آرایه سازان ماندگار

# کیپر

## راه حل احراز هویت چند عاملی

## مقدمه

روش مرسوم و نه‌چندان امن ورود به حساب کاربری بدین گونه است که ابتدا نام کاربری که هویت شخص را مشخص می‌کند و سپس کلمه عبور آشنایی که معمولاً برای بسیاری از حساب‌های برخط مورد استفاده قرار می‌گیرد، را درج می‌کنید. حسابی که ممکن است داده‌های حساس و حیاتی در خود داشته باشد و نشت این داده‌ها می‌تواند مشکلات جبران ناپذیری به همراه داشته باشد. اگر شما بر اساس تحقیقات TeleSign جزو ۵۴٪ از کاربرانی باشید که از پنج کلمه عبور متفاوت یا کمتر برای حساب‌های خود استفاده می‌کنند، به راحتی تحت تأثیر پدیده دومینو قرار خواهید گرفت! پدیده‌ای که براساس آن با لو رفتن یکی از کلمه‌های عبور شما باقی حساب‌های شما می‌تواند توسط نفوذگران مورد حمله قرار گیرد.

احراز هویت چند عاملی مفهوم جدیدی نیست و شما با آن قبلاً مواجه شده‌اید:

- ✓ در هنگام برداشت وجه از خودپردازها و خرید از پایانه‌های فروشگاهی علاوه بر استفاده از کارت بانکی، موظف به ورود پین (شماره هویتی شخصی) می‌باشید.
- ✓ برای خرید اینترنتی نیز علاوه بر ورود داده‌های کارت خود (شماره کارت، CVV2 و تاریخ انقضا) باید رمز پویای مربوط به حساب نیز که از طریق پیامک و یا رمزساز دریافت/ایجاد می‌شود را وارد نمایید.

احراز هویت چند عاملی فرآیندی است که به منظور افزایش میزان امنیت به شما امکان ارائه دو یا چند مؤلفه اعتباری برای ورود به حساب و تأیید هویت خود را می‌دهد. مؤلفه‌های اعتباری معمولاً در سه دسته قابل معرفی است: چیزی که شما فقط از آن اطلاع دارید (کلمه عبور، پین)، یا چیزی که شما در اختیار دارید (توکن امنیتی) و یا چیزی که شما هستید (اثر انگشت). برای افزایش امنیت، مؤلفه‌ها باید از دو دسته مختلف انتخاب شوند. بنابراین ارسال دو کلمه عبور مختلف به عنوان احراز هویت چند عاملی معنی‌دار نخواهد بود.

یکی از مهمترین جنبه‌های پیاده‌سازی احراز هویت چند عاملی، سهولت استفاده از آن است. به عنوان مثال برای ورود به حساب کاربری خود، علاوه بر ورود نام کاربری و کلمه عبور، به عنوان عامل دوم رمز یک‌بار مصرف ایجاد شده توسط برنامه رمزساز موجود در تلفن همراه خود و یا دریافت شده توسط پیامک را وارد می‌کنید. نقش حیاتی احراز هویت چند عاملی، اضافه نمودن لایه امنیتی جدیدی است که ورود به حساب شما را برای سرقت اطلاعات سخت‌تر می‌کند چرا که علاوه بر داشتن کلمه عبور، تلفن همراه شما نیز باید در اختیار نفوذگر باشد. این نکته که دسترسی به برنامه رمزساز تلفن همراه نیازمند عبور از لایه‌های امنیتی تلفن همراه (مانند اثر انگشت، الگوی ترسیمی و پین) می‌باشد، اجرای سناریوی دسترسی به حساب‌های کاربری شما را در عمل بسیار نزدیک به غیرممکن می‌کند. بدیهی است که جلوگیری از تمام جرم‌های برخط هدفی است غیرواقعی ولی برداشتن قدم‌های ساده‌ای مانند احراز هویت چند عاملی احتمال اینکه شما قربانی بعدی باشید را بطور قابل توجهی کاهش می‌دهد.

## طرح مسأله

یکی از نقاط کلیدی که احراز هویت چند عاملی می‌تواند نقش بسزایی در افزایش امنیت ایفا کند، شبکه‌های محلی مورد استفاده در شرکت‌ها و سازمان‌ها است. بطور مرسوم دسترسی به کامپیوترهای شبکه محلی بر اساس احراز هویت تک عاملی انجام می‌گیرد. نکته قابل توجه آن است که بطور معمول در سازمان‌ها، کلمه عبور مسأله‌ای کاملاً شخصی نبوده و طیف وسیعی از همکاران از آن اطلاع دارند. این مسأله علاوه بر امکان نشت اطلاعات کلیدی موجود در رایانه مقصد، به نفوذگران امکان اجرای سناریوهای پیچیده‌تر و پیشرفته‌تری برای دسترسی کامل به داده‌های موجود در شبکه می‌دهد. چرا که امکان اجرای سناریوهای نفوذ، با وجود کاربرِ احرازِ هویت شده به مراتب ساده‌تر می‌باشد.

تعداد قابل ملاحظه‌ای از سازمان‌ها با وجود صرف هزینه‌های بسیار در قالب دیواره‌های آتش، سوئیچ‌ها و مسیریاب‌های پیشرفته و ...، برای حفظ امنیت شبکه و داده‌های حیاتی خود همچنان از حفاظت نقاط ورودی بسیار حساس شبکه مانند ایستگاه‌های کاری و خدمت‌دهنده‌ها، نرم‌افزارهای سازمانی و ... تا حد زیادی ناتوان هستند. نشت اطلاعات از این طریق می‌تواند منجر به بروز مشکلات و آسیب‌های جبران ناپذیری برای سازمان و ذینفعان در جنبه‌های مختلف اقتصادی، اجتماعی، فرهنگی و سیاسی شود.

همین مسأله در مورد سایر نقاط ورودی سازمان مانند شبکه اختصاصی مجازی، نرم‌افزارهای سازمانی تحت وب، پست الکترونیک و ... صادق است. برای اجرای موفق راه حل جامع احراز هویت چند عاملی باید خدمات ارائه شده قابلیت یکپارچگی سریع و آسان با زیرساخت امنیتی موجود سازمان را فراهم آورند. این خدمات در عین سهولت کاربری، باید قابلیت استفاده از مؤلفه‌های متفاوت در سناریوهای مختلف را دارا باشند.

## کیپر (Qiper)

کیپر یک راهکار با پوشش کامل، برای اجرا و یکپارچه‌سازی احراز هویت چند عاملی در سازمان‌ها، بخصوص سازمان‌هایی که از خانواده محصولات مایکروسافت مانند ActiveDirectory در شبکه خود استفاده می‌کنند، می‌باشد. کیپر طیف متنوعی از عوامل که در این مستند از آن ها با نام توکن یاد می‌شود را پشتیبانی می‌کند. برای اجرای سناریوهای مختلف مقاوم‌سازی می‌توان از عوامل مختلف استفاده کرد. توکن‌های جاری پشتیبانی شده توسط کیپر عبارتند از:

- ✓ پیامک (SMS)
- ✓ خانواده رمزهای یکبار مصرف (TOTP و HOTP)
- ✓ اعلان به روش Push
- ✓ توکن‌های سخت افزاری FIDO2/U2F

با توجه به مشخصات عملکردی پشتیبانی شده توسط کیپر، با افتخار می‌توان آن‌را در رده محصولات مشابه ارائه شده توسط شرکت‌های معظمی مانند Fortinet، در سطح جهانی دسته بندی نمود. مزیت رقابتی کیپر نسبت به رقبای خارجی این است که به دلیل ایجاد زیرساخت های فنی توسط متخصصین ایرانی و انجام کلیه فرایندها در داخل کشور از تهدیدهای ساختاری بالقوه‌ی نمونه‌های خارجی مصون خواهد بود.

شرکت آرایه سازان ماندگار با در اختیار داشتن دانش طراحی و توانایی تولید بومی، مفتخر به ارائه راه‌حل و راهکار برای نیازهای امنیتی خاص است.

کیپر علاوه بر برآورده‌سازی نیازمندی‌های امنیتی خاص استفاده‌کننده، شخصی‌سازی راه‌حل براساس مقدورات، امکان‌سنجی شرایط موجود، هم در حوزه عملکرد و هم در حوزه طراحی، نصب، راه‌اندازی و درنهایت نگه‌داری، پاسخگوی نیازهای کاربران است.

دستاوردهای فرآیند طراحی و اجرای کیپر و مؤلفه‌های مربوطه:

- یکپارچه‌سازی بی‌دردسر و آسان با زیرساخت‌های امنیتی موجود در سازمان و کاربری و راهبری با سهولت هرچه بیشتر
- حفظ امنیت و برآورده‌سازی نیازهای مربوطه

تمامی مؤلفه‌های مورد نیاز برای پیاده‌سازی زیرساخت احراز هویت چند عاملی در زیر یک چتر واحد ارائه می‌شوند که این امر موجب کسب اطمینان خاطر استفاده‌کننده از یکپارچگی و سازگاری کامل مؤلفه‌ها با یکدیگر و کل زیرساخت موجود و همچنین امنیت ارائه شده کیپر می‌باشد. در عین حال هزینه تمام شده کلی استفاده از راهکار به نسبت سایر ارائه‌دهندگان بسیار پایین‌تر بوده و در ازای هر واحد هزینه، ارزش افزوده بیشتری توسط استفاده‌کننده دریافت خواهد شد.

# معماری راه حل

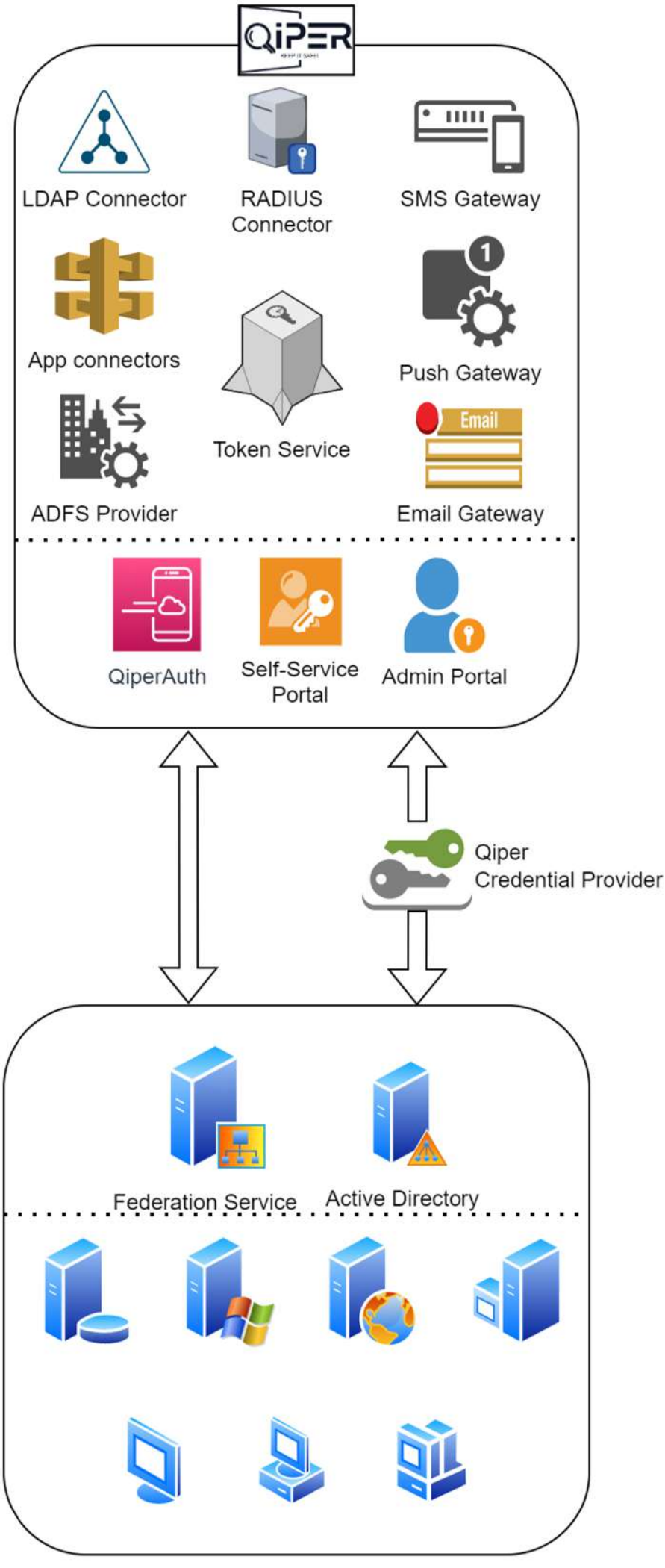
در این بخش به معرفی معماری کلی کیپر و مؤلفه‌های مربوطه می‌پردازیم.
در طراحی کیپر تلاش بر آن بوده تا بدون اعمال تغییرات در زیرساخت موجود فرد یا سازمان استفاده‌کننده، امکان استفاده از احراز هویت چند عاملی در زیرساخت فراهم شود. در شکل روبرو نمای کلی کیپر و مؤلفه‌های مربوطه ارائه گردیده است.

در قلب کیپر خدمت‌دهنده توکن قرار دارد که وظیفه ایجاد، مدیریت و تصدیق هویت توکن‌ها را بر عهده می‌گیرد. منظور از توکن عوامل احراز هویت دوم کاربران است که هم‌اکنون شامل عوامل زیر می‌باشد:

- ✓ پیامک (SMS)
- ✓ خانواده رمزهای یک‌بار مصرف (TOTP و HOTP)
- ✓ اعلان به روش Push
- ✓ توکن‌های سخت افزاری FIDO2/U2F

خدمت‌دهنده توکن از اتصالات مختلفی جهت ارتباط با ارائه‌دهنده‌های سرویس پیامک، پست الکترونیکی و اعلان Push جهت ارسال Challenge مربوطه در زمان احراز هویت استفاده می‌کند.

**کیپر** با استفاده از رابط LDAP با زیرساخت ActiveDirectory در ارتباط است. این ارتباط در قالب فقط خواندن بوده و هیچ‌گونه تغییری توسط کیپر در زیرساخت موجود اعمال نمی‌گردد. وظیفه این مؤلفه دریافت اطلاعات کلی کاربران مانند نام کاربری و همچنین فرایند احراز هویت می‌باشد.


QiPER
LDAP Connector
RADIUS Connector
SMS Gateway
App connectors
Push Gateway
Token Service
ADFS Provider
Email
Email Gateway
QiperAuth
Self-Service Portal
Admin Portal
Qiper Credential Provider
Federation Service
Active Directory


## اجرای فرایند احراز هویت

برای اجرای فرآیند احراز هویت چند عاملی در زمان ورود کاربر به ایستگاه‌های کاری و خدمت‌دهنده‌ها، کیپر مؤلفه QiperCP را ارائه نموده است که جایگزین Windows Credential Provider شده و با برقراری ارتباط با Active Directory و خدمت‌دهنده توکن فرآیند را چه در زمان ورود محلی و چه در زمان ورود از راه دور (Remote Desktop) اجرا خواهد نمود.

علاوه بر صفحه ورود ویندوز، کیپر با ارائه مؤلفه‌های اتصالی امکان اتصال احراز هویت چند عاملی را برای مؤلفه‌های مختلف ارائه می‌دهد. لیست برخی از مؤلفه های قابل استفاده در زیرساخت کیپر عبارتند از:

- ✓ Active Directory Federation Service
- ✓ FreeRADIUS
- ✓ Microsoft NPS server
- ✓ OpenVPN

فرآیند تعریف و استفاده از احراز هویت چند عاملی بسیار ساده است. مدیران سیستم بطور معمول کاربر را تعریف نموده و دسترسی‌های لازم را تنظیم می‌کنند. کاربر با مراجعه به پرتال کاربران با استفاده از نام کاربری و کلمه عبور، توکن خود را ایجاد، سپس با استفاده از توکن امکان ورود به سرویس‌های مجاز را خواهد داشت. همچنین در صورتی که توکن کاربر از نوع رمزهای یک‌بار مصرف یا Push باشد، کاربر می‌تواند از برنامه تلفن همراه QiperAuth به منظور مدیریت توکن‌های خود استفاده نماید. در صورتی که به هر دلیلی کاربر، توکن خود را از دست بدهد، می‌تواند با استفاده از پرتال کاربران، توکن خود را غیرفعال نماید. در صورت تأیید مدیر سیستم، کاربر مجدداً قادر به ایجاد و استفاده از توکن جدید خواهد بود.

**قابل ذکر است براساس نیاز هر سازمان امکان ارائه خدمات پشتیبانی، شخصی‌سازی و توسعه وجود دارد.**

آرایه سازان ماندگار

metaVAS
Empowered imagination

02
احراز هویت چندعاملی
به وسیله سخت‌افزار

01
احراز هویت چندعاملی
به وسیله سرور

03
احراز هویت چندعاملی
به وسیله اپلیکیشن

QiPER
KEEP IT SAFE!

کیپر

راه حل احراز هویت چند عاملی


**تماس با ما:**

خیابان کریمخان، بین ایرانشهر

و ماهشهر، پلاک ۱۴۲، طبقه ۲

۰۲۱-۸۷۱۲۸

Info@metavas.com

www.metavas.com

www.qiper.ir