات

مرتضی اسدی*، محمدرضا زمانی و کسری توکلی
شرکت ره آورد سامانه‌های امن (رهـ سا)، تهران، ایران

اطلاعات مقاله

تاریخچه مقاله:
تاریخ دریافت: ۱۵ فروردین ۱۴۰۳
تاریخ پذیرش: ۱۰ شهریور ۱۴۰۳
انتشار آنلاین: ۱۰ شهریور ۱۴۰۳

کلمات کلیدی:
احراز اصالت چند عاملی
فایدو
رمزنگاری نامتقارن
زیست سنجی
بی‌نیاز از گذرواژه

نوع مقاله: فنی و ترویجی

چکیده

گذرواژه‌ها به عنوان اولین راهکار احراز اصالت همزمان با پیدایش شبکه جهانی اینترنت و ارائه خدمات برخط مورد استفاده قرار گرفته‌اند. مخاطرات امنیتی استفاده از گذرواژه‌ها و آسیب‌پذیری آنها در برابر انواع حملات سایبری، باعث شده است که دیگر این شیوه امن نباشد. طی سال‌های اخیر ارائه‌دهندگان خدمات برخط تلاش کرده‌اند با استفاده از انواع روش‌های احراز اصالت چندعاملی از کاربران و داده‌های خود در برابر حملات سایبری محافظت نمایند. اگرچه این روش‌ها در کاهش آمار وقوع رخنه‌های امنیتی موفق بوده‌اند، عموما منجر به ایجاد پیچیدگی بیشتر برای کاربران نیز گردیده‌اند. استاندارد فایدو با استفاده از رمزنگاری نامتقارن و الزام ذخیره‌سازی کلیدخصوصی در ابزار کاربر و ترکیب آن با عوامل زیست‌سنجی، احراز اصالت را به امن‌ترین روش ممکن برای سامانه‌ها و ساده‌ترین راه برای کاربران انجام می‌دهد. این استاندارد با وضع قوانینی در سیستم عامل‌ها، مرورگرها و ابزارهای احراز اصالت، تمام روند احراز اصالت را رصد و از خطرات احتمالی جلوگیری می‌کند. شرکت ره‌آورد سامانه‌های امن با پیاده‌سازی این استاندارد به صورت بومی، احراز اصالت فایدو را تحت عنوان محصول نشانه برای تلفن‌های همراه هوشمند ارائه داده است که در این مقاله، کاربردها، مشخصات و قابلیت‌های این استاندارد و محصول تهیه شده اشاره می‌شود.

۱ مقدمه

در حالی که ما در حال گذار به اقتصاد دیجیتال [1] هستیم، امنیت سایبری در تعاملات برخط امری حیاتی است. به کارگیری روش‌ها و روندهایی که برای حفاظت اطلاعات بوجود آمده و در شرف تکوین هستند، در موفقیت این تحول دیجیتالی نقش اساسی ایفاء می‌کنند.

شرکت ره‌آورد سامانه‌های امن (رهسا) از بدو تاسیس تمرکز خود را بر تولید و عرضه محصولات و ارائه خدمات سخت‌افزاری و نرم‌افزاری در حوزه امنیت فضای تبادل اطلاعات (افتا) و به خصوص زیر ساخت کلید عمومی (PKI) و احراز اصالت دیجیتال داشته و همواره فن‌آوری‌های نوین را رصد کرده و خود را با نیازهای این صنعت به‌روز نموده است. با توجه به زمان شروع فعالیت، بدون شک این شرکت یکی از پیشگامان عرصه امنیت اطلاعات و ارتباطات و معرفی‌کننده مفاهیم جدید در این حوزه در کشور است [۱].

در حال حاضر فایدو [2] (FIDO) جدیدترین و امن‌ترین استاندارد احراز اصالت است که علاوه بر بانکداری دیجیتال، کاربردهای بسیاری نیز در سایر زمینه‌های امنیت فضای تولید و تبادل اطلاعات دارد، بطوریکه هر گونه فعالیت در دنیای مجازی و ورود به سامانه‌های مبتنی بر شبکه که نیازمند احراز اصالت و تبادل اطلاعات امن و رمزنگاری شده است را تحت تأثیر قرار می‌دهد [۱-۶].

*نویسنده مسئول
آدرس‌های رایانامه: asadi@rsa.ir (مرتضی اسدی)، reza@rsa.ir (محمدرضا زمانی)، kasra@rsa.ir (کسری توکلی)

[1] Digital Economy

[2] FIDO (Fast Identity Online)

بطور یقین در آینده بسیار نزدیک فایدو به سرعت گسترش یافته و در همه عرصه‌های زندگی ما فراگیر می‌شود. این مقاله قصد دارد با مرور مفاهیم استاندارد و پروتکل فایدو، آینده این فن‌آوری را به تصویر کشیده و کاربردهای آن در بخش‌های مختلف از جمله اداری، صنعتی، بانکی، کسب و کارهای برخط در کشور را بیان نماید.

۲ انجمن فایدو

در سال ۲۰۱۳ انجمن فایدو[1] به عنوان یک سازمان صنعتی باز با هدف ایجاد استانداردهای احراز اصالت و کاهش وابستگی روزافزون به گذرواژه‌ها تاسیس شد. در واقع این انجمن که یک سازمان غیرانتفاعی است با هدف جایگزینی گذرواژه با یک پروتکل امن و سازگار با صنایع که استفاده از آن نیز آسان باشد، شکل گرفته است. انجمن فایدو مجموعه‌ای از مشخصات و پروتکل‌های احراز اصالت امن و مستحکم بصورت ترکیبی از معیارهای زیست سنجی به عنوان عامل اول و تملک به عنوان عامل دوم را منتشر کرده است. در شکل ۱ برخی از مهم‌ترین اعضاء این انجمن نشان داده شده است. تنوع اعضاء در این انجمن مثال‌زدنی است [۷].

لیست شرکت‌ها و مؤسساتی که در انجمن فایدو عضو هستند به مرور زمان افزایش یافته است. در بین این شرکت‌ها می‌توان به سازندگان تراشه‌های الکترونیکی، سازندگان رایانه و گوشی‌های همراه هوشمند، بانک‌ها و شرکت‌های معظم Microsoft، Apple و Google اشاره کرد که همگی عضو این انجمن بوده و تضمین پشتیبانی از آن را در سطح سیستم عامل Windows، MacOS، Android و iOS ارائه داده‌اند.

شکل ۱. برخی از اعضاء انجمن فایدو [۷]

بدین ترتیب استاندارد فایدو روی همه لپ‌تاپ‌ها، رایانه‌ها، تبلت‌ها و گوشی‌های همراه هوشمند قرار دارد. بر اساس اعلامیه انجمن فایدو، بیش از چهار میلیارد دستگاه با پشتیبانی فایدو از ژانویه سال ۲۰۲۲ در سراسر جهان به کار گرفته شده است. این موضوع چالش بزرگی پیش روی ما قرار داده است زیرا بشر هرگز تجربه پشتیبانی گسترده و فراگیر این استاندارد را در رایانه‌ها، لپ‌تاپ‌ها و گوشی‌های همراه خود نداشته است.

همانطور که پیش‌تر نیز ذکر شد، استفاده از گذرواژه[2] می‌تواند تهدید امنیتی جدی برای کاربران سامانه‌ها باشد. استاندارد فایدو، این عوامل تهدید را به دلیل حذف گذرواژه‌ها به حداقل کاهش داده و کاربران می‌توانند

[1]FIDO Alliance [2]Passwordless

ورود به سامانه‌های مورد نظرشان را بی‌نیاز از گذرواژه تجربه کنند. بدین ترتیب استفاده‌کنندگان فایدو می‌توانند به سامانه‌های مورد نظر جهت انجام کارهای شخصی، اداری و تجاری وارد شده و در محیطی کاملاً امن و مطمئن احراز اصالت شوند. با به کارگیری این فن‌آوری هر کسی می‌تواند از کلید امنیتی مبتنی بر فایدو استفاده کرده بطوریکه دیگر نیازی به داشتن گذرواژه‌های متعدد برای ورود به رایانه/لپ‌تاپ و حساب‌های کاربری/خدمات برخط مانند Microsoft، Office، GhitHub یا هر مورد دیگری که زیرساخت فایدو را پشتیبانی می‌کند، نداشته باشد. بطور کلی و خلاصه می‌توان مزایای استفاده از استاندارد فایدو برای احراز اصالت را به شرح زیر بیان کرد [۸]:

- امنیت بالاتر: فرآیند احراز اصالت در سامانه توسط جفت کلید عمومی و خصوصی صورت می‌پذیرد. با توجه به اینکه کلید خصوصی همیشه در ابزار کاربر باقی می‌ماند (این ابزار می‌تواند یک کلید فیزیکی یا هر نوع احرازکننده[3] باشد)، امکان احراز اصالت بدون دسترسی به این کلید یا نسخه‌برداری از آن توسط رخنه‌گر وجود ندارد.
- تجربه کاربری بهتر: وجود گذرواژه‌های متعدد موجب خستگی و سردرگمی کاربران می‌شود. در عوض به کمک روش احراز اصالت فایدو، فقط کافی است که کاربر دکمه‌ای را فشرده و یا از طریق اثرانگشت، تشخیص چهره یا اتصال سخت‌افزار، این کار را جایگزین گذرواژه کند. این قابلیت برای پرسنل فن‌آوری اطلاعات و راهبران شبکه که نیاز به برقراری ارتباط از راه دور با کارسازهای[4] مختلف و استفاده از گذرواژه‌های گوناگون را دارند، بسیار کاربردی است.
- حفاظت در برابر حملات: با استفاده از استاندارد فایدو دیگر نباید نگران حملات صیادی[5]، فرد در میان[6] و فرد در مرورگر[7] بود. در صورتی که رخنه‌گرها گذرواژه را نیز در اختیار بگیرند، نمی‌توانند به حساب کاربری حفاظت شده توسط فایدو، دسترسی پیدا کنند.
- استفاده گسترده و پشتیبانی کامل: استاندارد فایدو توسط بسیاری از شرکت‌های مختلف و صنایع گوناگون در سراسر دنیا استفاده می‌شود. این استاندارد برروی تمامی مرورگرهای وب و سیستم عامل‌ها، به صورت پیش‌فرض نصب و پیاده‌سازی شده است.
- هزینه: استفاده از گذرواژه‌ها هزینه‌های پنهانی دارد. این رمزها در بعضی مواقع بازنشانی[8] می‌شوند که این امر نیازمند کمک یک نفر آموزش‌دیده است. علاوه بر این، هزینه‌های بسیاری که رخنه سایبری بوجود می‌آورد غیرقابل محاسبه است [۶].

۳ کاربردهای متعدد استاندارد فایدو در جهان

در حال حاضر کارهای علمی و بررسی‌های زیادی در خصوص استاندارد فایدو و ویژگی‌های امنیتی آن انجام شده است [۹]. استاندارد احراز اصالت فایدو کاربردهای گوناگونی در اکثر جنبه‌های زندگی ما دارد. در ادامه برخی از کاربردهای مهم این استاندارد ذکر می‌شود.

[3]Authenticator [4]Servers [5]Phishing [6]Man In The Middle (MITM) [7]Man In The Browser (MITB) [8]Reset

۱.۳ بانک‌ها و مؤسسات مالی

بانک‌ها و مؤسسات مالی و اعتباری مهمی در سراسر جهان به سمت روش‌های احراز اصالت مبتنی بر فایدو تغییر جهت داده و یا در حال حرکت به این سمت می‌باشند [۱۰-۲۱].

در حال حاضر سه بانک مهم آمریکایی Barclays، Wells Fargo، Bank of America، پنج بانک مهم اروپایی در کشورهای فرانسه، آلمان و بریتانیا Sparkasse، Marchfelder، BNP Paribas، Boursorama، Banque Standard Charted و همچنین بانک‌های متعددی در آسیا از قبیل ژاپن، چین، سنگاپور و مالزی، همچنین سایر مؤسسات مالی از جمله Visa، Maser Card، PayPal، American Express استاندارد فایدو را به طور کامل در سامانه‌های خود لحاظ نموده‌اند. کاربران می‌توانند علاوه بر روش‌های سنتی، تجربه احراز اصالت امن و بی‌نیاز از گذرواژه را نیز داشته باشند.

آنچه مسلم است این تحول در آینده‌ای نزدیک به کشور ما نیز وارد خواهد شد و تمامی ارکان سامانه‌های سنتی را در برخواهد گرفت. بدین ترتیب تمامی سامانه‌هایی که از روش‌های سنتی گذرواژه به تنهایی یا به همراه عامل دوم رمز یکبار مصرف [1] استفاده می‌کنند، جای خود را به احراز اصالت بی‌نیاز از گذرواژه و امن فایدو خواهند داد. کاربران بانک‌ها جهت اتصال اینترنتی به سامانه‌های مورد نظر خود، نیازی به وارد کردن گذرواژه، استفاده از ابزارهای رمزساز و یا انتظار دریافت رمز پیامکی نخواهند داشت؛ به جای آن، تنها با فشردن یک دکمه و ارائه مشخصه زیست سنجی خود در گوشی تلفن همراه، به راحتی و بصورت کاملا امن و مطمئن به حساب کاربری خود در بانک وارد خواهند شد [۲۲].

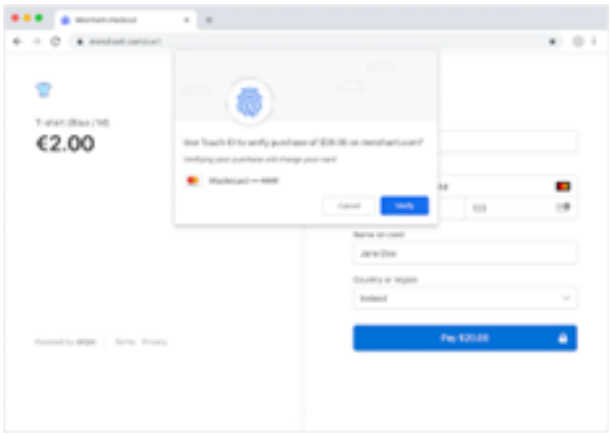
پیش‌بینی می‌شود که در آینده نزدیک نئوبانک‌ها، فراهم‌کنندگان خدمات پرداخت [2] (PSPs) و بانک‌های دولتی و خصوصی کشور نیز به این سمت حرکت خواهند کرد؛ ولی همانطور که در گزارش تحلیلی مؤسسه گارنتر در خصوص نقشه راه تحول و توسعه فایدو بیان شده است [۲۳]، سطح علاقه‌مندی عمومی به استفاده از این استاندارد به طور کامل به شفاف‌سازی نیازمندی و ضرورت این اقدام برای آنها بستگی داشته و همچنین نقاط قوت استاندارد فایدو و نقاط ضعف روش‌های احراز اصالت سنتی برای مسئولان و تصمیم‌گیران در این زمینه بایستی شرح داده شود.

۲.۳ تأییدیه پرداخت امن

تأییدیه پرداخت امن [3] (SPC) نیز یکی دیگر از جنبه‌های جذاب و جدید استاندارد احراز اصالت فایدو است که در تابستان سال ۲۰۲۳ منتشر شد. استاندارد فایدو بر رمزنگاری کلید عمومی استوار است تا بتواند کمبودها و نقاط ضعف امنیت و محرمانگی را برطرف نماید. این استاندارد احتمال خطر حملات سایبری را کاهش داده و اجازه می‌دهد که بانک‌ها بتوانند خدمات برخط بهتر و بیشتری در حوزه بانک‌داری دیجیتال از جمله افزایش محدوده تراکنش‌های مشتریان را ارائه دهند.

تأییدیه پرداخت امن بر اساس قابلیت‌های استاندارد WebAuthn تولید شده است که از طریق آن فراهم‌کنندگان خدمات پرداخت (PSP) می‌توانند یک تجربه پرداخت امن را برای مشتریان فراهم کنند. این استاندارد در حال حاضر توسط مرورگرهای Google Chrome و Microsoft Edge پشتیبانی می‌شود.

مطابق شکل ۲، مراحل کار بطور خلاصه بدین صورت است: ابتدا بانک صادرکننده کارت مشتری، حساب کاربری وی را با اعتبارنامه فایدو مرتبط می‌کند. در حین تراکنش برروی پایگاه وب فروشنده، کاربر کارت فوق‌الذکر را انتخاب می‌کند تا عملیات پرداخت را انجام دهد. در این زمان، شرکت PSP به بانک صادرکننده کارت متصل شده و در خصوص اعتبارنامه متصل به کارت سوال می‌کند؟ بانک صادرکننده کارت نیز بخش قابل اشتراک‌گذاری اعتبارنامه را در اختیار PSP قرار می‌دهد. سپس شرکت واسط به SPC رجوع کرده و مرورگر که صفحه تأیید تراکنش [4] را باز کرده، از کاربر برای تأیید مبلغ پرداخت، نام فروشنده و شماره کارت سوال می‌کند. اگر کاربر مثلاً از طریق MacOS در حال اتصال است، می‌تواند از قابلیت TouchID برای تأیید پرداخت استفاده کند [۲۴].



شکل ۲. خلاصه مراحل تأیید پرداخت امن [۲۵]

۳.۳ کسب و کارهای اینترنتی

علاوه بر بانک‌ها و مؤسسات مالی، کسب و کارهای اینترنتی شناخته شده‌ای از جمله ebay نیز برای امنیت اطلاعات مشتریان و نیز سهولت فرآیند احراز اصالت و فراهم کردن تجربه خرید راحت و خوشایند، فایدو را در سامانه‌های خود به کار گرفته است [۲۶]. کسب و کارهای فروش اینترنتی در کشور ما نیز توسعه بسیاری پیدا کرده است. این نحوه خدمت‌رسانی بعد از فراگیری کرونا با اقبال بیشتری در بین مشتریان روبرو شده است.

تعدد این‌گونه کسب و کارها در کشور بسیار زیاد است و بجز چند شرکت که طیف وسیعی از محصولات را دارند، سایر شرکت‌های خدمت‌رسانی اینترنتی در زمینه‌های تخصصی خودشان مانند فروش پوشاک، لوازم

[1] One Time Password (OTP) [2] Payment Service Providers (PSPs) [3] Secure Payment Confirmation (SPC)

[4] Transaction Confirmation

خانگی، دستگاه‌های الکترونیکی، آرایشی و بهداشتی و غیره فعالیت می‌کنند.

پس از تجربه ناخوشایند تاکسی اینترنتی Uber از حمله سایبری، مسئولان این کسب و کار را بر آن داشت که فایدو را جهت امن کردن خدمات برخط خود لحاظ کنند. در حال حاضر برنامه کاربردی گوشی همراه هوشمند Uber قابلیت کلید عبور [1] را به جای وارد کردن گذرواژه ساده یا رمز یکبارمصرف پیامکی به کاربران خود پیشنهاد می‌دهد و تاکید می‌کند که این روش ساده‌ترین و در عین حال امن‌ترین روش نسبت به سایر روش‌های احراز اصالت سنتی است [۲۷]. در کشور ما نیز تاکسی‌های اینترنتی متعددی فعالیت می‌کنند که می‌توانند از بروز مشکلاتی که برای Uber اتفاق افتاد، پیشگیری نمایند.

۴.۳ صنعت نمایش و سرگرمی

صنعت نمایش و سرگرمی نیز از قافله فن‌آوری عقب نمانده و به‌عنوان مثال Netflix با توجه به حساسیت محتوای نمایشی و تاریخ انتشار فیلم‌ها و سریال‌ها و جلوگیری از نفوذ به سامانه‌هایش مدتی است استاندارد فایدو را برای کارکنان خود به کار گرفته است. پیش‌بینی می‌شود که در آینده نزدیک این کار را برای ورود به سامانه و پرداخت‌های مشترکان خود نیز اجرا نماید [۲۸].

در کشور ما نیز مؤسسات متعدد و بنامی در این زمینه فعالیت می‌کنند که مسلماً با به کارگیری استاندارد فایدو و قابلیت‌های احراز اصالت آن می‌توانند در جهت تنظیم محتوای نمایشی و ارائه خدمات به رده‌های مختلف سنی و نیز امنیت کارسازهای خود بهره گیرند.

۵.۳ اینترنت اشیاء (کنترل دسترسی)

اینترنت اشیاء [2] کاربردهای بسیار گسترده‌ای در کشورهای جهان دارد و بسیاری از خدمات پرداخت و کنترل دسترسی، روز به روز به سمت خودکار شدن پیش می‌روند. یکی از جنبه‌های مهم اینترنت اشیاء، خودروها و خانه‌های متصل شبکه است. کاربردهای این فن‌آوری علاوه بر کنترل دسترسی افراد به خودرو و خانه خود بدون کلید و گذرواژه، امکان پرداخت عوارض، مالیات، اقساط، جریمه‌ها و غیره را نیز شامل شده و پرداخت این موارد می‌تواند به صورت خودکار انجام شود. بدیهی است که به کارگیری اطلاعات حیاتی و کارکردهای حساس در این خصوص نیازمند بستری امن و مطمئن جهت تبادلات اطلاعاتی و مالی است؛ فایدو می‌تواند راهکار بسیار مناسبی در این خصوص باشد [۲۹].

۶.۳ سامانه‌ها

استاندارد فایدو می‌تواند در ورود کاربران شخصی و اداری به سامانه نهادها و مؤسسات حساس از جمله شرکت‌های بیمه، دفاتر اسناد رسمی، ثبت احوال، شهرداری، بورس، مدارس و دانشگاه‌ها، ارگان‌های قضایی، پلیس، مراجع اسناد پزشکی و غیره نیز استفاده شود. در حال حاضر سازمان بهداشت انگلستان (NHS) پس از همه‌گیری کرونا، فایدو را به دلیل سهولت، امنیت و سرعت ورود کاربران به سامانه و آگاهی از به‌روزرسانی‌های لحظه‌ای، گسترش داده و در پایگاه وب خود لحاظ کرده است [۳۰]. از آنجا که در کشور ما نیز سامانه‌های فراوانی جهت احراز اصالت ورود و انجام کارهای اداری و ثبت دعاوی و غیره وجود دارد، استفاده از استاندارد امن و مطمئن فایدو می‌تواند کاربردهای متعددی داشته باشد.

۷.۳ ادارات دولتی و غیردولتی

تقریباً در اکثر ادارت و شرکت‌ها نیاز است که تیم راهبران شبکه و مدیران تاثیرگذار سازمان، بتوانند به صورت امن به شبکه و منابع آن دسترسی داشته باشند. این مسئله برای مدیران ارشد فنآوری اطلاعات و ارتباطات شرکت‌ها اهمیت مضاعف دارد. استفاده دیگر نرم‌افزارهای کاربردی مبتنی بر فایدو، کنترل دسترسی افراد به اماکن از جمله محیط‌های اداری بوده و بوسیله آن می‌توان حتی حضور وغیاب کارکنان و همچنین دسترسی افراد به مکان‌های مختلف سازمان را تحت نظر داشت. آمد و شد پرسنل مؤسسات اداری و کارخانجات و همچنین ورود آنها به سامانه‌ها و برنامه‌های کاربردی بالاخص برای کارمندان شیفت در صنایع مختلف از جمله پزشکی و بهداشتی نیز می‌تواند از مثال‌های دیگر فایدو و نرم‌افزار کاربردی مرتبط با آن باشد.

۸.۳ شبکه‌های اجتماعی و پیام‌رسان‌ها

با توجه به گستردگی فعالیت شبکه‌های اجتماعی و ضرورت حفظ حریم خصوصی کاربران این شبکه‌ها، استفاده از استاندارد فایدو در آنها بسیار ضروری بنظر می‌رسد. در حال حاضر شبکه اجتماعی Line به طور عملی این قابلیت را در سامانه خود اعمال کرده است. این شبکه خدمات خود را بسیار گسترده کرده و قابلیت‌هایی از جمله Line Pay، Block Chain، IOT، Clova را به سامانه خود افزوده است. پیش‌بینی می‌شود در آینده نزدیک سایر شبکه‌های اجتماعی نیز خدمات خود را افزوده و به همین علت نیاز به احراز اصالت امن داشته باشند [۷]. اخیرا پیام‌رسان واتساپ نیز قابلیت کلید عبور و استفاده از اثر انگشت یا تشخیص چهره را به نسخه به‌روزرسانی شده خود در Android افزوده است. با توجه به اینکه از طریق شبکه‌های اجتماعی و پیام‌رسان‌ها اطلاعات حساس و بعضاً تراکنش‌های مالی مبادله می‌شود، لذا امن‌سازی این بسترها توسط فایدو می‌تواند گزینه بسیار خوبی برای پیام‌رسان‌های داخل کشور نیز باشد.

۹.۳ احراز اصالت ابری

احراز اصالت ابری مبتنی بر فایدو [3] نیز بدون شک یکی دیگر از جنبه‌های جذاب استفاده از این استاندارد در آینده نزدیک می‌باشد. بدیهی است که بسیاری از خدمات و برنامه‌های کاربردی در آینده‌ای نه چندان دور

[1] Passkey [2] Internet of Things (IOT)

[3] FIDO Cloud

به روی زیرساخت‌های ابری منتقل شده و امن‌سازی بستر ابری نیز برای استفاده‌کنندگان شخصی و تجاری و چه بسا بانک‌ها و مؤسسات مالی و مشتریان آنها بسیار حیاتی خواهد شد [۳۱].

۱۰.۳ هویت ملی (شناسه دیجیتال)

با توجه به اینکه کارت‌های ملی هوشمند که به عنوان شناسه دیجیتال افراد محسوب می‌شود، حاوی اطلاعات بسیار مهم شهروندان یک کشور بوده و لذا لازم است که تبادل اطلاعات آنها در سامانه‌های مختلف بر اساس استاندارد امن و مطمئن فایدو صورت گیرد و این امر نیازمند تصمیم‌گیری و عزم ملی است.

۴ معرفی استاندارد احراز اصالت فایدو

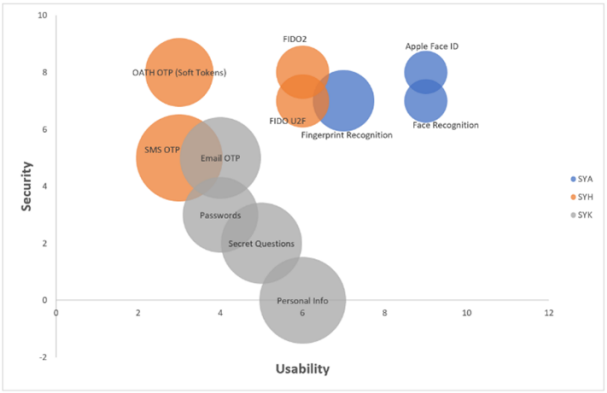
استاندارد احراز اصالت فایدو، یک جفت کلید رمزنگاری عمومی و خصوصی برروی ابزار کاربر که قابلیت فایدو در آن لحاظ شده است، ایجاد می‌کند. کلید خصوصی برروی ابزار کاربر باقی می‌ماند در حالی که کلید عمومی متناظر با کلید خصوصی، به کارساز احراز اصالت فایدو فراهم‌کننده خدمت ارسال می‌شود. هنگامی که یک احرازکننده [۱] ایجاد و ثبت شد، می‌توان از آن برای احراز اصالت امن کاربر بر روی آن دستگاه استفاده کرد. کاربر سپس قادر است که مشخصه زیست‌سنجی [۲] خود را ارائه دهد تا بصورت محلی روی ابزار تأیید شده و در صورت موفق بودن آن، تبادل اطلاعات رمزنگاری بین دستگاه مد نظر و کارساز احراز اصالت آغاز شود.

بطور کلی هر روش احراز اصالت می‌تواند بر اساس سه پارامتر کلیدی ذیل ارزیابی شود [۳۱]:

- سهولت استفاده [۳]: بدین معنی که چقدر کاربر نهایی می‌تواند به صورت طبیعی و بدون دردسر از این روش استفاده کند،
- امنیت [۴]: بیانگر آن است که برای رخنه‌گرها و خرابه کاران و افراد ناباب، نفوذ به ساز و کار احراز اصالت تا چه حد دشوار است،
- امکان به کارگیری [۵]: یعنی تا چه حد به کارگیری این روش برای تمام کاربران روی بسترها و ابزارها راحت است.

تمامی عوامل احراز اصالت بر اساس سه دسته‌بندی زیر تقسیم می‌شوند:

- چیزی که شما می‌دانید (SYK [۶]): به عنوان مثال یک گذرواژه یا حتی یک سوال در این دسته‌بندی قرار می‌گیرد. معمولاً SYK راحت‌ترین روش برای پیاده‌سازی برروی همه دستگاه‌ها و بسترهاست ولی به دلیل امنیت پایین، به راحتی هدف حملات صیادی و سایر موارد نفوذ قرار می‌گیرد.
- چیزی که شما دارید (SYH [۷]): در واقع یک ابزار فیزیکی در این دسته‌بندی قرار می‌گیرد. معمولاً این موارد از نظر حملات صیادی بسیار امن هستند زیرا کلید خصوصی ابزار احرازکننده [۸] را ترک نمی‌کند. البته موارد این دسته‌بندی ممکن است در معرض سرقت فیزیکی بوده و یا مورد استفاده غیرمجاز دیگران قرار گیرد.
- چیزی که شما هستید (SYA [۹]): روش‌های زیست‌سنجی مثل اثر انگشت و تشخیص چهره در این دسته‌بندی قرار می‌گیرند که بستگی به ابزاری دارد که کاربر از آن استفاده می‌کند. این موارد روش‌های بسیار امنی هستند به شرطی که تمام ابزارهای مورد استفاده کاربر این ساز و کار را داشته باشند. اغلب، اینگونه روش‌ها نیاز به یک شیوه پشتیبان نیز دارند؛ به عنوان مثال چنانچه خراشی روی انگشت فرد وجود داشته باشد ممکن است امکان ورود وی به سامانه و احراز اصالت وی میسر نشود.



شکل ۳. مقایسه گرافیکی روش‌های احراز اصالت بر اساس معیارهای SYA، SYH، SYK [۳۲]

در شکل ۳ معیارهایی که اشاره شد، در قالب توپ‌های رنگی نشان داده شده است. بر اساس شکل، استاندارد احراز هویت فایدو (FIDO2) دارای بالاترین امتیاز از نظر امنیت و سهولت کاربری است. استانداردهای FIDO U2F و احراز هویت مبتنی بر زیست سنجی (FIDO UAF) به دلیل آسیب‌پذیری نسبت به حملات صیادی (فیشینگ) امتیاز کمتری از نظر امنیت، نسبت به FIDO2 دارند [۳۳].

مزایای احراز اصالت بر اساس استاندارد فایدو عبارتند از:

- فن‌آوری به‌روز برای احراز اصالت کاربران بی‌نیاز از گذرواژه
- عدم نیاز به تحویل اطلاعات حساس و محرمانه به فراهم‌کنندگان خدمات
- مقاومت بالا در برابر حملات سایبری
- سهولت استفاده برای کاربران بانک‌ها و مؤسسات مالی
- ارائه آسان خدمات دولت الکترونیک و تجارت الکترونیک
- توسعه قابلیت‌های اینترنت اشیاء در برنامه‌های کاربردی گوشی‌های همراه هوشمند

همانطور که پیش‌تر نیز ذکر شد، هدف اصلی استاندارد فایدو سادگی ورود کاربران به سامانه‌ها است در حالی که به هیچ وجه مسائل امنیتی قربانی سهولت نشود. انجمن فایدو برای پشتیبانی از طیف گسترده موارد

[1] Authenticator [2] Biometric [3] Usability [4] Security [5] Deployability
[6] Something You Know (SYK) [7] Something You Have (SYH)
[8] Authenticator [9] Something You Are (SYA)

استفاده و حالات به کارگیری، سه پروتکل متفاوت به شرح زیر ارائه داده است [۳۴]:

- FIDO Universal Authentication Framework (UAF)
- FIDO Universal Second Factor (U2F)
- FIDO2

در ادامه هر کدام از موارد فوق به تفصیل توضیح داده خواهد شد.

۱.۴ پروتکل FIDO UAF

UAF، پروتکل بی‌نیاز از گذرواژه بوده که از ویژگی‌های زیست‌سنجی کاربران برای احراز اصالت استفاده می‌کند. در این روش، نیاز به یک کلید سخت‌افزاری مجزا حذف شده و هر گونه ابزار حاوی حسگر زیست سنج، می‌تواند نقش کلید امنیتی را بازی کند.

این پروتکل اجازه ثبت یک دستگاه فعال مثل گوشی همراه هوشمند یا تبلت در یک کارساز یا پایگاه وب پشتیبانی‌کننده فایدو را به کاربر می‌دهد. در این راهکار کاربر قادر است ابزار خود را با استفاده از احراز اصالت چند عاملی مثلاً از طریق انتخاب یک ساز و کار احراز اصالت محلی مانند اثر انگشت، تشخیص چهره و یا واردکردن پین ثبت کرده و صحت هویت خود را اثبات نماید. با به کارگیری این پروتکل، کاربر می‌تواند پس از ثبت‌نام اولیه، به سادگی عملیات احراز اصالت محلی را در هر زمان و مکان انجام دهد و دیگر نیازی به گذرواژه نبوده بلکه این استاندارد سطح بسیار بالایی از امنیت را فراهم می‌کند زیرا وابسته به رمزنگاری کلید عمومی است [۳۳-۳۶].

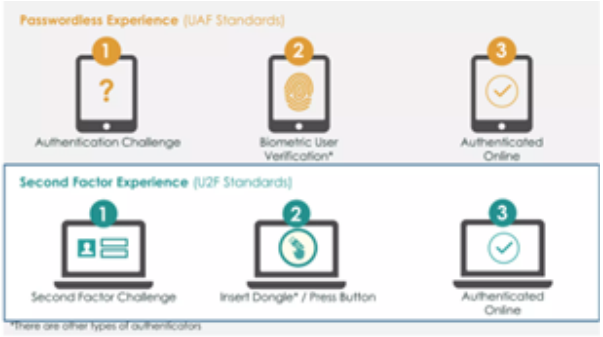
این پروتکل همچنین، امکان ترکیب ساز و کارهای تأیید هویت چندعاملی مانند اثر انگشت به همراه پین را نیز پشتیبانی می‌کند. پروتکل UAF شامل عملیات ثبت‌نام، احراز اصالت، تأیید تراکنش و لغو ثبت‌نام است. بخش بالای شکل ۴، نحوه احراز اصالت پروتکل UAF از طریق اثر انگشت را نشان می‌دهد.

۲.۴ پروتکل FIDO U2F

U2F پروتکل وابسته به کلید فیزیکی است که با استفاده از یک احرازکننده سخت‌افزاری [۱]، احراز اصالت را انجام می‌دهد. کلید مذکور می‌تواند به رایانه یا گوشی همراه متصل شده و چنانچه دستگاه سازگار با NFC [۲] باشد، از طریق ضربه زدن [۳] بر روی آن این کار انجام شود. این پروتکل به منظور احراز اصالت کاربر از یک عامل ثانویه [۴] قوی مانند یک حسگر لمسی که بر روی ابزار USB طراحی شده است، استفاده می‌کند. بخش پایین شکل ۴، نحوه احراز اصالت پروتکل U2F از طریق توکن سخت‌افزاری را نشان می‌دهد. در این شکل از کاربر خواسته شده است تا عامل دوم که کلید سخت‌افزاری است را به رایانه متصل نموده و با تأیید در خواست احراز اصالت (فشردن دکمه)، ادامه فرآیند را ممکن سازد [۳۷].

همانطور که در شکل ۴ ملاحظه می‌شود، تفاوت عمده دو استاندارد آن است که U2F احراز اصالت را ابتدا با دریافت رمز عبور و در ادامه به

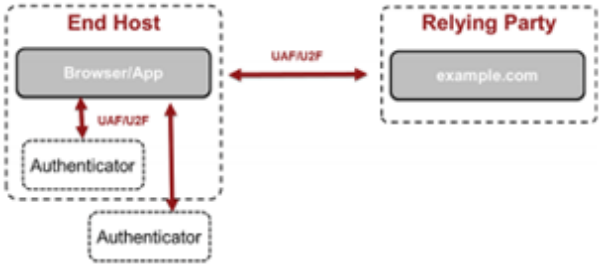
[1]Token [2]Near Field Communication (NFC) [3]Tap [4]Second Factor



شکل ۴. مقایسه استانداردهای U2F، UAF [۳۸]

کمک یک عامل دوم فیزیکی (توکن سخت‌افزار) انجام می‌دهد؛ در حالی که در استاندارد UAF، روند احراز اصالت، بدون رمز عبور و با تکیه بر دریافت زیست‌سنج‌ها صورت می‌گیرد.

از نقطه نظر معماری دو استاندارد فوق مشابه می‌باشند (شکل ۵). در واقع کاربران با یک سخت‌افزار حاوی کلید (احرازکننده) که پروتکل احراز اصالت را با یک کارساز وب که از مرورگر یا یک برنامه کاربردی [۵] فراخوان می‌شود، سروکار دارند. این شیوه، یک مدل احراز اصالت جدید است که پروتکل تبادل کلید از رمزنگاری کلید عمومی برای تأیید احرازکننده به سامانه متکی(RP [۶]) (به فایدو) استفاده می‌کند. در اختیار داشتن کلید خصوصی برای احرازکننده وقتی مفید است که کلید عمومی در کارساز ثبت شده باشد که این کار در طی نخستین ثبت‌نام اتفاق می‌افتد.



شکل ۵. شباهت‌های ساختار احراز اصالت در دو استاندارد UAF، U2F [۳۸]

احرازکننده ممکن است خارج از میزبان [۷] نهایی قرار داشته باشد. برای مثال، احرازکننده ممکن است از طریق رابط کاربری USB متصل بوده (مانند احرازکننده سخت‌افزاری USB) یا توسط فن‌آوری‌های رادیویی مثل بلوتوث هوشمند وصل باشد. در سایر موارد، میزبان نهایی ممکن است که خودش یک محیط اجرایی مورد اعتماد داشته باشد که این امر امروزه درلپ‌تاپ‌ها و گوشی‌های هوشمند بسیار رایج شده است [۳۸].

مهم‌ترین نقطه قوت استاندارد فایدو نسبت به احرازکننده‌های سنتی مبتنی بر رمز یکبار مصرف (OTP)، مقاوم بودن آن نسبت به حملات MITM/MITB است. به عنوان مثال احرازکننده‌های رمز یکبارمصرف

[5]Application [6]Relying Party (RP) [7]Host

مبتنی بر زمان Google (TOTP [1]) همچنان می‌تواند مورد حمله صیادی بی‌درنگ [2] قرار گیرند.

دلیل اینکه حملات MITM/MITB هرگز در استاندارد فایدو اتفاق نمی‌افتد آنست که پروتکل‌های U2F/UAF مبتنی بر تعامل واقعی بر اساس رمزنگاری کلید عمومی برروی ابزار است. این خاصیت باعث جلوگیری از حملات فوق‌الذکر می‌گردد.

۳.۴ پروتکل FIDO2

پروتکل فایدو۲ جدیدترین ویرایش استاندارد فایدو بوده و طیف وسیعی از مزایای احراز اصالت مبتنی بر معیارهای زیست‌سنجی را شامل می‌شود. پروتکل جدید فایدو۲ نسبت به ویرایش‌های قبلی استاندارد فایدو (U2F/UAF) در مقابل حملات مهندسی اجتماعی از جمله حملات صیادی (فیشینگ) مقاوم‌تر است [۳۳].

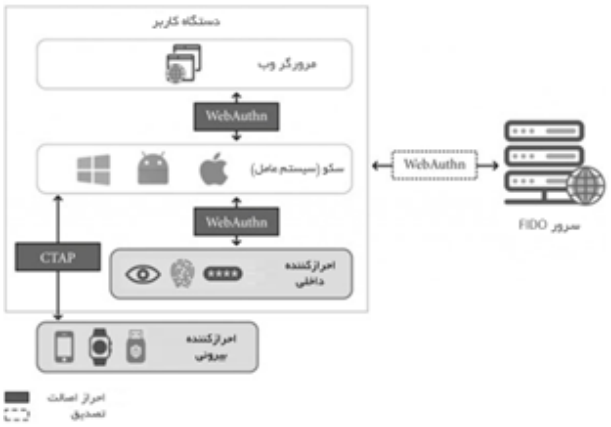
کاربران هنگام ورود به یک خدمت مبتنی بر فایدو۲ می‌توانند به راحتی از اثر انگشت یا چهره یا حتی صدا برای اثبات تملک کلید خصوصی استفاده کنند و در نتیجه حق دستیابی به داده و انجام تراکنش و غیره را به دست بیاورند. ویژگی فایدو۲ آنست که ابزار کاربر (مثلاً گوشی همراه هوشمند) می‌تواند به عنوان احرازکننده به کار رود.

هدف اصلی استاندارد فایدو۲ ارائه رابط برنامه نویسی کاربردی (API [3]) جهت احراز اصالت وب (WebAuthn [4]) است. استاندارد WebAuthn در سال ۲۰۱۸ توسط انجمن فایدو ارائه شد و امروزه توسط بسیاری از مرورگرهای مطرح مانند Google ،Micorosoft Edge ،Chrome Mozilla Firefox، Apple Safari و سیستم عامل‌های گوناگون پشتیبانی می‌شود. در شکل ۶، میزان سازگاری سیستم عامل‌ها و مرورگرها با استاندارد فایدو نشان داده شده است.

شکل ۶. سازگاری مرورگرها و سیستم عامل‌ها با استانداردهای فایدو [۳۸]

امروزه از طریق WebAuthn یک کاربر با لپ‌تاپی که در دست دارد و مرورگری که استاندارد WebAuthn را پشتیبانی می‌کند، می‌تواند از احرازکننده فایدو برای عملیات ثبت، ذخیره‌سازی و استفاده خدمات مختلف بر روی آن دستگاه استفاده کند و این کار را به همان سهولتی که اثر انگشت یا چهره خودش را روی دستگاه ارائه می‌کند، انجام دهد. در شکل ۷ ساختار احراز اصالت فایدو۲ از طریق WebAuthn به تصویر کشیده شده است.

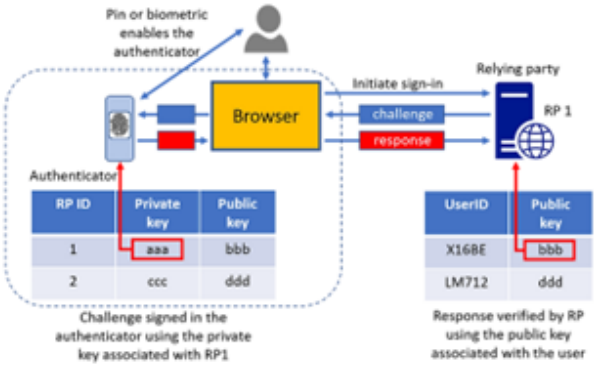
[1]Time-based One-Time Password [2]Real time [3]Application Programming Interface [4]Web Authentication (WebAuth)



شکل ۷. ساختار احراز اصالت فایدو۲ از طریق WebAuthn [۳۹]

اگر کاربر بخواهد به سامانه‌ای که در آن استاندارد فایدو۲ پشتیبانی شده، وارد شود، API مربوط به احراز اصالت وب (WebAuthn) که توسط فراهم‌کننده خدمت روی پایگاه وب مورد نظر نصب شده، قادر است تعامل بین سامانه مربوطه و احرازکننده اصالت کاربر (در این مورد مثلاً گوشی تلفن همراه یا کلید سخت‌افزاری) را آغاز کند.

احرازکننده ممکن است توسط اثر انگشت یا تشخیص چهره قفل شده باشد تا صحه بیشتری در تأیید هویت کاربر بگذارد و اجازه دسترسی غیرمجاز به خدمت را ندهد.



شکل ۸. ساختار کلید عمومی و خصوصی در استاندارد فایدو۲ [۴۰]

پروتکل استاندارد فایدو۲ شامل دو بخش اصلی است:

- WebAuthn
- CTAP [5]

همانطور که پیش‌تر بیان شد، WebAuthn یک استاندارد تحت وب بوده که به پایگاه‌های وب امکان می‌دهد برای احراز اصالت کاربران از روش‌هایی مانند اثر انگشت، تشخیص چهره یا استفاده از کارت‌های هوشمند بهره ببرند. WebAuthn با استفاده از رمزنگاری کلید عمومی، امنیت بالایی را در فرآیند احراز اصالت ارائه می‌دهد. با استفاده از

[5]Client To Authenticator Protocol (CTAP)

WebAuthn، کاربران می‌توانند بدون نیاز به گذرواژه، با معیارهای زیست‌سنجی خود به خدمات برخط دسترسی پیدا کنند. این استاندارد توسط W3C (کنسرسیوم وب جهانی) توسعه داده شده است و در بسیاری از مرورگرها و سیستم عامل‌ها پشتیبانی می‌شود.

CTAP پروتکلی است که ارتباط بین احرازکننده و سامانه کاربر را برقرار می‌کند. احرازکننده می‌تواند یک دستگاه سخت‌افزاری مانند کلید USB یا یک نرم‌افزار گوشی تلفن همراه باشد. CTAP از طریق تبادل درخواست‌ها و پاسخ‌ها، احراز اصالت دو عاملی را پیاده‌سازی کرده و از روش‌های امنیتی مانند رمزنگاری عمومی استفاده می‌کند.

جدول ۱. مقایسه استانداردهای FIDO2، UAF و U2F

	FIDO2	U2F	UAF
تمرکز استاندارد	احراز اصالت کاملا بی‌نیاز از گذرواژه	ذخیره سازی عامل دوم برای احراز اصالت دو عاملی	احراز اصالت بی‌نیاز از گذرواژه
شیوه احراز اصالت	شیوه‌های زیست سنجی کلیدهای امنیتی	استفاده از کلیدهای امنیتی	شیوه‌های زیست سنجی، احراز اصالت محلی
پلتفرم مورد پشتیبانی	پشتیبانی گسترده از انواع پلتفرم‌ها، مرورگرها و دستگاه‌ها	پلتفرم‌هایی که احراز اصالت دو عاملی را پشتیبانی می‌کنند	سطح پشتیبانی کمتر نسبت به فایدو۲
معیار زیست سنجی	ذخیره‌سازی و پردازش محلی روی تجهیز کاربر	—	ذخیره‌سازی و پردازش محلی روی دستگاه کاربر
موارد استفاده	احراز اصالت جامع برای انواع سناریوها	احراز اصالت دو عاملی در تمامی موارد پشتیبانی کننده از این روش	بسیار کم (احراز اصالت بی‌نیاز از گذرواژه ناشناس در دنیای واقعی)
سطح امنیت	مقاوم در برابر حملات صیادی	آسیب‌پذیر در برابر حملات صیادی	آسیب‌پذیر در برابر حملات صیادی

مطابق شکل ۸، مراحل و روند کار استاندارد WebAuthn به شرح زیر است:

- درخواست احراز اصالت: پایگاه وب یا خدمت برخط ابتدا درخواست احراز اصالت را به کاربر می‌دهد. این درخواست شامل ارسال یک چالش [1] به کاربر است که به صورت تصادفی ایجاد می‌شود.
- انتخاب احرازکننده: کاربر باید ابزار احرازکننده را انتخاب کند. این ابزار می‌تواند یک کلید امنیتی فیزیکی (مانند کلید USB)، دستگاه تشخیص اثر انگشت، تشخیص چهره و یا نرم‌افزار گوشی تلفن همراه باشد.
- احراز اصالت ابزار: سپس ابزار احراز اصالت با استفاده از یک کلید عمومی (که در مرحله ثبت‌نام ایجاد شده است) خود را به پایگاه وب معرفی می‌کند. این احراز اصالت از طریق یک فرآیند رمزنگاری امن انجام می‌شود.
- پاسخ به چالش: ابزار احراز اصالت پاسخی را به چالش ارسال شده توسط پایگاه وب ایجاد و آن را امضاء می‌کند. این امضاء با استفاده از کلید خصوصی مربوط به ابزار احرازکننده انجام می‌شود.
- تأیید احراز اصالت: پایگاه وب، دریافت پاسخ و امضای ابزار احراز اصالت را تأیید می‌کند. در صورتی که تأیید با موفقیت انجام شود، کاربر به پایگاه وب وارد می‌شود.

[1] Challenge

۵ محصول «نشانه» مبتنی بر فایدو۲

«نشانه» یک راهکار تخصصی برای احراز اصالت هوشمند است که در شرکت ره‌آورد سامانه‌های امن (رهسا) توسعه داده شده است. این راهکار بر مبنای استاندارد متن باز فایدو۲ و براساس مبانی رمزنگاری نامتقارن و به صورت کاملا بومی، ارائه شده و دارای تأییدیه فایدو و افتا می‌باشد. هدف محصول نشانه ارائه راهکاری کارآمد، به صرفه و آسان جهت کنار گذاشتن گذرواژه‌ها و مهاجرت به دنیای امن بی‌نیاز از گذرواژه برای افراد و سازمان‌ها است.

نشانه ابزارهای مختلفی در اختیار کابران قرار می‌دهد تا با کمترین هزینه و در کمترین زمان، ایمنی و سادگی احراز اصالت بدون گذرواژه را تجربه کنند.

شکل ۹. سه محصول نشانه شرکت رهسا [۴۱]

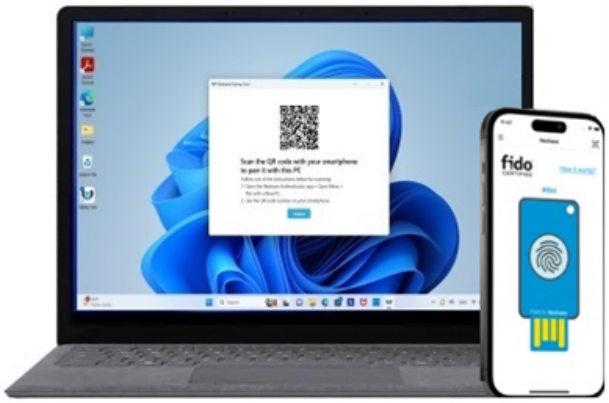
کاربران می‌توانند بدون پرداخت هزینه اضافی برای تهیه کلید سخت‌افزاری فایدو۲، از گوشی تلفن همراه یا کارت هوشمند خود به عنوان کلید امنیتی فایدو۲ استفاده کنند. این ابزارها که در شکل ۹ نشان داده شده است، عبارتند از:

نشانه کارت: کارت‌ها و نشان‌های شناسایی (RFID-NFC) در بسیاری از سازمان‌ها برای شناسایی اشخاص مورد استفاده قرار می‌گیرند. این کارت‌ها غالباً برای شناسایی کارمندان به منظور انجام اموری همچون حضور و غیاب (ورود و خروج) و همچنین محدودسازی دسترسی فیزیکی به برخی مناطق سازمان برای افراد مشخص استفاده می‌شوند. با ابزار نشانه کارت، سازمان‌ها می‌توانند از کارت‌ها و نشان‌های شناسایی، برای دسترسی به سامانه‌ها و نرم‌افزارها نیز استفاده نموده و عملیات احراز اصالت دیجیتال را ساده‌تر و سریع‌تر نمایند. در واقع این خدمت امکان

استفاده از کارت‌ها و نشان‌های شناسایی به عنوان کلید فایدو۲ را فراهم می‌کند.

نشانه توکن: یک کلید امنیتی USB محافظت شده با پین است که با تمام مرورگرهای وب که WebAuthn در آنها پشتیبانی می‌شود، سازگار است. نشانه توکن در خدمت‌های برخط مانند Azure AD، Dropbox، Facebook، Twitter، GitHub و موارد دیگر به‌طور یکپارچه کار می‌کند.

نشانه موبایل: با استفاده از برنامه کاربردی نشانه موبایل، گوشی هوشمند کاربر به یک کلید امنیتی فایدو۲ تبدیل می‌شود که می‌تواند از آن برای تعریف کلید عبور در خدمات مختلف استفاده نماید. کاربران برای استفاده از گوشی تلفن همراه هوشمند به عنوان کلید امنیتی بر روی رایانه شخصی، می‌توانند از ابزار اتصال نشانه [1] یا حتی بدون استفاده از هیچ ابزار یا سخت‌افزاری فقط با پویش [2] یک کد QR این ارتباط را برقرار کنند (شکل ۱۰).



شکل ۱۰. تصویر برنامه کاربردی نشانه موبایل و پویش QR [۴۱]

هر یک از این روش‌ها مزایا منحصر بفردی دارد که متناسب با نیاز و فضای مورد استفاده قابل انتخاب است. بطور کلی مزایای محصول نشانه عبارتند از:

- پشتیبانی از کلید عبور: کاربر می‌تواند بدون نیاز به ثبت مجدد هر دستگاه در هر حساب، به اعتبارنامه‌های ورود به سامانه فایدو در دستگاه‌های مختلف خود از جمله دستگاه‌های جدید دسترسی داشته باشد.
- بررسی نزدیکی با بلوتوث: نزدیکی رایانه شخصی و گوشی همراه کاربر تشخیص داده می‌شود تا امکان استفاده از کلیدهای عبور از راه دور و بدون مجاورت فیزیکی بین رایانه مورد استفاده و گوشی تلفن هوشمند وجود نداشته باشد.
- امکان ورود برون خط [3]: در هر زمان و از هر کجا، کاربر می‌تواند به داده‌های خود دسترسی داشته باشد، حتی زمانی که در هواپیما بوده یا اتصال اینترنت ندارد.
- پشتیبانی از چندین کلید امنیتی: کاربر می‌تواند چندین کلید امنیتی مجزا داشته باشد تا کلیدهای عبور خود را بر اساس مصرف شخصی یا سازمانی تفکیک نماید.

در شکل ۱۱ نحوه کاربری و استفاده از برنامه کاربردی نشانه، به تصویر کشیده شده است.

۱.۵ ساختار ثبت نام و احراز اصالت محصول نشانه

نظر به اینکه محصول نشانه بر اساس آخرین ویرایش استاندارد فایدو۲ طراحی شده است، لذا تعاملات لازم با استاندارد WebAuthn در آن درنظر گرفته شده است.

WebAuthn دارای سه نهاد اصلی احرازکننده، کاربر و سامانه متکی (به فایدو) بوده و آنها در دو فرآیند ثبت و احراز اصالت در تعامل با یکدیگر کار می‌کنند.

همانطور که در شکل ۱۲ نشان داده شده است، یکی از انواع احرازکننده‌ها می‌تواند گوشی تلفن همراه کاربر باشد که در آن نرم‌افزار کاربردی نشانه موبایل نصب شده است. تمام ارتباطات بین موجودیت‌های فوق معمولاً توسط یک مرورگر وب انجام می‌شود.

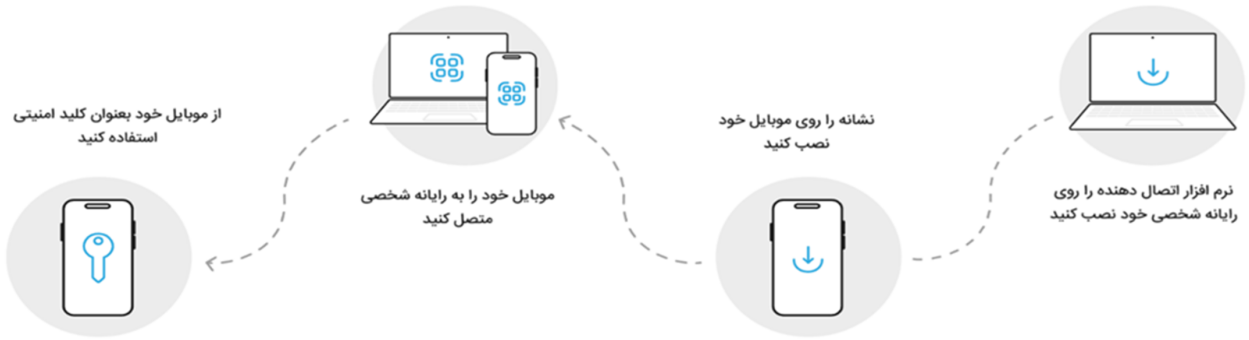
در شکل ۱۳ روند ثبت نام کاربر در استاندارد فایدو به تصویر کشیده شده است. فرآیند ثبت‌نام باعث می‌شود که احرازکننده مجموعه جدیدی از اعتبارنامه‌های کلید عمومی ایجاد کند که می‌تواند برای امضا چالش ایجاد شده توسط سامانه متکی (به فایدو) استفاده شود. بخش عمومی این اعتبارنامه‌های جدید، به همراه چالش امضاء شده، برای ذخیره به سامانه متکی بازگردانده می‌شود. سامانه متکی می‌تواند هر زمان که لازم باشد از این اعتبارنامه‌ها برای تأیید هویت کاربر استفاده کند.

پس از تکمیل روند ثبت نام، فرآیند احراز اصالت به سامانه متکی اجازه می‌دهد تا یک چالش را برای احرازکننده ارسال کند. سپس این چالش می‌تواند با کلید خصوصی متناظر که در احرازکننده ذخیره شده، امضاء شده و به سامانه مذکور ارسال گردد. به این ترتیب، سامانه متکی می‌تواند اعتبار کاربر را تأیید و هویت وی را ثابت کند. در شکل ۱۴ روند احراز اصالت استاندارد فایدو نشان داده شده است.

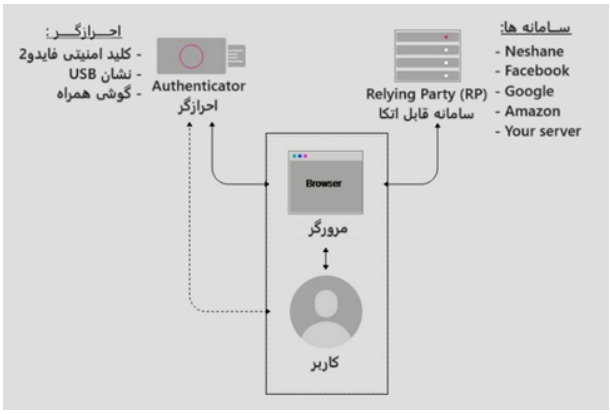
هر دو فرآیند فوق با کمک رمزنگاری کلید عمومی و امضای دیجیتال کار می‌کنند [۴۲]. همانطور که اشاره شدکلید خصوصی مخفی است و فقط کاربر (یا احرازکننده) به آن دسترسی دارد. در مقابل، کلید عمومی می‌تواند توسط هر کسی دیده یا ذخیره شود. کلید عمومی می‌تواند برای تأیید امضاهای تولید شده توسط کلید خصوصی استفاده شود. هیچ کلید دیگری، به جز کلید خصوصی، نمی‌تواند امضایی ایجاد کند که کلید عمومی بتواند معتبر بودن آن را تأیید کند. به این ترتیب، سامانه متکی (به فایدو) می‌تواند یک کلید عمومی را ذخیره کرده و از آن برای تأیید امضاهای انجام شده توسط کاربر که کلید خصوصی را در دست دارد استفاده کند.

در حال حاضر شرکت‌های معتبری در جهان از جمله IDmelon،

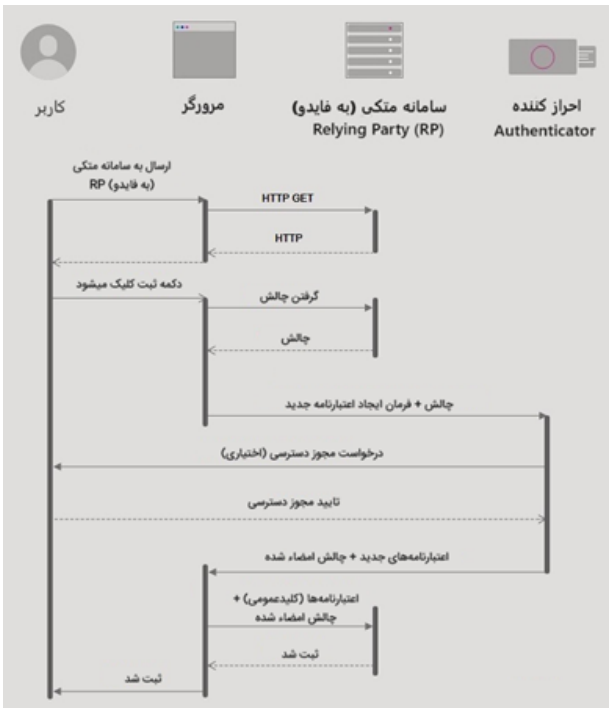
[1] Pairing Tool [2] Scan [3] Offline



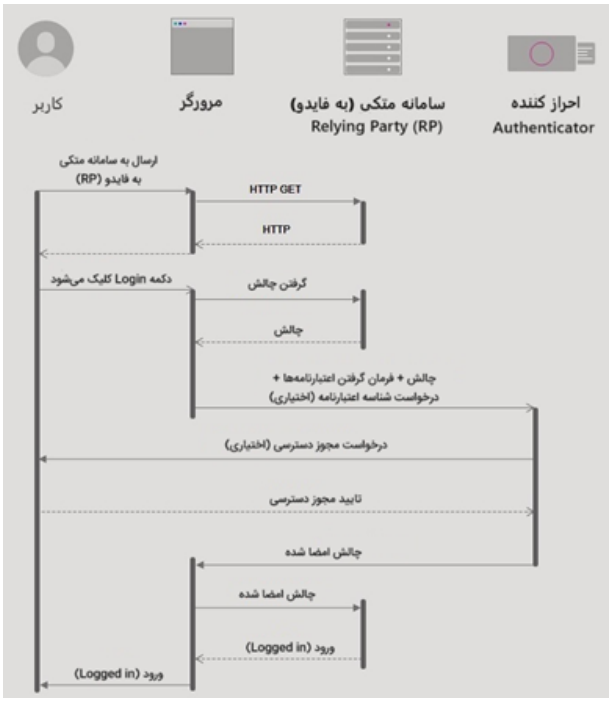
شکل ۱۱. نحوه کاربری برنامه کاربردی نشانه موبایل



شکل ۱۲. تعامل موجودیت‌های دخیل در فرآیندهای ثبت‌نام و احراز اصالت



شکل ۱۳. فرآیند ثبت نام در استاندارد فایدو [۴۱]



شکل ۱۴. فرآیند احراز اصالت در استاندارد فایدو [۴۱]

HYPR، Authtake و Akamai محصولات گوناگون احرازکننده فایدو۲، از جمله نرم‌افزار احرازکننده گوشی همراه را به مشتریان شخصی و اداری ارائه می‌دهند [۴۳–۴۶].

شرکت ره‌آورد سامانه‌های امن (رهسا) نخستین شرکت ایرانی است که این فن‌آوری را با موفقیت اجرا کرده است. لازم به ذکر است که در این طرح، استاندارد فایدو توسط کارشناسان این شرکت پیاده‌سازی و استفاده شده است. در کنار محصول نشانه موبایل، محصولات متنوع دیگری از جمله نشانه کارت و نشانه توکن برای پوشش طیف وسیع مشتریان این شرکت پیاده‌سازی و ارائه شده است [۴۱].

۶ نتیجه‌گیری

در این مقاله پس از معرفی مفاهیم استاندارد احراز اصالت فایدو، مزایا و قابلیت‌های آن جهت استفاده در بخش‌های گوناگون از جمله بانکداری، کسب و کارهای برخط، شرکت‌ها، سامانه‌ها، پیام‌رسان‌ها، نمایش خانگی، هویت ملی توضیح داده شد.

انجمن فایدو از هشت سال پیش روی استاندارد فایدو با هدف ایجاد استانداردهای احراز اصالت بی‌نیاز از گذرواژه فعالیت کرده است و در حال حاضر بسیاری از بزرگان فن‌آوری نرم‌افزاری، سخت‌افزاری و بانک‌ها و مؤسسات مالی و تولیدکنندگان ابزارهای کامپیوتری و تراشه‌های الکترونیکی با این انجمن همکاری دارند. بدین ترتیب گذرواژه که عامل دانستنی محسوب می‌شود (نقطه ضعف این سامانه‌ها) از صحنه کنار گذاشته خواهد.

در گزارش تحقیقی گارتنر پیش‌بینی شده که تا سال ۲۰۲۵، بیش از ۲۵ درصد تراکنش‌های احراز اصالت چند عاملی (MFA [1]) که از احرازکننده سخت‌افزاری استفاده می‌کنند بر اساس پروتکل فایدو بنا خواهند شد، چیزی که امروزه کمتر از ۵ درصد است [۲۳]. در نتیجه می‌توان به جرات گفت که استاندارد فایدو دورنمای آینده سامانه‌های احراز اصالت بوده و علاوه بر سادگی استفاده، دارای رمزنگاری بسیار قوی و غیرقابل نفوذ نیز می‌باشد.

قابلیت کلید عبور این استاندارد به زودی فایدو را به صدر توجه خواهد آورد. بدین ترتیب هر دستگاه گوشی تلفن همراه در جیب اشخاص می‌تواند یک کلید فایدو بوده و این قابلیت به گونه‌ای در سیستم عامل دستگاه تنیده شده که روند استفاده از آن برای کاربر محسوس نیست. بنابراین در آینده بسیار نزدیک دیگر شاهد این نیستیم که از گذرواژه حتی به عنوان عامل اضافه MFA نیز بهره گرفته شود و بدون شک حرکت به سمت دنیای عاری از گذرواژه صورت خواهد گرفت.

استانداردهای UAF، U2F نیز به مرور رنگ باخته و جای خود را به نسخه جدید استاندارد یعنی فایدو۲ خواهند داد و همه جنبه‌های احراز اصالت به قابلیت زیست‌سنجی رایانه‌ها و گوشی‌های همراه هوشمند برخواهند گشت.

این استاندارد به کاربر این امکان را می‌دهد که چندین دستگاه سازگار با فایدو مانند گوشی هوشمند، تبلت، لپ‌تاپ و رایانه را با یک بستر رمزساز احراز اصالت کنند. قابل ذکر است که در حال حاضر استاندارد WebAuthn در سمت انواع سیستم عامل‌ها (Windows، Android، iOS و ...) به طور کامل پیاده‌سازی و عملیاتی شده است و تنها لازم است استفاده از کلیدهای امنیتی فایدو۲ رواج پیدا کند. لذا آینده برنامه‌های کاربردی فایدو۲ روشن‌تر از سخت‌افزارهای مشابه به نظر می‌رسد.

بر همین اساس شرکت ره‌آورد سامانه‌های امن (رهسا) با رصد فن‌آوری‌های روز دنیا در زمینه احراز اصالت، اقدام به ارائه محصول بومی پیشرفته نرم‌افزار کاربردی نشانه موبایل نموده است که قادر است کلید امنیتی فایدو۲ را روی گوشی‌های تلفن همراه هوشمند پیاده‌سازی و عملیاتی کند.

[1] Multi Factor Authentication

مراجع

[1] Rahavard samanehaye amn co.

[2] FIDO Alliance. How fido addresses a full range of use cases. *FIDO Alliance: Mountain View, CA, USA*, 2022.

[3] Anna Angelogianni, Ilias Politis, and Christos Xenakis. How many fido protocols are needed? surveying the design, security and market perspectives. *arXiv preprint arXiv:2107.00577*, 2021.

[4] David W Chadwick, Romain Laborde, Arnaud Oglaza, Remi Venant, Samer Wazan, and Manreet Nijjar. Improved identity management with verifiable credentials and fido. *IEEE Communications Standards Magazine*, 3(4):14–20, 2019.

[5] Simone Bussa, Riccardo Sisto, and Fulvio Valenza. Formal verification of the fdo protocol. In *2023 IEEE Conference on Standards for Communications and Networking (CSCN)*, pages 290–295. IEEE, 2023.

[6] *THALES digital identity and security. The Evolution of Digital Banking Authentication*. January 2023.

[7] *FIDO Alliance*.

[8] Haonan Feng, Jingjing Guan, Hui Li, Xuesong Pan, and Ziming Zhao. Fido gets verified: A formal analysis of the universal authentication framework protocol. *IEEE Transactions on Dependable and Secure Computing*, 20(5):4291–4310, 2022.

[9] Romain Laborde, Arnaud Oglaza, Samer Wazan, François Barrere, Abdelmalek Benzekri, David W Chadwick, and Rémi Venant. A user-centric identity management framework based on the w3c verifiable credentials and the fido universal authentication framework. In *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, pages 1–8. IEEE, 2020.

[10] Bank of america. online banking security.

[11] Chase bank.

[12] Liberty bank america. digital banking agreement personal and business, 2023.

[13] Banner bank.

[14] Wells fargo bank.

[15] Boston consulting group. the rise of digital banking in southeast asia, December 2020.

[16] Ian pollari. the future of digital banking, kpmg australia, 2023.

[17] Marchfelder bank.

[18] Sparkasse bank germany.

[19] Boursorama banque. using token2 fido2 keys with boursorama banque client area.

[20] Bank of america. how to add a token2 fido2 key to your bank of america online account.

[21] Standard chartered bank.

[22] Thales group. breaking free from passwords: Passkeys and the future of digital banking, 2022.

[23] Corbett Liz. Take 3 steps toward passwordless authentication. *Gartner Research and Conslting company*, 2022.

[24] Ian jacobs. secure payment confirmation. stripe experiment and next steps, March 2021.

[25] Authenton germany. why should i authorize my online payments with fido token.

[26] Fido alliance. ebay's journey to passwordless with fido, March 2021.

[27] Uber blog. use passkeys wherever you sign in to uber, October 2023.

[28] Fido alliance. netflix's journey with webauthn.

[29] Hypr co. how does fido support iot. security-security encyclopedia.

[30] Fido alliance. national health service (nhs) uses fido authentication for enhanced login.

[31] Keyless. why banks should urgently move away from otps, October 2023.

[32] Sumedh inamdar. comparison of user authentication methods on three parameters, Mar 2019.

[33] Enis Ulqinaku, Hala Assal, AbdelRahman Abdou, Sonia Chiasson, and Srdjan Capkun. Is real-time phishing eliminated with {FIDO}? social engineering downgrade attacks against {FIDO} protocols. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 3811–3828, 2021.

[34] Anna Angelogianni, Ilias Politis, and Christos Xenakis. How many fido protocols are needed? analysing the technology, security and compliance. *ACM Computing Surveys*, 56(8):1–51, 2024.

[35] Haonan Feng, Hui Li, Xuesong Pan, Ziming Zhao, and T Cactilab. A formal analysis of the fido uaf protocol. In *NDSS*, 2021.

[36] Haonan Feng, Jingjing Guan, Hui Li, Xuesong Pan, and Ziming Zhao. Fido gets verified: A formal analysis of the universal authentication framework protocol. *IEEE Transactions on Dependable and Secure Computing*, 20(5):4291–4310, 2022.

[37] Dirk Balfanz. Fido u2f implementation considerations. *FIDO Alliance Proposed Standard*, pages 1–5, 2015.

[38] Hannes Tschofenig. Web cryptography: Supporting the fido protocol family, 2014.

[39] Ejin Kim and Hyoung-Kee Choi. Security analysis and bypass user authentication bound to device of windows hello in the wild. *Security and Communication Networks*, 2021(1):6245306, 2021.

[40] John crsaddock. now you can trust fido too, December 2019.

[41] Neshane co.

[42] Anna Angelogianni, Ilias Politis, and Christos Xenakis. How many fido protocols are needed? surveying the design, security and market perspectives. *arXiv preprint arXiv:2107.00577*, 2021.

[43] David W Chadwick, Romain Laborde, Arnaud Oglaza, Remi Venant, Samer Wazan, and Manreet Nijjar. Improved identity management with verifiable credentials and fido. *IEEE Communications Standards Magazine*, 3(4):14–20, 2019.

[44] Haonan Feng, Jingjing Guan, Hui Li, Xuesong Pan, and Ziming Zhao. Fido gets verified: A formal analysis of the universal authentication framework protocol. *IEEE Transactions on Dependable and Secure Computing*, 20(5):4291–4310, 2022.

[45] Jones Michael, Lundberg Emil, Jones J.C., and Kumar Akshay. Web authentication: An api for accessing public key credentials -level 2. *W3C Recommendation*, 2021.

[46] Simone Bussa, Riccardo Sisto, and Fulvio Valenza. Formal verification of the fdo protocol. In *2023 IEEE Conference on Standards for Communications and Networking (CSCN)*, pages 290–295. IEEE, 2023.

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2024, Volume 22, Number 1 (pp. 61–73)
https://monadi.isc.org.ir

FIDO Authentication Standard: Key Applications for Securing Information Exchange

Morteza Asadi *, Mohammad Reza Zamani and Kasra Tawakoli

Rahavard Samanehaye Amn (RAHSA)

ARTICLE INFO.

Article history:
Received: April 3, 2024
Accepted: August 31, 2024
Published Online: August 31, 2024

Keywords:
Multi Factor Authentication
FIDO
Asymetric Cryptography
Biometric
Passwordless

Type: Technical paper

ABSTRACT

Passwords have been utilized as the primary means of authentication since the inception of the World Wide Web and the introduction of online services. The security risks associated with the use of passwords and their vulnerabilities to various types of cyberattacks have rendered this method no longer secure. In recent years, online service providers have sought to protect their users and data from cyber threats by implementing various multi-factor authentication methods. Although these methods have been successful in reducing the incidence of security breaches, they have generally resulted in increased complexity for users. The FIDO standard employs asymmetric encryption, mandates the storage of the private key on the user's device, and combines it with biometric factors, thereby enabling the most secure authentication method for systems while simplifying the process for users. This standard monitors the entire authentication process and prevents potential risks by establishing regulations within operating systems, browsers, and authentication tools. Rahavard Samanehaye Amn Company has implemented this standard locally, offering FIDO authentication under the product name "Neshane" for smart phones. This article discusses the applications, specifications, and capabilities of this standard and the developed product.

* Corresponding author
Email addresses: asadi@ rsa.ir (Morteza Asadi), reza@rsa.ir (Mohammad Reza Zamani), kasra@rsa.ir (Kasra Tawakoli)