TOSAN
NEGIN SOFTWARE DEVELOPMENT CO.
شرکت توسعه سامانه های نرم افزاری نگین (توسن)

ماژول صدور کلمه عبور یکبار مصرف

(One Time Password Generator)

جهت ارائه در سایت توسن

بهار ۱۳۸۹

www.tosan.com

تهران، خیابان آفریقا، کوی نور، شماره ۱۸
تلفن: ۸۲۱۹۸۰۰۰ دورنگار: ۸۸۷۸۲۷۴۲

فهرست مطالب

مقدمه:

امروزه کاربران با آسودگی خاطر و با سرعت بالا از بانکداری الکترونیک استفاده می کنند و دیگر هیچ محدودیتی جهت کار در ساعات اداری بانکها ندارند.

در کنار فرصت های باورنکردنی برای انجام بانکداری الکترونیک ، چالشهایی نیز جهت حفظ امنیت این راه پر پیچ و خم رو به رشد وجود دارد.

در حال حاضر روشهای گوناگونی برای حمله به سیستمهای کامپیوتری تحت شبکه وجود دارد. از انواع این حملات می‌توان به حدس زدن کلمات عبور ضعیف و نامناسب ، تست کردن تمامی حالتهای ممکن ، حملات بر اساس لغتنامه ها و بی‌دقتی و اشکال درپیکربندی سیستم اشاره کرد.

روشهای هوشیارانه برای افزایش انواع حمله های اینترنتی از قبیل دزدی هویت ، در صورت بروز می تواند خسارات جبران ناپذیری به بار آورد.

از نکات مهم در سیستمهای بانکداری اینترنتی و تجارت الکترونیکی اعتماد به طرف مقابل آن می‌باشد به این معنی که مطمئن باشیم طرف مقابل ما دقیقا همان کسی است که ادعا می‌کند.

امروزه در اکثر سرویسهای بانکداری اینترنتی ، نیاز به ورود نام کاربری و رمز عبور می باشد که در صورت ثابت و ایستا بودن این رمز عبور ، امکان فاش شدن آن توسط افراد سودجو بسیار زیاد می باشد.

مکانیزم امنیتی که جهت جلوگیری از این خطرات می توان بکار برد ، استفاده ازOTP (One Time Password) یا همان "رمز عبور یکبار مصرف "می باشد.

هدف استفاده از OTP پیچیده تر شدن دسترسیهای غیر مجاز به منابع اطلاعاتی می باشد،تجربه نشان داده است دسترسی به رمزهای ایستا که توسط کاربران ایجاد میشود بسیار ساده میباشد،در نتیجه OTP یا کلمه های عبور یکبار مصرف ، مکانیزم جدیدی است که برای تایید هویت معرفی میگردد. این مکانیزم مشکلات استفاده از کلمات عبور ثابت را حل کرده به این صورت که کاربر برای هر جلسه کاری خود کلمه عبور مجزایی داشته باشد .

دستگاههایی که توسط آنها می توان رمز یکبار مصرف تولید نمود OTP Token نام دارند که دارای انواع مختلفی می باشند.

OTP Token یک سیستم مستقل نیست و کاری که انجام میدهد با سیستمهای دیگر کامل می شود ، به عبارت دیگر کلمات عبوری که تولید می کند توسط سیستم دیگری بنام AAServer یا سرور تایید هویت مرکزی بررسی می شوند .این سیستم دارای واسط کاربری ساده ای می باشد و کار کردن با آن نیاز به آموزش خاصی ندارد. کاربر به راحتی و بدون نیاز به تایپ و یا به یادسپاری هرگونه دستوری می تواند برای تولید کلمه عبور از آن استفاده نماید .

در مستند حاضر قابلیت ها ، معماری ، تکنولوژی و امنیت سیستم OTP وابزارهای سخت افزاری مورد استفاده در این راستا مورد بررسی قرار گرفته است.

۱–دسته بندی انواع OTP Token :

به منظور تولید کلمات عبور یکبار مصرف از ابزاری به نام OTP Token استفاده می گردد . که این ابزار می تواند به صورت سخت افزاری (OTP Token های دارای کارت هوشمند و OTP Token های بدون کارت هوشمند) و یا نرم افزاری (نرم افزارهای قابل نصب برروی pc و یا موبایل) در اختیار کاربر قرار گیرد.

۱-۱-Otp Token های مبتنی بر کارت هوشمند :

این دستگاه ها متشکل از یک کارت هوشمند و یک توکن به عنوان کارتخوان هوشمند می باشند .در این دستگاهها کلیه الگوریتم ها درکارت هوشمند قرار می گیرند و توکن فقط جهت خواندن اطلاعات کارت و نمایش رمز تولید شده بکار می رود.

۱-۲- OTP Token های بدون کارت هوشمند :

این دستگاهها در دو دسته قابل ارائه می باشند:

۱-۲-۱- مدل غیرکارتی : توکن ها به تنهایی و بدون نیاز به کارت هوشمند امکان تولید و نمایش رمز تولید شده را دارند .این توکن ها براساس نوع الگوریتم موجود در مدلهای مختلف قابل ارائه می باشند

۱-۲-۲-**مدل کارتی**: این دستگاههای تولید رمز یکبار مصرف ، درواقع فقط یک کارت می باشند .این کارتها دارای یک صفحه نمایش برروی خود بوده وبه تنهایی و بدون نیاز به هیچ کارتخوانی قادر به تولید و نمایش رمز یکبار مصرف هستند.

۱-۳- OTP Token نرم افزاری :

در این سیستم ، رمز یکبار مصرف توسط یک نرم افزار تولید می شود که این نرم افزار قابل نصب و بکارگیری برروی موبایل و PC می باشد.

شرکت توسن امکان ارائه کلیه مدلهای فوق را به مشتریان خود دارا می باشد.

۲– قابلیت های سیستم

قابلیت های اصلی این سیستم عبارتند از:

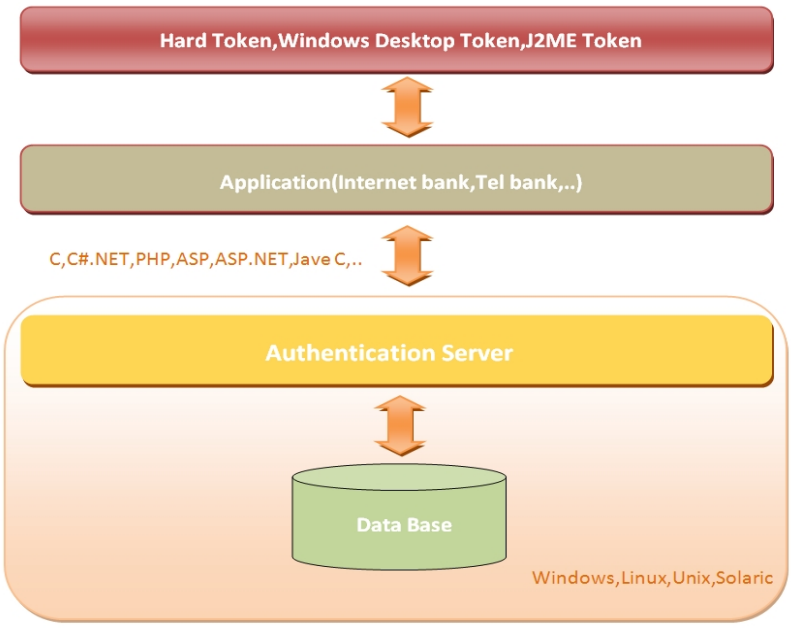
- امکان استفاده از برنامه OTP هم به شکل مستقل در یک کارت و هم به شکل Multi Application در کنار سایر برنامه های کارت (در OTP Token های دارای کارت هوشمند)
- استفاده از الگوریتم های استاندارد جهت تولید کلمه عبور
- تأیید کلمه عبوری تولید شده کاربر توسط AA Server
- استفاده یک و فقط یکبار از کلمه عبوری تولید شده و غیرقابل استفاده بودن کلمه عبوری درصورت فاش شدن آن
- منحصر بفرد بودن شماره سریال OTP Token های سخت افزاری در تمام دنیا

۳–ویژگی های سیستم

۳-۱- معماری نرم افزاری:

OTP Token ها یک سیستم مستقل نیستند و کاری که انجام می دهند با سیستم های دیگر کامل میشود به عبارت دیگر کلمات عبوری که تولید می کنند توسط سیستم دیگری بنام AAServer یا سرور تایید هویت مرکزی بررسی می شود .

شمای کلی معماری نرم افزاری این سیستم در شکل زیر قابل مشاهده می باشد:



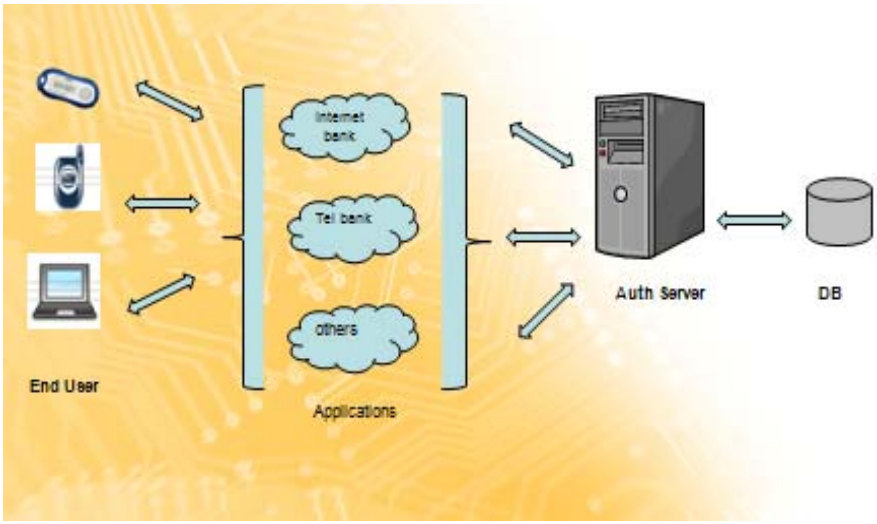
۲-۳-امنیت سیستم

به علت یکبار استفاده از رمز ایجاد شده توسط کاربر احتمال ورود کاربری دیگر به سیستم به واسطه رمز قبلی برای سرقت اطلاعات و یا دسترسی به اطلاعات امکانپذیر نمی باشد.همچنین در صورت آسیب دیدگی فیزیکی و باز شدن سخت افزار OTP Token ، محتویات چیپ داخلی آن از بین رفته و قابل بازگشت نمی باشد و در نتیجه نمی توان ازآن برای بدست آوردن اطلاعات کاربر استفاده کرد.

۴–سرور تایید هویت (AA Server) و قابلیت های آن :

AA Server یک سیستم تایید هویت مرکزی است که عمل تایید هویت تمامی کاربران را به صورت متمرکز انجام می دهد. این سیستم دارای قابلیت ارتباط با سایر سیستمها از جمله اینترنت بانک و تلفن بانک است و می تواند کاربران این سیستمها را نیز تایید هویت نماید . به این ترتیب این سیستم ها نیز می توانند عمل تایید کاربران خود را به AA Server واگذار نمایند.

ساختار کلی سیستم به صورت زیر می باشد :

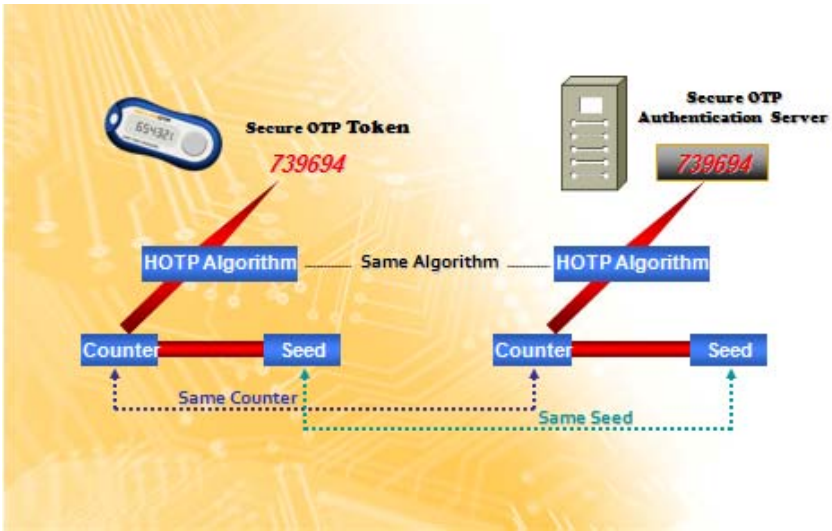


قابلیت های سرور تایید هویت شامل موارد زیر می باشد :

۱-۴-تایید هویت کاربران :

وظیفه عمده AA Server تایید هویت کاربران است . تایید هویت به دو صورت استاتیک و OTP انجام میشود . در تایید هویت استاتیک ، مانند آنچه در سیستمهای معمولی برای تایید هویت استفاده میشود ، رمز کاربر در دیتابیس AA Server نگهداری میشود و در هنگام Login به سیستم با رمز وارد شده ، مقایسه می گردد اما در تایید هویت OTP ، هم AA Server (ســـــرور تایید هویت مرکزی) و هـم OTP Token کلمه رمز یکبار مصرف را تولید می کنند. در تایید هویت OTP کاربر با استفاده از OTP Token ای که دراختیار دارد کلمه رمز را تولید می کند و این کلمه رمز را مثلا در صفحه Login اینترنت بانک وارد می کند . اینترنت بانک ، عمل تایید هویت کاربر را به AA Server واگذار می نماید . AA Server بااستفاده از داده هایی که برای کاربر ذخیره کرده و الگوریتمی که دارد، کلمه رمز مربوط به این جلسه کاری را تولید میکند (دقیقا به همان صورتی که در OTP Token رمز تولید میشود) و این کلمه رمز را با آنچه که کاربر فرستاده است ، مقایسه می نماید . اگر این دو رمز با یکدیگر یکی باشد کاربر را تایید می کند .

اما اگر این دو رمز با یکدیگر یکی نباشند احتمال دارد که شمارنده OTP Token کاربر به دلیل استفاده نا مناسب از آن ، با شمارنده سمت سرور یکی نباشد (در مورد OTP Token هایی که براساس شمارنده کار می کنند)مثلاً کاربر همین طور ، رمز OTP تولید کرده باشد ، اما از این رمزها استفاده نکرده باشد (تعداد ساخته شدن رمز پارامتریک است ولی چون با زیاد شدن تعداد رمز های تولید شده و استفاده نکردن از آن توسط کاربر باعث پایین آمدن استاندارد امنیتی می شود بنابراین پیشنهاد تولید ده عدد رمز در نظر گرفته می شود) . در این حالت ، شمارنده OTP Token کاربر اضافه شده ، اما شمارنده کاربر سمت سرور اضافه نشده است . در نتیجه رمزهایی که این دو تولید می کنند با یکدیگر متفاوت میگردد . در این وضعیت ، یعنی هنگامی که رمزی که کاربر ارسال نموده با رمزی که سرور تولید کرده متفاوت است ، AAServer چند بار دیگر نیز رمز OTP را با شمارنده های بعدی تولید میکند (معمولاً تا ۱۰ رمز بعدی)و اگر در هر یک از این مراحل ، رمز ارسال شده با رمز سرور یکی شد ، کاربر را تایید هویت میکند و مقدار جدید شمارنده را نیز ذخیره می کند



۴-۲-مدیریت کاربران :

وظیفه دیگر AAServer تعریف کاربران در سیستم است . برای اضافه کردن کاربر به سیستم ، باید اطلاعات کاربر در سیستم ذخیره شود . این قابلیت در سیستم وجود دارد که اطلاعات کاربر را از Core دریافت نماییم . همچنین مدیر سیستم میتواند کاربر را فعال یا غیرفعال نماید . کاربری که غیرفعال است نمی تواند به هیچ سیستمی Login نماید.

۴-۳-تخصیص OTP Token به کاربر :

در مرحله تولید ، OTP Token به هیچ کاربری تخصیص داده نمی شود . با تخصیص OTP Token به کاربر درمرحله Personalizing ، توکن فعال میشود و می توان برای ورود به سیستم از آن استفاده نمود . لازم به ذکر است که هر کاربر می تواند تنها یک OTP Tokenاز یک نوع خاص داشته باشد .

۴-۴-تغییر تنظیمات OTP Token :

هر OTP Token حاوی یک سری اطلاعات است که برای تولید OTP از آنها استفاده میشود . مدیر سیستم برخی از این اطلاعات را میتواند ویرایش نماید . مثلا میتواند تعداد مجاز رمزی که کاربر می تواند اشتباه وارد کند را تغییر دهد و یا طول کلمه عبور یک بارمصرفی را که OTP Token کاربر تولید میکند تغییر دهد ، مثلا OTP Token یک کاربر ، رمز ۶ رقمی تولید کند و توکن کاربر دیگر ، رمز ۸ رقمی .

۴-۵- همزمان سازی OTP Token با سرور :

در حالتی که شمارنده OTP Token کاربر با شمارنده سرور متفاوت است و از حالت تقارن با سرور خارج می شود ، (در مورد دستگاههایی که بر مبنای شمارنده کار می کنند).در این وضعیت ، کاربر نیاز دارد بدون مراجعه حضوری و تعویض OTP Token ، بتواند دوباره از آن استفاده نماید . برای این کار لازم است کاربر، شماره کاربری خود، شمارنده دستگاه ، مکانیزم مورد نظر ، و OTP ای که با این ویژگیها تولید می شود را برای AAServer ارسال نماید . اگر با این اطلاعات وارد شده ،OTP تولید شده در سمت AAServer ، همان OTP ارسال شده توسط کاربر باشد ، پس مشکلی وجود ندارد و فقط دستگاه تولید رمز یکبار مصرف از حالت تقارن خارج شده است . در اینصورت AAServer شمارنده خود را به شمارنده دستگاه کاربر تغییر می دهد و به کاربر پیغام میدهد که می تواند از دستگاه دوباره استفاده نماید .

در انتهای این مستند به بررسی اجمالی قابلیتها و مشخصات TOSAN AAServer پرداخته شده است.

۵–انواع مدلهای OTP Token قابل ارائه توسط توسن

ایجاد بستری امن برای مشتریان و کاربران بانکی یکی از مهمترین چالشهای شرکتهای ارائه دهنده راهکارهای بانکی می باشد،بر پایه همین سیاست شرکت توسن اقدام به ارائه انواع دستگاههای تولید رمز یکبار مصرف نموده است تا امکان انتخاب مدل مورد نظر مشتریان را با توجه به شرایط و نیازهای آنها برآورده سازد.

در این بخش به بررسی انواع محصولات قابل ارائه توسط توسن در زمینه سیستم OTP خواهیم پرداخت:

۱- Self-Key Negin

۲- Securemetric

۵-۱-Self-Key Negin :

دستگاه Self-Key تولید شده توسط شرکت توسن بوده و نحوه کار آن بر پایه کارت هوشمند می باشد .

بدین ترتیب که کلیه الگوریتم ها در کارت هوشمند موجود می باشند و رمز عبور یکبار مصرف توسط این کارت تولید می گردد.

رمز عبور تولید شده توسط کارت هوشمند می بایست به طریقی به کاربر اعلام شود . به همین منظور به هر کاربر علاوه بر کارت هوشمند یک دستگاه ماژول نمایشگر کلمه عبور ارائه می گردد . این ماژول سخت افزاری ، کوچک و قابل حمل بوده و از یک چیپ و یک صفحه نمایش LCD جهت نمایش کلمه عبور تشکیل شده است . با قرارگرفتن کارت هوشمند در محل مخصوص ماژول OTP و با فـــــــرمان کاربـــــر و استفاده از یکی از مکانیزم های (Code ، E-Code ، Sign) که شرح آن در ادامه آمده است کلمه عبور تولید شده و در صفحه نمایشگر ماژول نشان داده می شود .

۱- اجرای دستورات سیستم مبتنی بر شمارنده (Code)

در این مکانیزم ، تولید کلمه عبور یکبار مصرف نیاز به واردکردن رمز استاتیک کارت نداشته وبا انتخاب این تابع توسط کاربر کلمه عبور تولید و نمایش داده می شود . به عنوان مثال برای ورود به سیستم و شناسایی هویت کاربر در سیستم اینترنت بانک می توان از کلمه عبور OTP از نوع Code استفاده نمود.

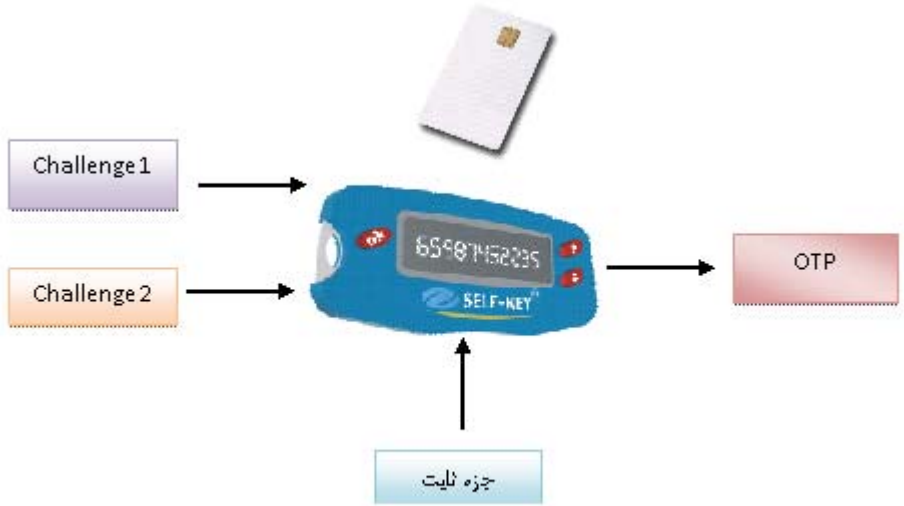
۲- اجرای دستورات سیستم مبتنی بر شمارنده – رمز (E-Code)

استفاده از مکانیزم E-code که مبتنی بر شمارنده می باشد ، نیاز به وارد کردن یک PIN در توکن دارد (که به جزء 'رمز ' در نام این مکانیزم اشاره دارد) . کاربر با انتخاب این تابع و وارد کردن کلمه عبور ثابت ، کلمه عبوری مناسب با آن جلسه کاری را به دست می آورد .

۳- اجرای دستورات سیستم مبتنی بر درخواست و پاسخ (Sign)

در مکانیزم Sign شمارنده ای وجود ندارد . این الگوریتم به یک جزء ثابت و دو جزء متغیر نیاز دارد که ورودیهای متغیر در آن را اصطلاحا Challenge می نامیم .

توکن ، ورودیهای Challenge1 , Challenge2 را از سرور دریافت میکند و OTP را تولید می کند . به عنوان مثال برای سرویس انتقال وجه که از اهمیت بالایی برخورداراست می توان از رمز عبور یکبار مصرف از نوع Sign می باشد استفاده نمود .



توکن کارت هوشمند ، برای کاربران Personalize می شود و نیز در زمان شخصی سازی ، مدیریت کلیدهای رمزنگاری منحصربه فرد تولید شده برای هرکارت ، ازمهمترین مولفه امنیتی این سیستم در تولید OTP می باشد . این کلیدها به کارت ارسال شده و درآن نگه داری می شود.

Secure Metric –۵–۲

شرکتSecure metric یکی از شرکتهای پیشرو در ارائه راهکارهای پرداخت در دنیا می باشد .یکی از اهداف اصلی این شرکت ارائه انواع راهکارهای امنیتی در زمینه های بانکداری بوده که در این راستا نیز اقدام به تولید انواع سخت افزارهای امنیتی و توکن های تولید رمز یکبار مصرف نموده است

شرکت توسن نیز در راستای ایجاد بستری امن برای کاربران اینترنتی و ارائه محصولات دارای کیفیت بالابه مشتریان خود ، اقدام به اخذ نمایندگی انحصاری این شرکت در ایران نموده است تا ضمن تضمین امنیت برای مشتریان خود، امکان انتخاب محصولات مختلف سخت افزاری را در اختیار آنها قرار دهد.

۱-۲-۵- انواع OTP Token های غیر کارتی Securemetric :

Secure OTP Event–۱

در این مدل ، توکن براساس شمارنده کار می کند.بدین معنی که به ازای هربار فشار دکمه دستگاه ،یک واحد برشمارنده آن اضافه می شود و الگوریتم موجود در این توکن با استفاده از این شمارنده ، یک رمز جدید تولید می نماید. که این رمز یکبار مصرف می باشد.

Secure OTP Time–۲

این ابزار براساس real time clock توکن و سرور کار می کند. به این صورت که هر ۶۰ ثانیه یکبار ، رمز آن عوض می شودو این قابلیت باعث می شود که محدوده زمانی برای دستیابی و سوء استفاده از این رمز بسیار کوتاه شده و این باعث بالا بردن ایمنی می شود.

Secure OTP Hybrid-۳

در این مدل ، توکن قابلیت ارائه Event base OTP و PKI (Public Key Infrastructure) رابه صورت همزمان به کاربر دارد.

این توکن هم می تواند جهت تولید رمز یکبار مصرف و هم به عنوان محل امنی جهت نگهداری گواهینامه های دیجیتالی و اعتبار نامه ها ، هنگام استفاده از محیط های PKI بکار رود.

این دستگاه ، ابزار بسیار مناسبی جهت Authentication قوی و همچنین انجام تراکنش های ایمن و حفاظت از دیتاها می باشد.

Secure OTP CR -۴ (Challenge & Response)

دراین مدل توکن ، ورودی Challenge توسط کاربر از سرور دریافت گردیده و پس از ورود آن به توکن ، این دستگاه اقدام به تولید یک رمز یکبار مصرف می نماید.

۲-۲-۵- انواع OTP Token های مدل کارتی تولید رمز یکبار مصرف Securemetric :

محصولات این شرکت شامل انواع Card OTP به شرح زیر نیز می باشد :

۱- Event One Key Card OTP:

کارتی که از قابلیت امکان تولید رمز یکبار مصرف برپایه قابلیت Event برخوردار بوده و به منظور نمایش این رمز دارای یک صفحه نمایش برروی کارت می باشد.

۲- Time One Key Card OTP:

کارتی که از قابلیت تولید رمز یکبار مصرف برپایه Timeبرخوردار بوده و به منظور نمایش این رمز دارای یک صفحه نمایش برروی کارت می باشد

۳- Challenge & Response 12 Keys Card OTP:

این کارت به منظور تولید رمز یکبار مصرف ، از قابلیت Challenge & Response استفاده می نماید که بدین منظور و جهت ورود Challenge ، دارای ۱۲ کلید ورودی می باشد و همجنین رمز تولید شده را نیز با استفاده از صفحه نمایش موجود برروی کارت نمایش می دهد

۳-۲-۵- سایر محصولات Securemetric :

سایر تولیدات این کمپانی نیز جهت ایجاد راهکارهای امنیتی به شرح زیر می باشد:

- **Secure token ST2 & ST3**

(USB pkI token)

- **Secure COS(Cryptographic Smart Card)** :

(PKI smart card)

۴-۲-۵- مشتریان Securemetric :

برخی از بانکهایی که از محصولات این شرکت استفاده کرده اند:

- MayBank2e
- Public Bank
- EON BankGroup
- PKI System Authentication
- Retail e-Banking Authentication
- Public PKI Authentication
- 2FA Authentication Partnership

۵-۲-۵- پروژه های Securemetric:

برخی از پروژه هایی که در آنها از محصولات این شرکت استفاده شده است:

- Prime Minister Office Network and VPN Authentication
- Government e-Procurement System Authentication
- Certificate Authority Projects in Malaysia
- Public PKI Authentication
- Vendor e-Procurement System Authentication
- Patient Record and Work Flow System Authentication
- Authentication Solutions for Financial and Government

همچنین شایان ذکر است که در کلیه مدلهای توکن نامبرده قابل ارائه توسط توسن ، امکان حک نمودن لوگوی بانک یا موسسه برروی این سخت افزارها موجود می باشد .

۶– مروری بر TOSAN AAServer:

در ذیل به بررسی مختصری از مشخصات و قابلیت های TOSAN AAServer خواهیم پرداخت:

Key features :

Wide range of authentication methods

• OATH-based one-time password (OTP) authentication.
• Static secrets, in full or partial mode, including passwords, PINs.
• Pluggable framework enables easy adoption of new authentication methods.

Comprehensive management tools

• Support for a wide range of authentication methods plus easy adoption of new methods enables organizations to consolidate multiple physical methods into a single logical authentication model within a Service Oriented Architecture.
• Full lifecycle management of user credentials and physical devices.
• All authentication and administration actions are recorded within a centralized audit log.
• Administration tools including token/ card activation, PIN reset and password maintenance.
• Multiple service channel support (Web, IVR, ATM etc.) using a single authentication platform.

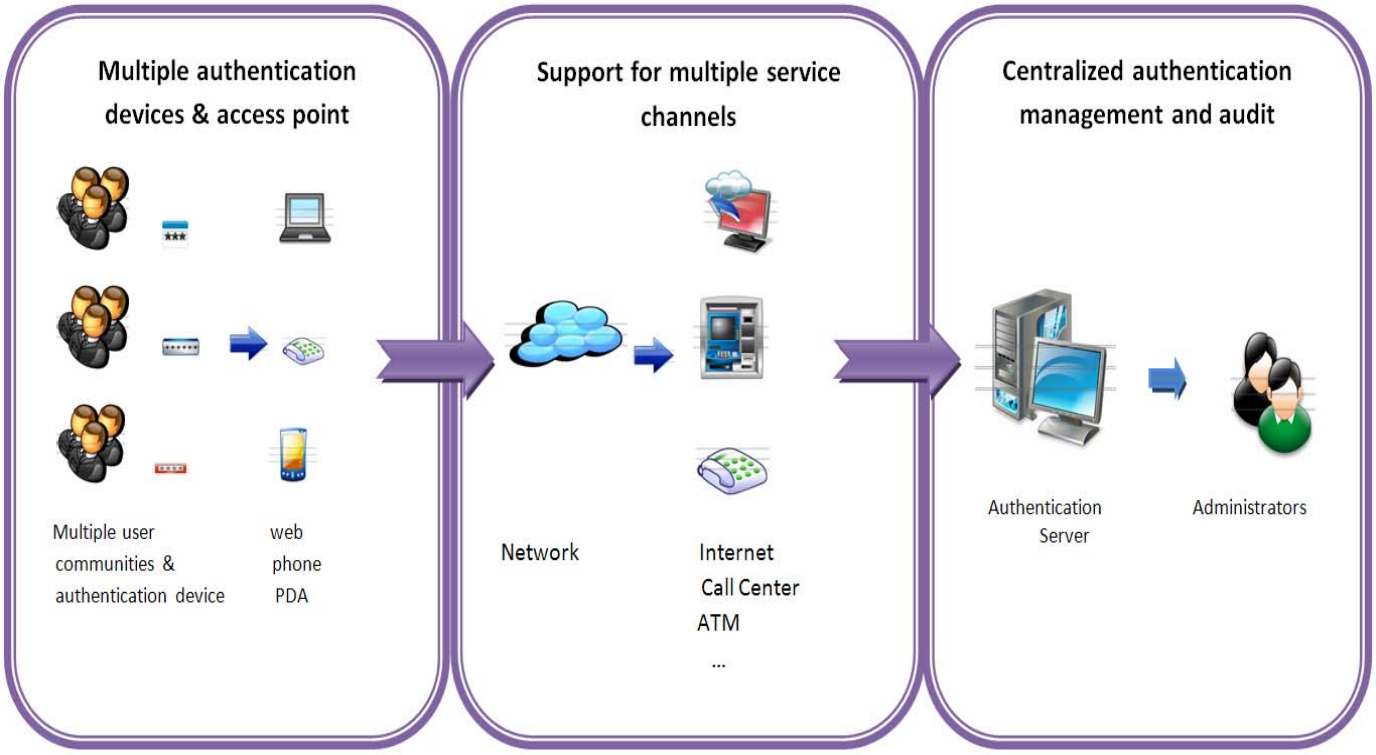
Rapid deployment capabilities

• Authentication Server can be deployed on a variety of platforms.
• All Authentication Server functions are exposed through a standards-based public API that can be accessed via SOAP for easy integration to a wide range of environments.

Technical specification

Operating systems
• Windows, Linux
Devices
• Kishware self-key
• secure metric event base token
• secure metric time base token
• secure metric challenge/response token
• Any hardware or software tokens compliant with OATH HOTP algorithm
Authentication schemes
• One-time passwords (OTP)
- ActivIdentity one-time passwords
- OATH one-time passwords
• PIN verification
• Static passwords (e.g. username / password logins)
Administration features
• Password management
- Auto generation
- Help desk change/reset
- Set up
• Device management
- Synchronise
- Unlock
- Assign/unassign
- Import
• Credential management
- Status (enable/disable)
- Channel specific usage policies
- Usage statistics
- Maintains validity periods
• User and permission management
- User and user group management
Standards compliance
• Sun J2EE™
• Java RMI and SOAP v1.1
• OATH HOTP
Integration
• Java RMI
• Sun Java™, C and C#
• SOAP clients (available for Sun Solaris™, Windows®, AIX, Redhat Linux, SUSE™ Linux)
Encryption information
• Protects cryptographic keys using HSM
• Triple DES encryption / decryption of secrets

شمای کلی TOSAN AAServer **:**


Multiple authentication devices & access point
Multiple user communities & authentication device
web
phone
PDA
Support for multiple service channels
Network
Internet
Call Center
ATM
...
Centralized authentication management and audit
Authentication Server
Administrators