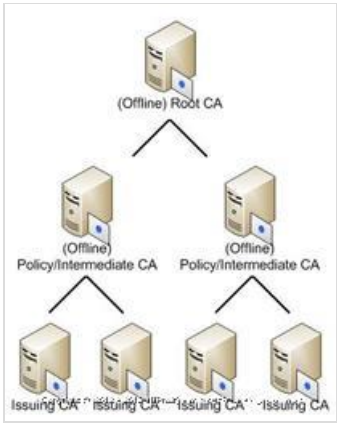
آموزش طراحی زیرساخت کلید عمومی (PKI) قسمت ۲ : ساختار سلسله مراتبی (نسخه چاپی)



در قسمت اول از این سری مقالات با کاربردهای PKI و برخی نیازمندی های آن در طراحی و پیاده سازی آشنا شدیم . قطعا تا اینجا متوجه شده اید که ساختار PKI یک ساختار سلسله مراتبی یا موروثی است و در اینگونه ساختارها همیشه یک یا چند والد یا Parent و چندین فرزند یا Child وجود دارد ، مشابه این طراحی را در بسیاری از ساختارهای مشابه مانند ساختار DSN و همچنین Domain های Active Directory در یک Forest مشاهده کرده اید . در این مقاله به نکاتی که در طراحی این ساختار در PKI نیاز است اشاره خواهیم کرد . منظور از طراحی ساختار سلسله مراتبی برای CA ها در PKI در واقع تعیین تعداد CA های موجود در PKI و همچنین روابط اعتمادی یا Trust Relationship بین آنها می باشد. در بیشتر شبکه های متوسط و رو به بزرگ استقرار بیش از یک CA پیشنهاد می شود.

طرح ریزی زیرساختار CA

قبل از اینکه شما به پیاده سازی ساختار PKI ای بپردازید که نیازهای امنیتی شما و سازمانتان را برطرف کند ، بایستی چند تصمیم مهم که در خصوص تعداد و شیوه قرار گیری CA ها در ساختار PKI می باشد در سازمان گرفته شود . طرح ریزی زیرساختارهای CA در سازمان شما نیازمند تصمیم گیری در خصوص موارد زیر است :

- محل قرار گیری CA های ریشه یا Root CA
- استفاده از CA های داخلی یا Third-Party
- انواع CA و نقش های آن
- تعداد CA های مورد نیاز

طراحی CA های ریشه یا Root CA ها

یک زیرساختار CA شامل یک سلسله مراتب و ساختار موروثی از CA ها می باشد که در بین تک تک آنها اعتماد یا Trust وجود داد و هر یک از آنها توانایی احراز هویت Certificate های یکدیگر را در این ساختار دارا می باشند. در این زیرساختار یک قدرت مطلق یا قدرت نهایی وجود دارد که در راس ساختار قرار گرفته است ، به این راس هرم یا شاخه در اصطلاح Root CA یا CA ریشه گفته می شود . بدون شک در هر ساختاری از CA یک Root CA وجود دارد. وظیفه اصلی Root CA انتخاب و پذیرش سایر CA های موجود در مجموعه جهت انتشار و مدیریت Certificate هایی است که در مجموعه سازمان صادر و مدیریت می شود.

انتخاب CA داخلی یا Third-Party CA

بسـته به کارکرد هایی که شـما نیاز دارید ، قابلیت هایی که زیرساختارهای فناوری اطلاعات و مدیران فناوری اطلاعات سازمان شما دارند و همچنین هزینه هایی که سازمان شما می تواند متقبل شود ، شما می توانید پایه و اساس زیر ساختار CA خود را بر اساس CA های داخلی بنا کنید و یا از CA های Third-party و یا ترکیبی از این دو را استفاده کنید.

CA های داخلی

اگر سازمـان شـما بیشتر فعالیت های تجاری و مروادات الکترونیکی خود را با سایر سازمان های همکار مـدیریت و کنترل می کنـد و قصـد نظارت بر شـیوه صدور و استفاده Certificate ها دارد ، بهترین گزینه اسـتفاده از CA ها داخلی می باشد ، مهمترین مزیت های اسـتفاده از CA های داخلی عبارتند از :

- به سازمان اجازه مدیریت و هدایت مستقیم بر روی خط مشی امنیتی سازمان را می دهد.
- به سازمان اجازه می دهد که بتواند Certificate Policy خود را به خط مشی امنیتی سازمانی اضافه کند.
- می تواند با زیر ساختار Active Directory Domain Services سازمان یکپارچه سازی شود.
- براحتی می توان با هزینه ای بسیار پایین قابلیت های جدیدی به آن اضافه کرد و آن را توسعه داد.

مضرات استفاده از CA های داخلی نیز شامل موارد زیر می باشد :

- سازمان بایستی Certificate های خود را مدیریت کند.
- زمـانی که برای پیاده سازی CA های داخلی صـرف می شود بسـیار بیشتر از زمانی است که برای استفاده از CA های خارجی صرف می شود
- سازمان بایستی خطرات و مشکلاتی که در ساختار PKI به وجود می آید را قبول کند.

CA های خارجی

اگر سازمـان شـما بیشتر فعـالیت ها و مراودات الکترونیکی خود را با مشتریان خارجی انجام می دهـد و می خواهـد که فرآینـد صـدور و مدیریت Certificate هـا در جای دیگری انجام شود ، بهترین گزینه اسـتفاده از ساختار CA های خارجی است ، مزایای اسـتفاده از CA های خارجی یا Third-Party CA ها به شرح زیر می باشند :

- به مشتریان شـما اجازه می دهد که درجه اعتماد بالاتری به سازمان شـما داشـته باشـند و از امنیت در تبادلات خود با سازمان شما مطمئن باشند.
- به سازمان شما این اجازه را می دهد که از مزیت استفاده از یک سرویس دهنده حرفه ای استفاده کنید.
- به سازمان این اجازه را می دهد که از یک ساختار امنیتی Certificate Based را بدون نیاز به راه اندازی CA داخلی استفاده کند.
- کلیه مسائل تجاری مربوط به Certificate ها و مشکلات مربوط به آن بر عهده سرویس دهنده مربوطه می باشد.

مضرات استفاده از Third-Party CA ها به شرح زیر می باشند :

- هزینه ها به ازای هر Certificate برای سازمان تا حدودی بالا می رود
- ممکن است برای مـدیرت و توسـعه دو عـدد اسـتاندارد مدیریتی نیاز باشد ، یکی برای مدیریت داخلی Certificate ها و یکی برای مدیریت Certificate های تجاری که بصورت خارجی صادر می شوند.
- قابلیت انعطاف پذیری و انجام تنظیمات و مدیریت آنها قطعا برای داخل سازمان محدود می شود.
- سازمان بایستی به Third-Party CA برای دسترسی پیدا کردن به CRL دسترسی داشته باشد.
- عملیات Auto Enrollment غیر ممکن است.
- Third-Part CA هـا معمولاـ قـابلیت کمی برای یکپرچگی بـا دایرکتوری های داخلی و نرم افزارهای کاربردی درون سازمانی دارنـد و یکپارچه کردن آنها با زیرساختارهای سازمانی داخلی معمولا مشکل ساز می شود.

تعریف انواع CA و نقش های آن

برای طراحی زیرساختار CA شما بایستی انواع مختلف CA هایی که در ویندوز سرور ۲۰۰۸ وجود دارند و نقشی که می توانند در شبکه شما ایفا کنند را به درستی درک کنید. سرویس Windows Server ۲۰۰۸ Certificate Services از دو نوع CA پشتیبانی می کند که به شرح زیر می باشند :

- Enterprise CA
- Standalone CA

هر دو نـوع Enterprise و Standalone می تواننـد به عنـوان Root CA و یا Subordinate CA در شـبکه فعالیت کنند. Subordinate CA ها همچنین می توانند به عنوان Intermediate CA یا CA های سـطح میانی که به عنوان Policy CA نیز شناخته می شوند و یا Issuing CA که برای صدور Certificate می باشـد ، مورد اسـتفاده قرار بگیرند. قبل از اینکه زیرساختار CA های خود را ایجاد کنیـد ، شـما بایستی نوع CA های مورد استفاده و نقشی که در ساختار PKI بر عهده دارند را به دقت در طراحی خود تعیین کنید.

مقایسه Enterprise CA و Standalone CA ها

Enterprise CA بصورت کامـل با اکتیودایرکتوری یکپارچه می شونـد . آنها Certificate ها و CRL ها را در اکتیودایرکتوری منتشـر می کنند. Enterprise CA هـا از اطلاعـات ذخیره شـده در اکتیودایرکتوری از قبیل اکانت های کاربری و Security Group ها برای تاییـد یا عدم تایید درخواست های Certificate اسـتفاده می کنند. آنها از Certificate Template ها اسـتفاده می کنند. زمانیکه یک Certificate صادر می شود ، Enterprise CA اطلاعات موجود در Certificate Template برای تولید Certificate ای با خاصـیت های مرتبط با نوع Certificate در خواست شده ، استفاده می کند.

اگر شـما می خواهیـد که فرآینـد تایید خودکار Certificate هـا و همچنین صـدور خودکار Certificate هـا یا Auto Enrollment داشته باشید بـایستی از Enterprise CA ها اسـتفاده کنیـد. این امکانات صـرفا در زیرساختارهای CA ای وجود دارنـد که بـا زیرساختار اکتیودایرکتوری یکپارچه شده اند. علاوه بر این ، تنها Enterprise CA ها هستند که می توانند Certificate هایی صادر کنند که برای استفاده در Smart Card های ورود به سیسـتم مورد اسـتفاده قرار بگیرند ، این امر به این دلیل است که این فرآیند نیاز به این دارد که Smart Card Certificate ای که صادر می شود به یک کاربر موجود در اکتیودایرکتوری مرتبط شود.

Standalone CA هـا از زیرساختـار اکـتیودایرکتوری اسـتفاده نمی کننـد و از طرفی از Certificate Template ها نیز اسـتفاده نمی کننـد. در صورتیکه از Standalone CA ها اسـتفاده میکنیـد ، تمامی اطلاعاتی که برای صدور Certificate مورد نظر نیاز می باشـد را بایستی در درون درخواست یا Request خود بگنجانیـد. بصورت پیشـفرض تمـامی درخواست های Certificate ای کـه برای CA ارسال می شوند در صـف pending در CA باقی می مانند تا مدیر CA آنها را تایید کند.شما می توانید Standalone CA ها را به گونه ای طراحی کنید که به درخواست های رسیده برای دریافت Certificate را بصورت خودکار پاسـخ داده و Certificate را صادر کنند ، اما اینکار پیشـنهاد نمی شود زیرا از لحاظ امنیتی درخواستی که به CA ارسال شده است هنوز احراز هویت نشده به مرحله صدور خواهد رسید.

از لحاظ بحث کارایی سیسـتم ، Standalone CA ها با قابلیت صـدور خودکار Certificate سریعتر از Enterprise CA ها عمل می کنند. اما به این موضوع هم توجه کنید که در محیط های سازمانی بسیار بزرگ وجود چنین CA ای باعث بالا رفتن بار کاری مدیر CA خواهد شد ، زیرا هر روز بـایست بصورت دستی تک تک درخواست ها را بررسـی و در صورت نیاز تاییـد کنـد. به همین دلیل است که از Standalone CA ها معمولا در محیط های شـبکه های Extranet و یا اینترنت اسـتفاده می شود. در واقع شما زمانی از Standalone CA ها استفاده می کنید که تعداد کاربران شـما محدود است و از لحاظی درخواستی که برای صدور Certificate به CA ارسال می شود لزوما نبایستی دارای یک اکانت کاربری وینـدوزی باشد. علاوه بر این شـما زمانی از Standalone Ca ها اسـتفاده می کنید که از یک Directory Service از نوع Third-Party اسـتفاده می کنیـد و یـا ساختار اکتیودایرکتوری وجود نـدارد که بخواهیـد با آن یکپارچه شویـد. نکته قابل توجه در این است که شـما در طراحی ساختار PKI خود می توانید از ترکیبی از Enterprise CA ها و Standalone CA ها استفاده کنید.

جدول یک : مقایسه امکانات Enterprise CA ها و Standalone CA ها

نوع امکان	Enterprise CA	Standalone CA
انتشار Certificate ها در اکتیودایرکتوری و استفاده از اکتیودایرکتوری برای اعتبارسنجی درخواست های Certificate	X	
آفلاین کردن CA		X
امکان صدور خودکار Certificate ها	X	
امکان تایید دستی Certificate ها توسط مدیر		X
امکان استفاده از Certificate Template ها	X	
احراز هویت درخواست ها با استفاده از اکتیودایرکتوری	X	

جدول یک : مقایسه امکانات Enterprise CA ها و Standalone CA ها

معمولا شما زمانی از یک Standalone CA استفاده می کنید که یکی از موارد زیر وجود داشته باشد :

- CA مورد نظر یک Offline CA است که در سطح Root و یا Intermediate مشغول به فعالیت است .
- استفاده از Template های درخواستی برای Certificate ها نیاز نیست.
- یک فرآیند امنیتی قوی برای تاییدیه Certificate ها لازم است.
- تعداد Certificate هایی که صادر می شوند محدود است و فرآیند صدور Certificate بصورت دستی قابل پذیرش است.
- کاربرهای درخواست کننده Certificate نمی توانند از وجود اکتیودایرکتوری استفاده کنند و یا نیازی ندارند.
- قصد صدور Certificate برای Router ها با استفاده از NDES SCEP را دارید.

معمولا شما زمانی از یک Enterprise CA استفاده می کنید که یکی از موارد زیر وجود داشته باشد :

- تعداد زیادی Certificate بایستی بصورت خودکار تایید و صادر شوند.
- دسترسی پذیری و خطاپذیری یک اجبار است.
- مشتریان می خواهند از مزایای یکپارچگی با اکتیودایرکتوری بهره مند شوند.
- امکاناتی نظیر Auto enrollment و Certificate Template های قابل تغییر مورد نیاز است .

- آرشیو سازی کلید ها و بازیابی آنها برای برون سپاری مورد نیاز است.

CA های ریشه یا Root CA

Root CA در واقع CA ای است که در بالاترین سطح از سلسله مراتب ساختار PKI قرار گرفته است ، تمامی Client ها و سازمان بایستی بدون قید و شرط به این CA اعتماد کنند. تمامی زنجیره هایی که دز ساختار PKI وجود دارند در نهایت به Root CA ختم می شوند. بدون توجه به اینکه شما از Enterprise CA یا Standalone CA استفاده می کنید ، شما در نهایت بایستی یک Root CA داشته باشید.

با توجه به اینکه در این سلسله مراتب مرجعه بالاتری برای دریافت Certificate وجود ندارد ، Root CA برای خود نیز Certificate صادر می کنید که در اطلاح به آن Self-Signed Certificate گفته می شود. خوب پس تا همینجا نتیجه می گیریم که در هر جایی که ما یک Self-Signed Certificate مشاهده کردیم ، آن CA در واقع یک Root CA می باشد. تصمیم گیری در خصوص اینکه یک CA به عنوان Trusted Root CA فعالیت کند می تواند هم در سطوح بالای سازمانی اتخاذ شود و یا در همان قسمت فناوری اطلاعات سازمان تصمیم گیری شود.

Root CA به عنوان پایه و بنیاد اصلی مدل اعتماد یا Trust Model ای است که شما در سلسله مراتب CA خود استفاده می کنید. این CA در واقع شما را از صحت وجود اطلاعاتی که در یک Certificate وجود دارد مطمئن می کند. CA های مختلف می توانند با استاندارد های مختلفی این ارتباط را برقرار کنند ، بنابراین قبل از پیاده سازی ساختار و مدل اعتماد برای تایید کلید های عمومی حتما خط مشی ها و دستورالعمل های مربوط به Root CA را به درستی تدوین کنید.

Root CA مهمترین رکن و قسمت در سلسله مراتب CA می باشد. اگر Root CA شما دچار مشکل و اختلال شود ، تمامی CA هایی که در این سلسله مراتب قرار گرفته اند نیز دچار اختلال و مشکل خواهند شد. شما می توانید با قطع کردن ارتباط Root CA با شبکه و استفاده از CA های Subordinate یا میانی برای صدور Certificate ها ، امنیت این ساختار را تا حدود زیادی بالا ببرید.

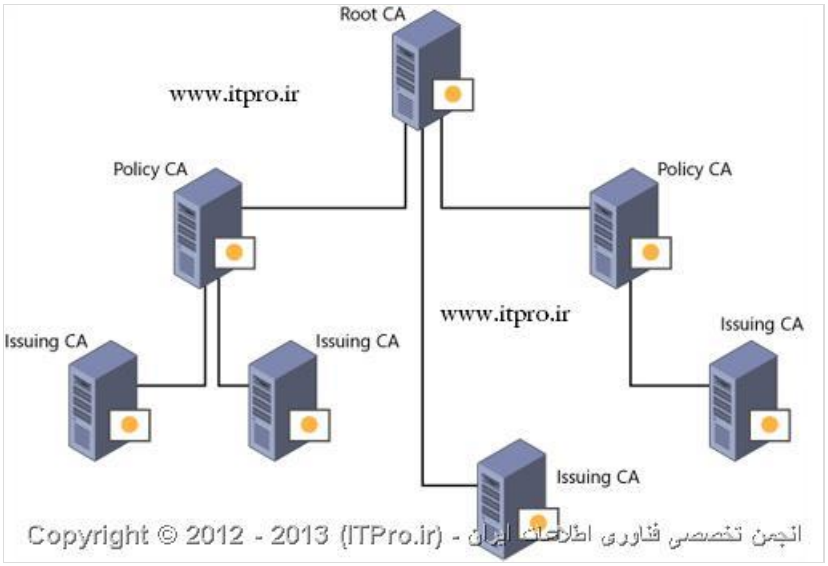
CA های وابسته یا Subordinate CA

CA هایی که به عنوان Root CA در ساختار قرار نمی گیرند به عنوان Subordinate CA یا CA های وابسته معرفی می شوند. اولین Subordinate CA ای که در ساختار شروع به کار کند ، Certificate خود را از Root CA دریافت می کند . اولین Subordinate CA می تواند از این کلید دریافت شده برای صدور Certificate های برای اطمینان از صحت سایر Subordinate CA ها استفاده کند. این Subordinate هایی که در بالاترین سطح قبل از Root CA قرار می گیرند به عنوان Intermediate CA یا CA های سطح میانی نیز شناخته می شوند. یک Intermediate CA برای Root CA به عنوان Subordinate CA شناخته می شود اما برای سایر CA هایی که در سلسله مراتب قرار دارند به عنوان CA مرجع شناخته می شود.

به Intermediate CA ها به عنوان Policy CA نیز اطلاق می شود ، این نامگذاری به این دلیل است که این CA می تواند به عنوان جدا کننده کلاس های Certificate که به وسیله Policy ها انجام می شود مورد استفاده قرار می گیرد. برای مثال ، تفکیکی Policy های یا Policy Separation شامل سطح اطمینانی است که CA ها برای شناسایی کاربرانی که در مناطق جغرافیایی مختلف از سرویس مورد نظر استفاده می کنند . یک Policy CA می تواند هم آنلاین باشد و هم آفلاین باشد. بسیاری از سازمان ها از یک Root CA و دو عدد Policy CA استفاده می کنند ، یکی برای پشتیبانی از کاربران داخلی و یکی دیگر برای پشتیبانی از کاربرانی که در بیرون از سازمان هستند.

سطح بعدی در ساختار سلسله مراتبی CA معمولا شامل Issuing CA ها یا CA های صادر کننده Certificate می باشد. Issuing CA ها برای Computer ها و User ها Certificate صادر می کنند و همیشه در حالت آنلاین قرار دارند. در بسیاری از ساختار های سلسله مراتبی CA پایین ترین سطح Subordinate CA ها با RA ها که مراکز ثبت نام هستند جایگزین می شوند ، RA ها می توانند در نقش واسط CA ها برای احراز هویت شناسه User ای که درخواست Certificate داده است ، ثبت درخواست های ابطال Certificate و انجام عملیات بازیابی

کلید یا Key Recovery مورد استفاده قرار بگیرند. برخلاف CA ها RA ها Certificate صادر نمی کنند و همچنین CRL تولید نمی کنند ، بلکه کلیه فعالیت هایی که انجام می دهند را از طریق CA ای که تحت امر آن هستند انجام می دهند . ساختار سلسله مراتبی CA مشابه شکل شماره یک شامل Policy CA ، Root CA و Issuing CA ها می باشد.



شکل شماره یک : ساختار سلسله مراتبی PKI و CA

استفاده از CA ها آفلاین

برقراری امنیت برای ساختار PKI یکی از مهمترین مسائل موجود است . اگر یک مهاجم بتواند به CA شما دسترسی پیدا کند ، حال چه بصورت فیزیک و یا بصورت شبکه ای ، می تواند کلید خصوصی CA را دریافت کرده و با استفاده از آن به اطلاعات حساسی در شبکه شما دسترسی پیدا کند. به خطر افتادن کلید یک CA در ساختار اعتبار و امنیت همان CA و تمامی CA هایی که در زیرمجموعه آن قرار می گیرند را زیر سئوال می برد . به همین دلیل شما نبایستی Root CA ها را بصورت مستقیم به شبکه سازمان خود متصل کنید. برای اطمینان از قابل اعتماد بودن زیرساختار CA شما بایستی تمامی CA هایی که در نقش صادر کننده Certificate یا Issuing CA هستند را از قبیل Root CA و Intermediate CA ها را از مدار خارج کرده و در حالت آفلاین قرار دهید . با اینکار خطر و ریسک کشف رمز شدن کلید خصوصی CA تا حدود زیادی کم می شود.شما می توانید از روش های زیر CA را به حالت Offline در بیاورید :

- با نصب و راه اندازی Standalone CA در یکی از ویندوز سرورهای ۲۰۰۰ یا ۲۰۰۳ یا ۲۰۰۸ یا ۲۰۱۲
- بوسیله قطع کردن ارتباط فیزیکی سرور با شبکه
- بوسیله خاموش کردن کامپیتور سرور
- بوسیله غیرفعال کردن سرویس CA

مطمئن شوید که CA در حالت آفلاین در محلی امن و با حداقل دسترسی های مجاز نگهداری شود. توجه کنید که حتما Root CA ای که بصورت آفلاین ایجاد می کنید را در حالت Standalone و در یک شبکه Workgroup ایجاد کنید . ایجاد و راه اندازی Root CA در سروری که در عضویت دامین می باشد بعد از مدتی که شما CA را از شبکه قطع می کنید برای برقراری ارتباط مجدد بین CA و اکتیودایرکتوری به دلیل از بین رفتن Secure Channel موجود در این میان ، برای CA مشکل ایجاد خواهد کرد. این مشکل به این دلیل است که رمز عبور حساب کامپیوتر یا Computer Account موجود در اکتیودایرکتوری هر ۳۰ روز یکبار بایستی تعویض شود. به همین دلیل شما می توانید با

عضویت سرور در یک Workgroup و آفلاین کردن آن از بروز چنین مشکلاتی جلوگیری کنید.نصب Root CA به شکل Enterprise Root CA به دلیل آفلاین شدن CA ممکن است مشـکلاتی را برای بروز کردن اکتیودایرکتوری در هنگـام آفلاین بودن CA ایجاد کند . بنابراین در هنگام ایجاد Root CA از مدل Enterprise استفاده نکنید.

زمانیکه قرار است یک CA به عنوان Offline CA در نظر گرفته شود ، شـما همچنان قادر خواهید بود که Certificate ها و CRL های آن را در درون اکتیودایرکتوری منتشر کنید. شما بایستی Offline CA را هر چنـد وقت یکبار به حالت آنلاین در بیاورید که بتواند اطلاعات مربوط به CRL ها و تولید CRL جدید را بروز رسانی کند که این مورد معمولا بصورت برنامه ریزی شده برای Root CA انجام می شود. همچنین دلیل دیگری که شما بایستی در وهله های زمانی معین Root CA را به حالت آنلاین در بیاورید ، صدور Certificate برای Subordinate CA ها می باشد. به دلیل اینکه Offline CA ها معمولا حجم و تعداد کمی درخواست برای صدور Certificate در وهله های زمانی مختلف دارند ، هزینه نگهداری و مدیریت Offline CA ها به مراتب پایینتر از CA های دیگر می باشد.

تعیین تعداد CA های مورد نیاز در ساختار PKI

بعد از اینکه شما نیازهای کاربری و همچنین نرم افزارهای مرتبط با PKI را مشخص کردید ، می توانید به بررسی تعداد CA های مورد نیاز در ساختار PKI بپردازید.اگر سازمان شما به تعداد محدودی Certificate نیاز دارد و نیاز اساسی به این ساختار احساس نمی شود ، شما می توانید از تنها یک CA در ساختار اسـتفاده کنید که همه نقش ها را بر عهده خواهد داشت. با استفاده از تنها یک CA شما می توانید ضمن اسـتفاده از تمـامی مواردی که از ترکیب هـای مختلف CA برداشت می شـود ، از Certificate Template ها نیز اسـتفاده کنید. بهرحال اگر دسترسـی پذیری و فعالیت های توزیع شده مربوط به Certificate Services برای شـما دارای اهمین است ، شما بایستی از چندین CA در ساختار PKI اسـتفاده کنید.شـما همچنین زمانی می توانیـد از ترکیب چندین CA اسـتفاده کنیـد که می خواهیـد وظایف مربوط به صدور Certificate و اهداف دیگر را در سـرورها بصورت تفکیک شده استفاده کنید. برای تعیین تعداد CAهای مورد نیاز بایست به سئوالات زیر به ترتیب پاسخ دهید :

- **آیا شما فقط یک CA نیاز دارید ؟** اگر استفاده از Certificate در سازمان شـما صرفا برای تعداد محدود و یا حتی فقط یک نرم افزار است و در یک محل محدود مورد اسـتفاده قرار می گیرد و ۱۰۰ توانایی های مورد نظر از یک ساختار PKI ایده آل مد نظر شما نیست و همچنین دسترسی پذیری CA یک امر حیاتی به حساب نمی آید ، شـما می توانید فقط از یک سرور به عنوان CA استفاده کنید. در غیر اینصورت شما حتما و حداقل به یک Root CA و چندین Subordinate CA نیاز خواهید داشت.

- **اگر شما به بیش از یک عدد CA نیاز دارید به چه تعداد Root CA نیاز دارید ؟** معمولا و بر حسب پیشنهاد شما یک عدد Root CA دارید که به عنوان نقطه اصلی اعتماد یا Single Point Of Trust معرفی می شود. این بیشتر به این دلیل است که نگهداری و محافظت از Root CA ها در برابر سوء اسـتفاده ها و مشـکلات هزینه زیادی در بر دارد. استفاد از چندین سرور به عنوان Root CA دردسرهای نگهداری از آنها را به یکباره چندین برابر می کند.بهرحال سازمان هایی که از ساختارهای مدیریت توزیع شده استفاده می کنند و دارای قسـمت های تجاری مجزایی می باشند به بیشتر از یک CA ریشه نیاز خواهند داشت و دردسرهای آن را هم قبول می کنند.

- **به چه تعداد Intermediate CA و Policy CA نیاز داریم ؟**
- **به چه تعداد Issuing CA و RA نیاز داریم ؟**

تعیین تعداد Intermediate CA ها و Issuing CA هایی که برای ساختار PKI شما لازم است بسته به فاکتورهای زیر است :

- همانطور که در مقاله اول عنوان کردیم Certificate ها برای اهداف مختلفی از جمله امنیت در ایمیل ، احراز هویت در شبکه و موارد مشابهی از اینگونه استفاده می شوند ، هر کدام از این Certificate ها دارای قالب و Template مخصوص به خود هستند که بسته به نوع استفاده شما از Certificate های صادر شده استفاده از CA های جداگانه برای هر یک از سرویس های ذکر شده مدیریت هر یک از این موارد را که تفکیک می شوند بسیار ساده تر خواهد کرد.

- تقسیم بندی های سازمانی و جغرافیایی می توانند در طراحی ساختار CA شما تاثیرگذار باشند ، شما برای سازمان ها و تقسیم بندی های سازمانی که در محل های فیزیکی دور از هم قرار گرفته اند ، ممکن است بخواهید خط مشی های خاص خود را طراحی کنید ، با استفاده از Subordinate CA های تفکیک شده به لحاظ سازمانی و جغرافیایی مدیریت Policy ها نیز براحتی تفکیک خواهد شد.

- توزیع بار کاری ایجاد و صدور Certificate ها یکی از معیارهایی است که بایستی در نظر گرفته شود ، شما می توانید چندین Issuing CA در طراحی خود در نظر بگیرید به گونه ای که بار کاری صدور Certificate ها برای سایت ها و شبکه و سرورها بین آنها تقسیم شود و سرویس دهی بهتری داشته باشید.برای مثال ، اگر پهنای باند بین سایت های فیزیکی شما کم است شما می توانید یک Issuing CA در هر یک از سایت های خود قرار دهید تا کارایی و استفاده بهینه از Certificate Services در هر سایت انجام شود.

- انعطاف پذیری تنظیمات نیز یکی دیگر از موارد مهم در تعیین تعداد CA های میانی می باشد. شما می توانید تناسب بین CA ها در خصوص پارامترهای محیطی مثل طول کلید ، حفاظت فیزیکی ، حفاظت در مقابل حملات شبکه ای و ... را با استفاده از ایجاد تعادل بین امنیت و قابلیت استفاده از آن CA ایجاد کنید. برای مثال شما می توانید کلیدها و Certificate های مربوط به CA های میانی و issuing CA هایی که دارای درجه ریسک بالایی هستند را در وهله های زمانی سریعتر و بدون از بین رفتن Trust Relationship بین CA ها و Root CA جدید سازی کنید.

- بدون شک استفاده از سرویس های جایگزین برای Certificate Services نیز یک ملاک اصلی به حسای می آید. اگر یک Enterprise CA دچار مشکل شود ، سرویس جایگزین یا بهتر بگوییم سرور جایگزین می تواند سرویس های دچار مشکل شده را پشتیبانی کرده و سرویس را از دسترسی پذیری بالایی برخوردار کند.

سعی کنید همیشه در طراحی های سازمانی از تعداد معقولی و با توجه به نیازهای سازمانی خود ، CA و RA بکار ببرید. اگر سازمان کوچکی دارید و می دانید که بار کاری CAها صرفا بر عهده یک نفر خواهد بود از طراحی و پیاده سازی ساختار های پیچیده و گسترده خودداری کنید زیرا در نهایت به ضرر شما تمام خواهد شد و دردسرهای مدیریتی آن بر عهده خودتان می افتد. فراموش نکنید که اضافه شدن CA های زیاد با اینکه کارایی را افزایش می دهد اما از جهتی مدیریت سخت تر و نقاط ضعف امنیتی سیستم را نیز بیشتر خواهد کرد.
ورزشکار باشید

نویسنده : محمد نصیری
منبع : جزیره امنیت اطلاعات و ارتباطات وب سایت توسینسو

#CA__میانی #کاربردهای_PKI #طراحی_PKI #مرکز_صدور_گواهینامه #مقایسه_Enterprise_و_Standalone_CA_ها
#معماری_PKI #طراحی_ساختار_CA #PKI_ریشه

varzdar

با تشکر از زحمات شما مقاله خوبی بود.

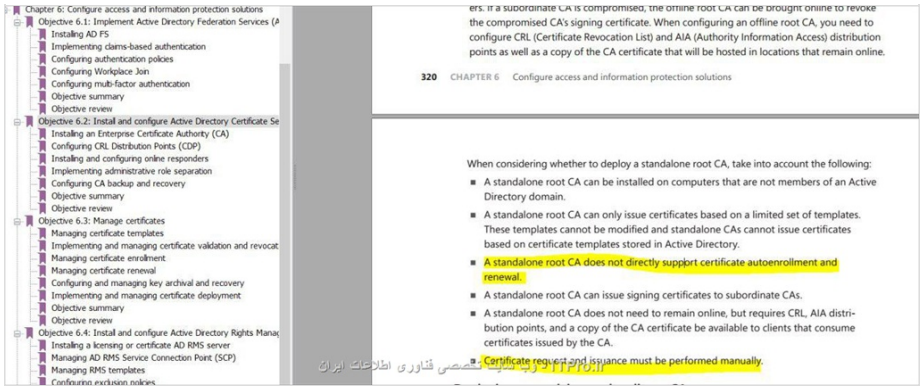
a.Jahanshahlo

عالی بود ممنون.

آزاده

سلام و وقتتون بخیر

در این مقاله نوشته شده "بصورت پیشفرض تمامی درخواست های Certificate ای که برای CA ارسال می شوند در صف pending در CA باقی می مانند تا مدیر CA آنها را تایید کند.شما می توانید Standalone CA ها را به گونه ای طراحی کنید که به درخواست های رسیده برای دریـافت Certificate را بصـورت خودکـار پاسـخ داده و Certificate را صـادر کننـد ، امـا اینکـار پیشـنهاد نمی شود" اما در رفرنس مایکروسافت این طور عنوان شده



یعنی جمله اول این نوشته رو تایید اما جمله دوم نقص می کنه و میگه درخواست و صدور گواهینامه در مد Standalone فقط به صورت دستی امکانپذیره

ممنون میشم کمی در این مورد توضیح بدید

تشکر

محمد نصیری

خانم آزاده ، این مقاله فقط مایکروسافتی نیست ، محدودیت های CA مایکروسافت داخلش لحاظ نشده.

آزاده

درسته ، به این نکته دقت نکرده بودم ، مچکرم

مطلب اصلی