پروپوزال راه اندازی CA Server

در رمزنگاری به مرجع صدور گواهی دیجیتال (certificate authority) یا (certification authority) که به‌صورت خلاصه به آن CA Server می‌گویند، یک شخص حقیقی یا حقوقی است که گواهی‌های دیجیتال (گواهی‌های کلید عمومی) را صادر می‌کند. گواهی دیجیتال تضمین می‌کند که موضوع گواهی مورد نظر ما به اسم همان صاحبی است که در آن گفته شده است. این گواهی به دیگران (کسانی که بر اساس این گواهی کار خود را انجام می‌دهند) اجازه می‌دهد که به امضاها و بیانیه‌هایی که با کلید خصوصی گواهی یاد شده تولید شده‌اند، اطمینان کنند. در مدل ارتباط با اعتماد، مرجع صدور گواهی دیجیتال یا همان CA Server شخص ثالث مورد اطمینانی است که از سوی هر دو سمت گواهی یعنی صاحب گواهی و شخص اعتماد کننده به گواهی معتمد به حساب می‌آید.
یک مرجع صدور گواهی دیجیتال، گواهی‌های دیجیتالی صادر می‌کند که شامل یک کلید عمومی و هویت صاحب آن است. کلید خصوصی متناظر به این سادگی در اختیار همه گذاشته نمی‌شود و توسط کاربر مقابل که کلید برای آن تولید شده است، مخفی می‌ماند. گواهی نیز به نوبه خود، تأیید یا اعتباری است از سوی مرجع صدور گواهی دیجیتال، به‌طوری که بیان می‌دارد کلید عمومی ذکر شده در گواهی متعلق به شخص، ارگان، سرویس‌دهنده یا هویتی که در گواهی به آن اشاره شده است. تعهد یک مرجع صدور گواهی دیجیتال برای طرح بیان شده در بالا، تضمین و مهر تأئیدی است برای استفاده کننده‌کنندگان از گواهی، به‌طوری که کاربران و شخصیت‌هایی که بر اساس گواهی کار می‌کنند بتوانند به اطلاعات منتقل شده بر اساس گواهی مذکور اعتماد کنند. مراجع صدور گواهی دیجیتال از استانداردها و آزمون‌های بسیاری برای منظور فوق استفاده می‌کنند. اصولاً مرجع صدور گواهی دیجیتال مسئول جمله زیر است: «بله، این شخص همان کسی است که ادعا می‌کند و ما به عنوان مرجع صدور گواهی دیجیتال، آن را تائید می‌کنیم».

اگر کاربر به مرجع صدور گواهی دیجیتال اطمینان دارد و تشخیص می‌دهد که امضای دیجیتالی مرجع صدور گواهی دیجیتال درست است، می‌تواند مطمئن باشد که کلید عمومی حقیقتاً متعلق به هویتی است که گواهی برای آن صادر شده است. مثال:
رمزگزاری با کلید عمومی را می‌توان برای رمز کردن ارتباط بین دو قسمت مورد استفاده قرار داد. این رخداد معمولاً زمانی که مثلا یک کاربر به یک سایت وارد می‌شود و می‌خواهد که پروتکل HTTP را به صورت امن اجرا کند. در این مثال فرض می‌کنیم که کاربر در صفحه خانگی بانک خود با آدرس www.bank.example وارد می‌شود تا خدمات بانکی آنلاین انجام دهد. وقتی که کاربر صفحه خانگی www.bank.example را باز می‌کند، یک کلید عمومی را همراه با تمام اطلاعاتی که صفحه مرورگر سایت نمایش می‌دهد دریافت می‌کند. زمانی که کاربر اطلاعاتی را در صفحه بانک وارد و تائید می‌کند (یعنی اطلاعاتی را به بانک برمی‌گرداند)، اطلاعات پیش از فرستاده شدن به‌وسیله مرورگر سایت و با استفاده از کلید عمومی که توسط www.bank.example ارائه شده رمزنگاری می‌شوند. کلیدی که به‌وسیله آن اطلاعات را می‌توان از حالت رمزنگاری خارج کرد، کلید خصوصی می‌گویند و تنها برای بانک شناخته شده است. در نتیجه حتی اگر کسی بتواند به داده‌هایی که رد و بدل شده‌اند دسترسی پیدا کند، تنها توسط بانک و با استفاده از کلید خصوصی قابل رمزگشایی هستند.
این مکانیزم تنها زمانی قابل اعتماد است که کاربر مطمئن باشد کسی که با او در ارتباط است بانک است. اگر کاربر آدرس www.bank.example را وارد کند ولی ارتباطش با بانک ربوده شده و یک سایت تقلبی (که سعی می‌کند خود را بانک نشان دهد) اطلاعات صفحه بانک را به مرورگر کاربر بفرستد، هم‌زمان با صفحه تقلبی یک کلید عمومی تقلبی نیز به کاربر می‌فرستد. کاربر فرم را با اطلاعات شخصی‌اش پر می‌کند و با تائید آن، داده‌ها با کلید عمومی تقلبی رمزی می‌شوند. صفحه تقلبی به اطلاعات کاربر دست پیدا می‌کند زیرا صفحه تقلبی دارای کلید خصوصی تقلبی متناظر با کلید عمومی است.

CA Server مرجع صدور گواهی دیجیتال یک سازمان است که کلیدهای عمومی، صاحب آن‌ها و هر طرفی که در ارتباط با اعتماد بااین سازمان است را نگهداری می‌کند. زمانی که مرورگر تارنمای کاربر کلید عمومی را از تارنمای www.bank.example دریافت می‌کند، می‌تواند با مرجع صدور گواهی دیجیتال تماس بگیرد تا مطمئن شود که آیا حقیقتاً کلید عمومی متعلق به www.bank.example است یا خیر. از آن‌جا که www.bank.exampleاز یک کلید عمومی که مرجع صدور گواهی دیجیتال آن را تائید کرده استفاده می‌کند، یک www.bank.example تقلبی تنها می‌تواند از همان کلید عمومی اصلی استفاده کند و از آنجا که www.bank.example تقلبی کلید خصوصی متناظر را در اختیار ندارد، داده‌های کاربر را نمی‌تواند رمزگشایی کند.

ابطال مرجع صدور گواهی دیجیتال

اگر یک CA Server خراب شود، آن‌گاه امنیت کل سیستم برای هر کاربری که مرجع مذکور به سلامت ارتباطش توسط صاحب گواهی دیجیتال و کلید عمومی تضمین داده است زیر سؤال می‌رود.
یکی از مهمترین قسمت های پیاده سازی CA SERVER، تصمیم‌گیری درباره ساختار آن است که به چه صورت سرویس نصب و پیکربندی شود:
Stand-alone CA: یک سرور CA که ضرورتا نیازی به اتصال و integrate شدن با AD DS را ندارد. یک stand-alone CA در واقع سروری‌ست که یا روی کامپیوتری که عضو دامین است، نصب می شود و یا سروری که در محیط workgroup حضور دارد. Stand-alone CA ها گاها به عنوان root CA داخلی استفاده شده و معمولا بعد از اینکه Certificate ها را برای سرورهای پایین دستی خود (subordinate) صادر کرد، به دلایل امنیتی آفلاین می‌شود. در این نوع CA، در واقع Certificate ها بصورت دستی (manual) صادر و اعمال شده و بر پایه یک سری نمونه‌های استاندارد هستند که نمی‌توانید آنها را تغییر دهید.
Enterprise CA: این CA سروری‌ست که با سرویس AD DS درگیر بوده و integrate شده است. Enterprise CAها معمولا عضو دامین بوده و گاها برای صدور Certificate به کاربران و کلاینت‌ها استفاده می‌شود. CA هایی که مسئول صدور Certificate هستند، معمولا همیشه آنلاین بوده و دردسترس هستند. (high available) از آنجایی که این سرورها با AD DS ادغام و integrate شده‌اند، هنگامی‌که اعضای دامین درخواست Certificate بدهند، بطور خودکارcertificate ها را صادر و اعمال می‌کنند. Certificateهایی که بصورت نمونه هستند نیز بسیار پیشرفته‌تر بوده و می‌توانید با توجه به نیازهای خود ویرایش کنید. تمامی کلیدهای رمزنگاری با integrate شدن با دایرکتوری محافظت می‌شوند.

پیشنهاد :

پیشنهاد می‌شود به اجرای یک CA سرور در محل هسته شبکه مجموعه و اجرای یک CA سرور ثانویه به صورت subordinate در محل DMZ مجموعه جهت ارائه سرویس به سیستم های داخل مجموعه و خارج از مجموعه (اعمال محدودیت دسترسی به سرور اصلی جهت افزایش امنیت).