مروری بر امضای دیجیتالی

الگوریتم کلید عمومی

کلید عمومی یا رمز گذاری نامتقارن از دو کلید متفاوت که به طور ریاضی به هم وابسته هستند استفاده می کنند . اگر چه تفاوتهایی در عملکرد آنها وجود دارد آنها را می توان به دو روش معمول برای رمز گذاری و امضای دیجیتالی تقسیم نمود.

رمز گذاری

RSA

منحنی بیضوی یا (ECDH) Diffic-Hellman (DH)

امضای دیجیتالی

RSA

الگوریتم امضای دیجیتالی و یا منحنی بیضوی DSA (ECDSA) الگوریتم کلید عمومی داخل سیستم وارد و با الگوریتم سریعتری ترکیب می شود که سیستم را قادر به استفاده از مقادیر زیاد دیتا می کند . ابتدا در خصوص رمز نگاری و سپس امضاء دیجیتالی بحث خواهیم نمود.

رمز نگاری

رمز نگاری جنبه محرمانگی را ایجاد می کند . اینکار از طریق جلو گیری از فهمیدن دیتا توسط هرفردی بجز یک دریافت کننده معین انجام می گیرد. رمز نگاری فرمی از کنترل دسترسی است که با استفاده از خاصیت اختصاصی مدیریت کلید صورت می گیرد. فقط دریافت کننده کلید لازم را برای بازگشایی رمز دیتا داشته و می تواند به آن دسترسی پیدا کند.

دو روش عمومی در فناوری کلید عمومی برای پشتیبانی رمزنگاری دیتا استفاده می شود، RSA و Diffie-Hellman .لفظ پشتیبانی ازاین جهت بکار برده شد ه که الگوریتم کلید عمومی در محاسبه برای استفاده از رمز نگاری کردن دیتا بسیار گران است . اینست که استفاده از (رمز گذاری کلید عمومی) برای رمز نگاری اتلاف وقت بوده و در اجرا مشکلاتی خواهد داشت .

بنا بر این به جای رمز نمودن دیتابه طور مستقیم الگوریتم کلید عمومی با یک الگوریتم متقارن کلید برای محافظت دیتا بکار می رود.

RSA

RSA بر اساس نام Adi shamir ,Ronald Rivet و Leonard Adlman نامیده شده که توسعه دهندگان الگوریتم می باشند.که شناخته ترینشان الگوریتم کلید عمومی است .

هنگامی که مردم درباره رمز نگاری کلید عمومی سؤال می کنند در واقع در مورد عملکرد RSA توضیح می خواهند . کیفیت RSA برگشت پذیر[1] بودن الگوریتم است.لازم به توضیح است از لحاظ تکنیکی RSA یا هر الگوریتم کلید عمومی برگشت پذیر نیست. الگوریتم کلید عمومی تابع یک سویه است لیکن از آنجایی برگشت پذیر خوانده می شود که دیتای انتقال داده شده می تواند با یک کلید متفاوت دیگری دوباره بدست بیاید .

با RSA می توان با استفاده از کلید خصوصی دیتایی را که قبلاً با کلید عمومی رمز نگاری شده را دوباره بدست آورد . این مفهوم در شکل 4.1 توضیح داده شده است. با RSA کلید عمومی جهت رمز کردن دیتا استفاده می شود و کلید خصوصی جهت بازگشایی رمز دیتا استفاده می شود. از آنجایی که کلید خصوصی هم دارد ، هر کسی می تواند دیتا را برای صاحب کلید رمز نگاری کند اما فقط صاحب کلید می تواند دیتا را بازگشایی رمز نماید.

.

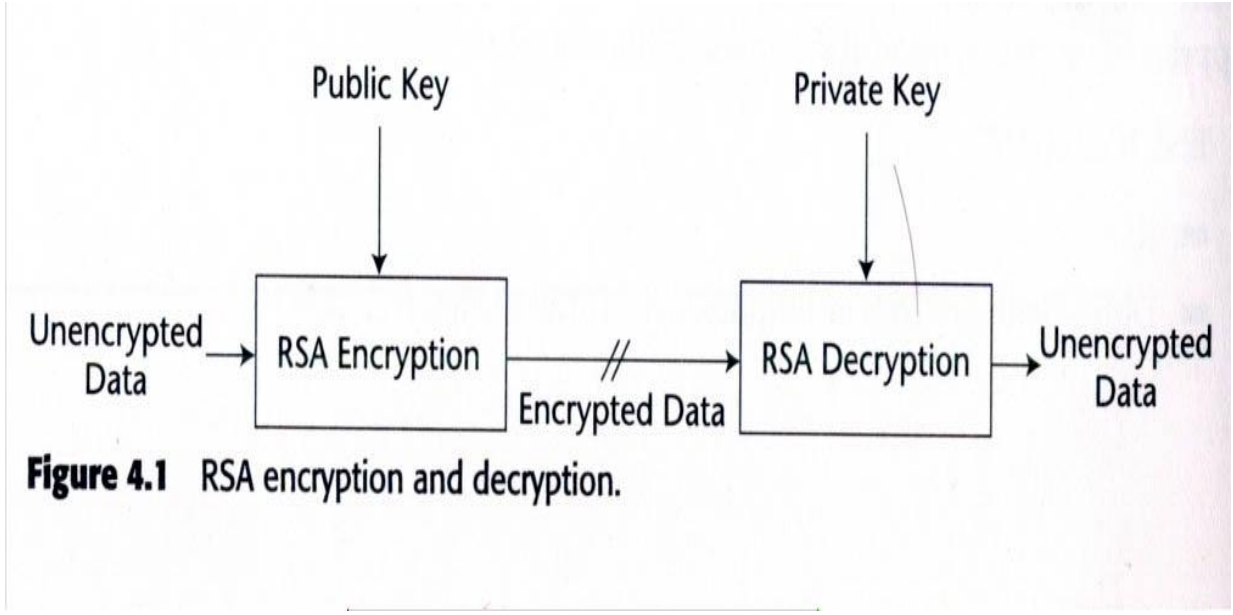
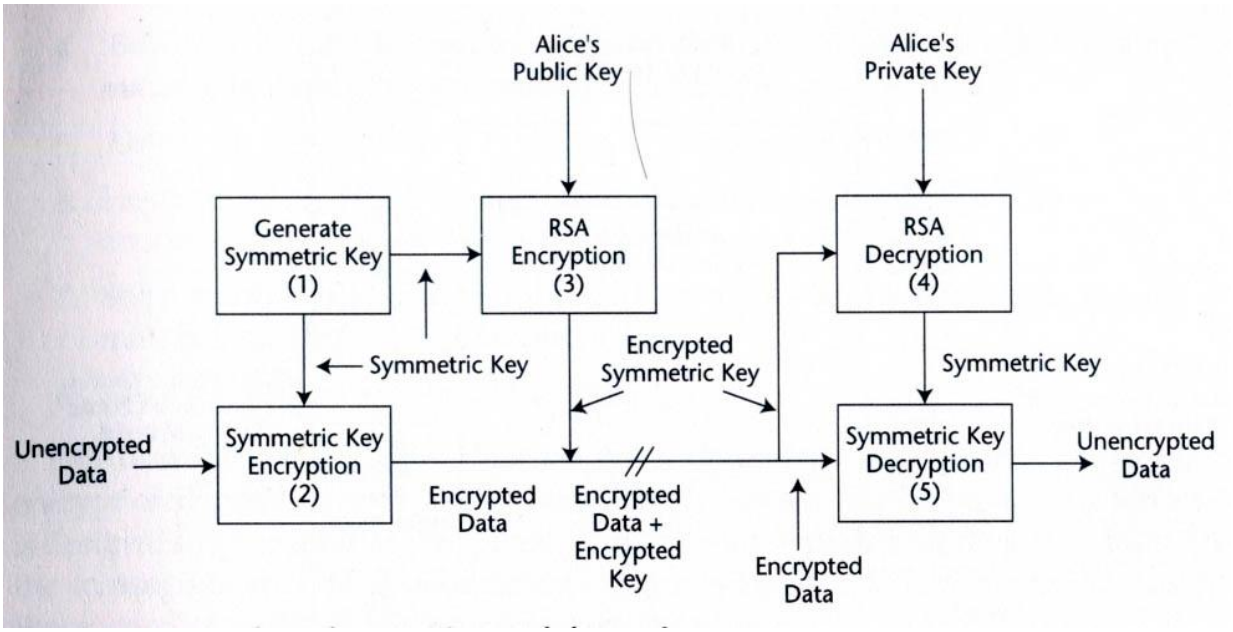


Figure 4.1 RSA encryption and decryption.



[1] Reversible

در اجرا قسمتی از رمز نگاری سیستم با RSA ، برای رمز نگاری نمودن از یک کلید متقارن استفاده می نماید.مثلاً باب می خواهد با روشی اطلاعاتی به آلیس بفرستد که فقط آلیس قادر به فهمیدن آن باشد باب با ابجاد یک کلید متقارن شروع می کند

۱ –او از این کلید جهت رمز نمودن دیتا با یک الگوریتم متقارن مانند DES استفاده می کند

۲ –با استفاده از کلید عمومی آلیس ، او کلید متقارن را رمز نگاری می کند که به پیغام رمز شده ضمیمه می شود. این رمز نگاری مراقبت می کند که فقط آلیس قادر به باز گشایی رمز و استفاده از کلید متقارن باشد.

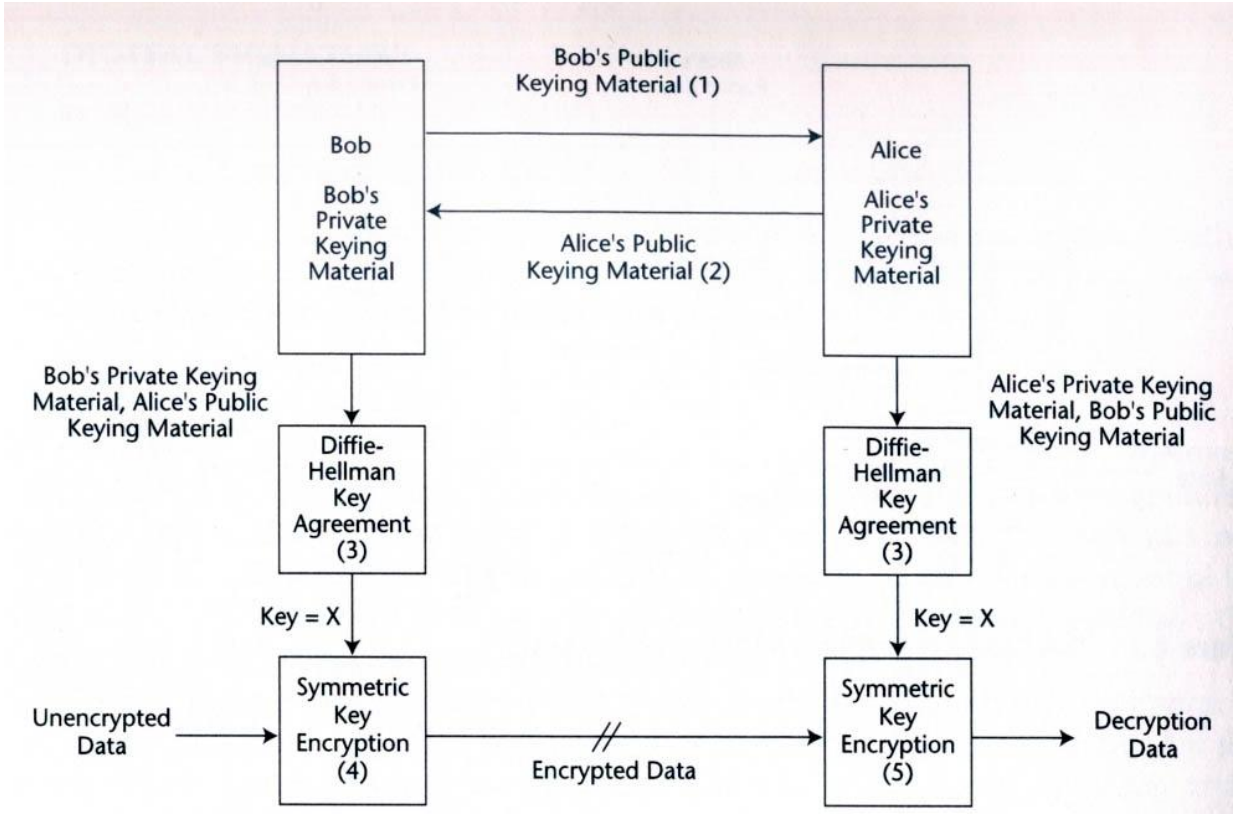
۳ –هنگامی که پیغام می رسد آلیس کلید متقارن رمز شده را از پیغام بیرون آورده و با استفاده از کلید خصوصی خود باز گشایی رمز می نماید.

۴ –با استفاده از کلید متقارن بدست آمده آلیس تمام پیغام را باز گشایی رمز می نماید.

Diffiec- Hellman ,Elliptic Curve Diffic – Hellman

(DH) و منحنی بیضوی (DH) الگوریتم های توافقی کلیدها می باشد .

الگوریتم به افتخار Martin Hellman , Whit fiell Diffie نامگذاری شده که توسعه دهندگان الگوریتم بودند. درکلید توافقی ، دو طرف اطلاعاتی را تبادل می کنند که به آنها اجازه می دهد یک بخش سری ر ا share شده را بدست آورند.



افراد غیر مجاز می توانند اطلاعات تبادل شده را جدا کنند اما آنها قادر به تعیین shard secret نیستند: این shard secret می تواند به عنوان کلید الگوریتم متقارن استفاده شود. فرایند توافقی کلید DH در شکل 4.3 نشان داده شده استدر شکل دو طرف باب و آلیس می خواهند تبادل اطلاعات کنند از رمز نگاری استفاده می کند.

۱) باب به آلیس کلید عمومی اش را می فرستد (این یک کلید نیست در واقع اطلاعاتی است که اجازه می دهد که کلید بدست آید)

۲) آلیس به باب مطالب کلید عمومی خود را می فرستد.

۳) هر کدام با استفاده نمودن از این اطلاعات و الگوریتم DH یک اطلاعات سری مشترک را بدست می آورند.

۴) باب ازاطلاعات سری به عنوان کلیدی برای رمزنمودن دیتا برای ارسال به آلیس با استفاده از یک الگوریتم کلید متقارن استفاده می کند.

۵) آلیس از اطلاعات سری برای رمزگشایی دیتای ارسالی باب استفاده می کند.

شکل 4.4 نشان می دهد که DH چگونه می تواند به عنوان سخت از یک سیستم رمز کننده استفاده شود.تبادل مطالب کلید شده مانند بحث قبلی به هم تأثیر گذار نیستند مطالب کلید شده عمومی می تواند در یک مکان شناخته شده ثبت شود. یک قهرمت می تواند به جای اینکه منتظر باشد که طرف دیگر کی دیتا را می فرستد . به سادگیدیتا را هنگامی که احتیاج دارد بر دارد . مطالب ذیل یک تبادل غیر همزمان را شرح می دهد.

۱_آلیس کلید خود را در یک کتابچه راهنما برای باب می گذارد که هر وقت که خواست برداشت کند.

۲-باب اطلاعات کلید شده عمومی DH آلیس را از کتابچه راهنما برمی دارد.

۳-باب یک ماده کلیدی یکتا برای این بخش تبادل شده بخصوص ایجاد می کند .که این ممکن است از ماده کلیدی که او قبلاً برای خودش در کتابچه راهنما ثبت کرده باشد،مجزا باشد.این از استفاده مجدد یک کلید متقارن یکسان برای تمام ارتباطات بین دو طرف پیشگیری می کند.

۴-باب از ماده کلید خصوصی خود با ماده کلید عمومی ثبت شده آلیس رمز نگاری می کند.

۵-با استفاده از کلید متقارن پیغام را برای آلیس رمز نگاری می کند.

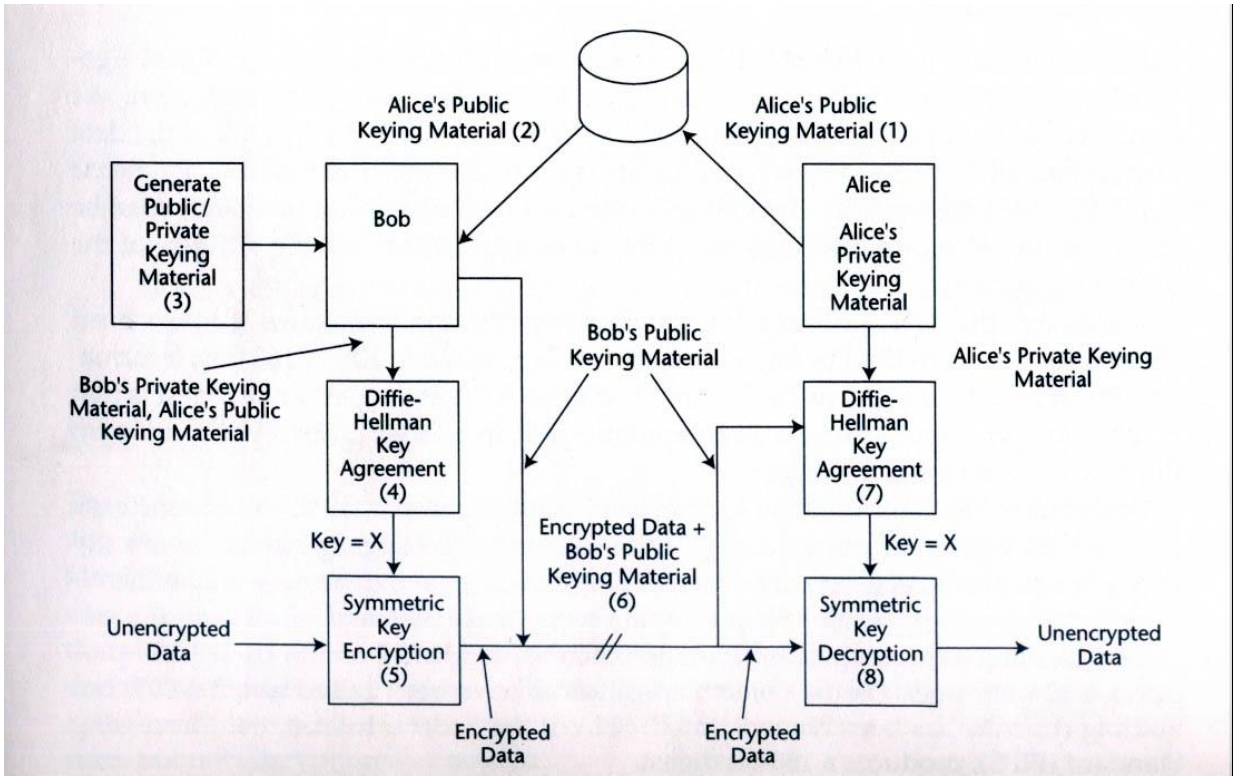
۶-او ماده کلید عمومی خودش را برای تبادل این پیغام به پیغام رمز شده ضمیمه کرده و این ترکیب را برای آلیس ارسال می کند.

۷-آلیس اطلاعات کلید باب را جدا کرده و آن را با کلید خصوصی خود ترکیب نموده وکلید متقارن را بدست می آورد.

۸-او این کلید را برای باز گشایی رمز پیغام بکار می برد.

یک مشکل سیستم Diffiec- Hellman آن است که کلید متقار ن استفاده شده برای رمز نمودن به اطلاعات ارسالی از فرستنده و گیرنده وابسته است . اگر یک پیغام بایستی به چند دریافت کننده ارسال شود، بایستی چند بار رمزنگاری گردد .با RSA پیغام یکبار رمز می شودو فقط کلید متقارن چند بار رمز شده ویکبار برای هر دریافت کننده کلید عمومی بکار می رود.

بحث قبلی از الگوریتم توافقی کلید Diffiec- Hellman استفاده کرده است اگرما از ECDH استفاده کنیم فرایند بسیار ساده تر می گردد. به هر حال در رمز نگاری منحنی بیضوی از نقاط تعریف شده بوسیله یک منحنی بیضوی درمی‌دان محدود ترجیحاً از م دل ورود صحیح برخی اعداد درجه اول مانند آنچه در Diffiec- Hellman بوداستفاده می کنیم.



امضاء دیجیتالی:

از آنجاییکه فقط صاحب کلید ، کلید خصوصی را نگه می دارد تابعی که از کلید خصوصی استفاده می کند برای کار صاحب کلید استفاده می شود نه کس دیگر. این عمل راهی به سوی جهان رمزنگاری به مفهوم امضاء دیجیتالی خواهد بود.

امضاء دیجیتالی بوسیله صاحب کلید خصوصی برای امضاءکردن اطلاعات الکترونیکی برای جلوگیری از جعل کردن بکار می رود. یک طرف صاحب کلیدخصوصی می تواندبا امضاء دیجیتالی به خوبی فرم را تکمیل کند.

امضاءدیجیتالی از امضاء دست خط قوی تر است چرا که امضاء به صورت ریاضی به دیتا نشان(sign) شده گره خورده است.

امضاء دیجیتالی نمی تواند از یک سند بریده شود وبه سند دیگر چسبانده شود.

همچنین هر تغییر دیتای Signed شده امضاء را بی اعتبار می کند. یک امضاء دیجیتالی از دیتای Sing شده و کلید خصوصی امضاء کننده ایجاد می گردد. امضاء به پیغام ضمیمه می گردد. هر فردی که پیغام را دریافت می کند تابع وابسته دیگری و با استفاده از کلید عمومی و یا امضاء و یا دیتای نهاده شده اجرا می کند (که بستگی به الگوریتم دارد). اگر اجرای این تابع نتیجه مورد انتظار را تصدیق کند، امضاء معتبر در نظر گرفته می شود. امضاء دیجیتالی چند سرویس سری (امنیتی) تولید می کند. آنها پیغام را از جهت اینکه فقط توسط صاحب کلید (که صاحب کلید خصوصی می باشد) و می تواند پیغام را امضاء کند، sing شده باشد،اعتبار می بخشند.

یک امضاء دیجیتالی همچنین با چک نمودن صحت پیغام از تغییرات غیرمجاز جلوگیری می کند.

اگر یک امضاء دیجیتالی نتواند به عنوان یک امضاء کننده تائید شود فرض می شود که متن پیغام تغییر کرده است. هنگامی که یک امضاء دیجیتالی به خودی خود برای جلوگیری از تکرار مجدد کافی نباشد ، یک ساختمان دیجیتالی می تواند نقش قسمت کلید برای جلوگیری از تکرار مجدد را بازی می کند.

پیغام Digest

قبل از اینکه در مورد الگوریتم های امضاء دیجیتالی بحث کنیم درخصوص الگوریتمهای پیغام digest (که به عنوان الگوریتمهای hashing نیز نامیده می شوند) بحث می کنیم.

در بحث رمز گشایی توضیح دادیم که چگونه الگوریتمهای متقارن مانند DES به عنوان رمز نگاری کننده دیتا بکار می روند و چگونه الگوریتم های کلید عمومی برای پشتیبانی یا بدست آوردن کلید متقارن استفاده می شود. این عمل سرعت رمز نگاری را به صورت قابل قبول حفظ می کند. یک همسازی مشابه باید برای امضاء دیجیتالی ساخته شود این همسازی شامل ایجاد یک digest از دیتای sing شده می باشد.

یک الگوریتم پیغام digest شده در هر اندازه که ارائه شود ، آن را داخل یک رشته با اندازه ثابت منتقل می کند. از آنجایی که یک میلیون byte و یا اطلاعات بیشتر به ۱۲۸ و یا ۱۶۰ بیت bit کاهش می یابد اطلاعات از دست می رود و انتقال قابل برگشت نیست.

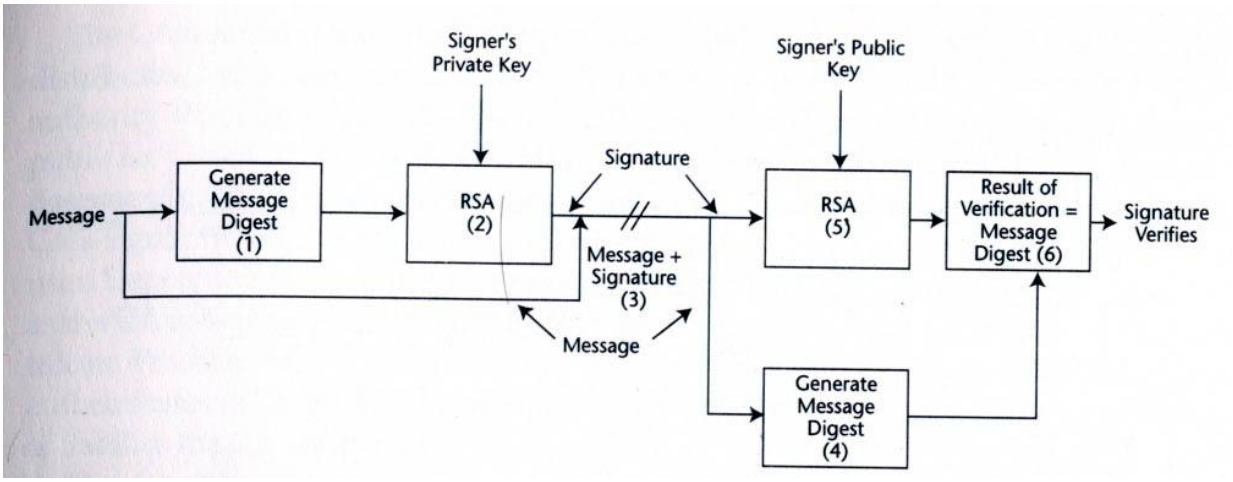
یک خاصیت اصلی digest آن است که یک input string شناخته شده با صدور محاسباتی قادر به کشف یا input string متفاوت با یک digest یکسان نیست.

از آنجایی که الگوریتم های کلید عمومی از نقطه محاسباتی گران هستند، به جای پیغام کامل پیغام digest شده sign می گردد. با الگوریتم digesting مناسب خواص امنیتی پیغام مسئله ای ساختگی نیست.

امضای روی پیغام ، پیغام را تصدیق کرده و اعتبار امضاء تایید می کند که یک پیغام تغییر نیافته است.

عموماً از دو الگوریتم digest کردن پیغام استفاده می شود. MD5 و SH1. MD5 یک Digest ۱۲۸ بیتی را ایجاد می کند برخی از تئوری ها از MD5 برخواسته‌اند اما هیچکدام واقعاً اثبات نشده اند.

SHA1 در استاندارد متحدسازی ،جریان اطلاعات یک digest ۱۶۰ بیتی را تولید می کند.



RSA

دقیقاً همان الگوریتم RSA استفاده شده برای رمز نگاری ، می تواند برای امضاء دیجیتالی استفاده شود.

استفاده از RSA برای امضاء در شکل ۴۰۵ نشان داده شده است.

۱ -ابتدا یک پیغام Digest محاسبه می شود.

۲ -کلید خصوصی برای علامت گذاری پیغام digest شده استفاده می شود.

۳ -امضاء به پیغام پیوست می شود و به دریافت کننده انتقال می یابد.

۴ -دریافت کننده digest پیغام دریافتی را محاسبه می کند.

۵ -سپس لازمه تایید امضاء خارج نمودن امضاء از پیغام و استفاده از RSA روی امضاء با کلید عمومی می باشد .

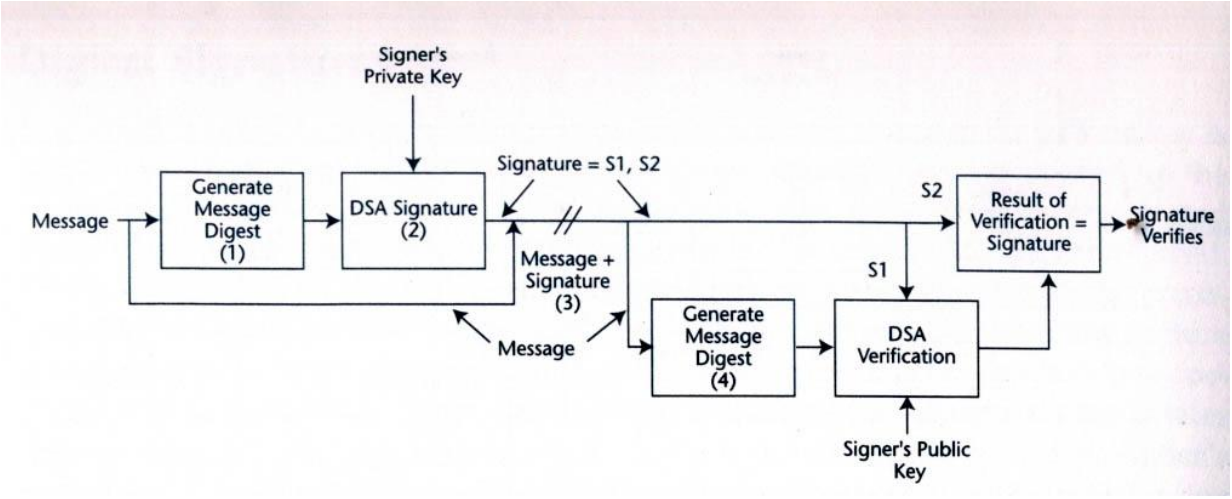
۶ -اگر نتیجه انتقال و digest محاسبه شده جدید برابر باشد، امضاء معتبر است.

DSA

انستیتو ملی استانداردها و تکنولوژی ،الگوریتم امضاء دیجیتالی را توسعه داده است. DSA (Digital signature Algorithm)

دلیل این توسعه ایجاد یک شق دیگر برای RSA است که بتواند برای امضاء استفاده شودو در رمز نگاری استفاده نشود .

دولت U.S در استفاده بی رویه و غیر قابل کنترل ازرمز نگاری متمرکز شده است. موقعیت دولت این بود که رمز نگاری قوی فقط برای استفاده دولت یا دیگر شرکت ها بوده است. استفاده از رمز نگاری بوسیله دیگران توانایی دولت را در استراق سمع بر فعالیت های قانون شکنان در بر خواهد داشت. یک شق دیگر RSA است که می تواند برای امضاء دیجیتالی استفاده شود اما به رمز نگاری شدن نیازی نیست.



الگوریتم DSA این ملزومات را دربردارد. با شکل ۴۰۶ عملکرد آن را به توضیح داده شده است با DSA:

۱ -پیغام باید یک پیغام digest را ایجاد کند.

۲ -پیغام digest علامت زده می شود امضاء به دو قسمت نوشته می شود.

۳ -سپس امضاء و دیگر اطلاعات پشتیبانی کننده به پیغام ضمیمه شده و به سمت دریافت کننده ارسال می گردند.

۴ -دریافت کننده digest پیغام را محاسبه کرده و یک تابع براساس کلید عمومی امضاء کننده، digest و امضاء اجرا می کند. اگر نتیجه این اجرا با قسمت امضاء برابر باشد امضاء معتبر است.

گواهی نامه های کلید عمومی

هنگامی که کلید عمومی می تواند آزادانه منتشر و پخش شده و توسط هر کسی نگهداری شود، هنوز باید برای اجتناب ازاینکه غیرواقعی نمایش داده شود ،امن گردد. برای اینکه سیستم کار کند، استفاده کنندگان کلید عمومی احتیاج دارند که اطمینان حاصل کنند که مالک کلید کیست و آنکه کلید صحیح بوده و تغییر داده نشده باشد. اگر این امکان وجود داشته باشد که کلید عمومی یک نفر با شخص دیگری جایگزین گردد، استفاده کننده کلید می تواند به هدایت شدن جهت انتقال با شخص دیگری بجز کسی که او انتظار دارد، گول زده شود.

در جامعه انسانی ما از روش معرفی نمودن در موقعیت مشابه استفاده می کنیم. کسی که ما می شناسیم و به او اعتماد داریم به ما شخص دیگری را که نمی شناسیم معرفی می نماید. هنگامی که این روش بوسیله شخص واقعی نتواند انجام شود نامه های معرفی می توانند مورد استفاده قرار گیرند . در این روش یک شبکه معتمد ساخته می شود.

در دنیای الکترونیکی گواهی نامه های کلید عمومی نقش نامه های معرفی را بازی می کنند. گواهی نامه ها به عنوان روشی در یک سازمان معتمد شناخته شد ه به عنوان (CA) تصدیق کننده گواهی نامه [۲]، برای معرفی ما به شخص منحصر به فردی توسط ضمانت کردن کلید عمومی آن فرد عمل می کند. گواهی نامه ها این امکان را برای دریافت کننده کلید عمومی فراهم می سازد که با اطمینان کسی که صاحب کلید است را بشناسد و مطمئن شود که کلید تغییر نیافته است. این روشی برای CA است که به یک شخص

[2]Certificate Authority

منحصر به فردی با کلید عمومی اش متصل گردد از جهتی که بدون اینکه کشف آن ممکن باشد تغییراتی را در آن انجام دهد.

CA از یک دیتابیس مرکزی (منطقی) ، برای تمام کلیدهای عمومی ثبت شده نگهداری می‌کند و گواهی نامه های کلید عمومی را توزیع می نماید. هر گواهی نامه لزوماً عبارتی است با تصدیق توضیحات اصول کلید عمومی. CA برای یک کلید عمومی منحصر به فرد با استفاده از کلید خصوصی آن برای علامتگذاری گواهی نامه کلید عمومی، ضمانت می کند که سندی الکترونیکی است شامل نام استفاده کننده و کلید عمومی در کنار دیگر اطلاعات می‌باشد. امضاء CA روی گواهی نامه نشان دهنده اینست که کلید عمومی متعلق به نام استفاده کننده می باشد که بسته به سیاست CA ، روش امضاء همچنین اطلاعات دیگر را مانند ضمانت CA برای اعتباربه استفاده کننده انتقال دهد. هر CA باید یک عبارت معمول گواهی نامه [۳] (CPS) داشته باشد. CPS عملکرد CA را توضیح داده که چطور یک سازمان و یا یک فرد منحصر به فرد را قبل از ثبت یک گواهی نامه تصدیق کرده و اینکه چه نوع تعهد و مسئولیت CA مفروض است. گواهی نامه امضاء همچنین ازنفهمیدن هر نوع تغییر کلید عمومی توسط استفاده کننده و جلوگیری می کند. اگر نگهدارنده کلید عمومی به CA اعتماد کند و امضاء CA روی گواهی نامه متعلق داشته و اینکه کلید عمومی صحیح است. نگهدارنده ممکن است از گواهی نامه جهت تصدیق پیغام که بوسیله مشخص نامیده شده در گواهی نامه شده و متعلق با کلید خصوصی او علامت گذاری شده ، استفاده نماید.

اینکه یک سازمان CA در یک کمیته خیلی بزرگ برای تمام کسانی که می خواهند به طور امن ارتباط برقرار کنند شناخته شود مشکل بزرگی است بنابراین ممکن است چندین CA وجود داشته باشد. CA ها داخل یک کمیته بخصوص داخل یک دستگاه سلسله مراتبی[۴] سازمان یافته هستند. برای مثال می تواند یک سلسله مراتب از بانکها و یا شرکتهای بیمه کننده [۵] وجود داشته باشد. هرکسی در سلسله مراتب می تواند از یک گواهی نامه ثبت شده توسط CA داخل سلسله مراتب استفاده کند که تبادلات با معنی دیتای محافظت شده با رمزنگاری با دیگر افراد منحصر به فرد در سلسله مراتب انجام دهد.

در یک شخص منحصر به فرد می توان تعلق داشتن به چندین سلسله مراتب را انتخاب نماید. یک سلسله مراتب ممکن است نسبت به دیگر سلسله مراتب ها استانداردهای سخت تری را برای شناسایی برای شخص منحصر به فرد قبل از ثبت گواهی نامه اختصاص وی بکار ببرد .

گواهی نامه آن اعتبار بیشتری از دیگر سلسله مراتب که سخت گیری کمتری دارند را در بر می گیرد.یک دستگاه سلسله مراتب ممکن است استفاده کنندگان کاربرد خاصی را پشتیبانی کند. گواهی نامه یک سازمان ممکن است برای انطباق های روزمره قابل قبول باشد ومعرفی ای از سازمان دیگری به بانک ممکن است به خرید چیزی نیاز باشد. وقتی ما از یک مرورگر وب استفاده می کنیم و یک پیغام POP روی صفحه بالا می آید از ما می پرسد آیاعلاقمند به پذیرفتن گواهی نامه CA هستیم. حتی اگر

---

[3] Certificate Practices Statement
[4] Hierarchy
[5] Insurance

دستگاه سلسله مراتبی فقط یک CA داشته باشد می توانیم. به طور مؤثر به دستگاه سلسله مراتبی گواهی نامه بپیوندیم.

ممکن است یک شخص منحصر به فرد دریک دستگاه سلسله مراتبی نیاز داشته باشد با یک شخص منحصر به فرد در یک دستگاه سلسله مراتبی دیگر ارتباط برقرار کند. این شخص منحصر به فرد ممکن است عضویت در هر دو دستگاه را در صورت امکان انتخاب کند . انتخاب دیگر این است که توسط نقطه مضاعف[۶] (ملتقی)دو دستگاه (احتمالاً نقاط مضاعف ریشه) همدیگر را به طور متقابل تصدیق [۷] نمایند. در طی تصدیق متقابل ، نقاط مضاعف راهی برای گواهی کردن اشخاص دریافت کنند. در یک سازمان برای تأیید گواهی از سازمان دیگر را ایجاد می نمایند. لازم است گواهی متقابل با دقت در تأمین کردن سیاستهای بکار برده شده توسط CAها و سازگاری آنها انجام گیرد.

شروع به کار یک دستگاه گواهی دهنده و CA ها لازم است به دقت انجام گردد. به طور معمول قیمتها ، اجرا، عملیات ثبت شرکت برای این سیستم ها وجود دارد. همچنین صدور تعهد وجود دارد که بایستی دانسته شود. CAها ممکن است گواهی نامه هایشان را با ضمانت های مالی پشتیبانی نمایند. امنیت ، بحران تصحیح آلت و افزار سیستم و ایجاد نشدن استرس به حد کافی می باشد. استاندارد طرز اجرا [۸] ازCA می خواهد که یک جمله طرز اجرا گواهی نامه را صادر کند که طرز اجرا CA را توضیح داده و آنرا تعهد نماید. به عنوان دو محصول شناخته شدۀ CA می توان EntrustوVersign را نام برد. Identrus که یک شبکه جهانی انستیتو مالی می باشد. مثالی از کنسرسیوم ضمانت شده CA می باشد.

Identrus استانداردهایی برای بانکها ایجاد کرده که به عنوان معتمد سه بخشی برای تبادلات تجارت الکترونیکی بکار می رود. چشم انداز Edentrus,Entrust,verisign ریشۀ CA را ایجاد کرده اند که در قلۀ یک درخت معکوس دستگاه CA قرارد دارد. ریشۀ CA یک گواهی خود تأیید شده [۹] می باشد . پس از ریشه CA های دیگر هستند که گواهی خود تأیید شده توسط ریشه را دارند. ترازهای بعدی می تواند برای ایجاد خالص نمودن اعضاء شریک و یا توزیع کار یمربوطه ایجاد شوند. CAهادرهرتراز گواهی نامه های تأییدشده تراز بالاتر را دارند. در نهایت به ترازی با CA هایی می رسیم که گواهی نامه های user را تأیید می کنند. برخی دستگاهها شامل ریشه و گواهی نامه های user هستند. ممکن است برخی، چندین تراز به اضافه ریشه و نودهای user را داشته باشند.

راه حل دیگر مسئله توزیع کلید عمومی ، اگر چه در اقدامات تجارتی خیلی محبوب نیست استفاده از یک فرم از شبکه های معتقد غیر متمرکز به عنوان محیط های براساس محرمانگی سطح بالا[۱۰](PGP) می باشد. با PGP ،user ها کلید خودشان را مستقیماً از طریق ابزار امنی توزیع می کنند که با آنها ارتباط برقرار می

---

[6] Nodes

[7] Cross-certify

[8] - practice

[9] self signed

[10] . Pretty Good Privacy

کنند. ابزار امن می تواند گذاشتن گواهی نامه روی فلاپی و توسط شخصی به طور دستی به user ارتباط گیرنده داده شود. همچنین با PGP یک بخش معتمد ،
کسی که ما از قبل می شناسیم و به او اعتماد داریم می تواند یک گواهی نامه برای شخص منحصر به فرد دیگری که می خواهد برای ما شناخته شود را امضاء کند (تأیید کند) با دقت در پذیرش کلید و گواهی نامه ها یک شخص منحصر به فرد می تواند حلقهٔ ارتباطاتش را گسترش دهد.

روش گواهی نامه

چندین روش متناوب برای گواهی کردن کلیدهای عمومی وجود دارد.بازگشایی کد دیتا، مدلهای معتمد و مفاهیم اختصاصی می تواند در تعداد این تبادلها تغییر ایجاد کند در این بخش ما روی خدمات گواهی نامه x.509 متمرکز خواهیم شد. گواهی نامه x.509 به عنوان معمول ترین گواهی نامه کلید عمومی مورد بحث اند. در کنار کلید عمومی مالک یک گواهی نامه کلید عمومی شامل امضای CA روی کلید عمومی و کلید عمومی صاحب CA می باشد. اطلاعات دیگر در گواهی نامه ها شامل version گواهی نامه ، نام صاحب کلید،تعیین نسب سازمانیصاحب کلید، نام CA ، مدت زمان اعتبار گواهی نامه ، الگوریتم استفاده شده برای امضاء گواهی نامه و پارامترهای کلید می باشد.

گواهی های کلید عمومی x.509 در Abstract syntax Notation1 (ASN.1) کدگذاری شده اند . که با استفاده از استاندارد x.400 email ISO توسعه داده شده است .آن یک روش غیر وابسته به plat form برای تشخیص و نمایش دادن دیتا می باشد.

اهداف ASN1 وقتی که توسعه داده می شد بسیار شبیه به XML کنونی می باشد. ولی به هر حال آن انعطاف پذیری XML را ندارد یک مسئله ASN1 اینست که عناصر دارای برچسب نمی باشند.نتیجتاً بایستی کاربردی [11] جهت دانستن اینکه دقیقاً کدام عناصردر ساختار دیتا هستند و به چه ترتیبی آنها بایستی جهت بدست آوردن عبارت دیتای درست چیده شوند، ساخته شود.

علی رغم مشکلات کار با ASN.1 بسیاری از کابردهای ساخته شده فرض گردید که آن فرمت کد گذاری می باشد.امروزه بسیاری از این کاربردها پشت سر گذاشته شده و توجهات روی XML به عنوان راه حلی برای نمایش دیتا بدون بستگی به Platform می باشد.اما گواهی نامه کلید عمومی هنوز به روش ASN.1 کد گزاری می شود.

عناصر ASN.1 شامل نوع ،طول و مقدار می باشد.چندین نوع پایه تعیین گردیده اند .آنها شامل زنجیره بیت ، هشت تایی [12] زنجیره Character و Booleans ها می باشد.نمونه های پیچیده ای می توانند با استفاده از نمونه های پایه ساخته شوند. بعلاوه مشخص کردن خلاصه دیتا ، دو روش کلید گذاری پایه [13] (BER) و روش تشخیص داده کد [14] (DER)مورد استفاده می باشند.با BER تکه های یکسانی از دیتا می توانند از چندین راه مختلف نمایش داده شوند. این آنالوگ به 1و1.0 و1.00 همه به یک مقدار نشان داده

[11] Application
[12] Octets
[13] Basic encoding Rules
[14] Distinguished Encoding Rules

می شوند DERفقط اجازه یک نمایش را می دهد. کد گذاری DER وقتی به یک نمایش محکم و دقیق مانند امضاء دیجیتالی لازم است بکار برده می شود.

زیرساخت کلید عمومی

گواهی نامه های کلید عمومی به وجود یک زیرساخت مدیریتی جهت پشتیبانی ،تولید توزیع و فسخ گواهی نامه نیاز دارد . این زیرساخت، زیرساخت کلید عمومی [۱۵] (PKI) نامیده می شود. از آنجایی که مدیریت گواهی نامه اغلب به کلیدها گره خورده ،PKI ها اغلب به خوبی شامل مدیریت کلیدها می گردند. چندین اجزای ترکیبی برای PKI وجود دارد. CAکه قبلاً در موردش صحبت کردیم همچنین می تواند سند نام نویسی[۱۶] (RA) و یک کتابچه راهنما [۱۷]باشد. معمولاً بعلاوه اجزای نرم افزاری یک جمله اجرایی گواهی نامه (CPS) وجود دارد که عملکرد PKI، شاخص های امنیتی، و وسعت تعهد CAها شرح داده شده است.روش های زیادی برای عملکرد PKI وجود دارد .یکی از مفاهیم عملیاتی PKI در شکل 4.7 نمایش داده شده است.

۱ -آلیس با ایجاد یک کلید دو تایی عمومی- خصوصی فرایند را آغاز می نمایند.

۲ -نرم افزار موجود درسیستم آلیس کلید عمومی وی را داخل یک گواهی درخواست وارد می کند. او معمولاً گواهی درخواست را با استفاده از کلید خصوصیش (جفت ۲عدد) کلید عمومی در درخواست sign می نماید.

۳ -گواهی های خورد sign شده به یک RA ارسال می گردند زیرا ممکن است یک درخواست خود sign شده به اندازه کافی برای شناساییی هویت به CA جهت صدور گواهی نامه مستند نباشد.

۴ -قبل از اینکه CA گواهی صادر نماید، آلیس باید RA را متقاعد سازد (که به طور عملی به CA سپرده می شود) او همانی است که ادعا می کند RA معمولاً شامل شخص و نرم افزار استفاده شده جهت ایجاد درخواست گواهی نامه می باشد.مهمترین عملیات RA تصدیق هویت ارائه دهنده می باشد. برای مثال اگر آلیس بتواند RA را متقاعد نماید که او سو می باشد و RAبا کلید عمومی آلیس برای سو درخواست گواهی نامه نماید، آلیس می تواند خودش را به جای سو جا بزند.

۵ -یکبار هویت آلیس تصدیق شده است ، RA درخواست گواهی کلید عمومی خود Sign شدهٔ آلیس را گرفته آن را Sign می کند متناوباً اگر دریافت کننده امضاء حاضر به پذیرش ریسک باشد. آلیس می تواند به عنوان RA ی خودش عمل کرده و درخواست گواهی نامه را خودش Sign کند امضای آلیس روی درخواست اولیه با جفت شدن کلید عمومی داخل درخواست ثابت می کند که او مالک کلید خصوصی است . دوباره بدست آورد. گاهی اوقات برای اطمینان حاصل نمودن از اینکه

[15] Public key Infrastructure
[16] Registration Authority
[17] Directory

کلیدها به طور صحیح ایجاد شده اند، نگهدارنده کلید بایستی جفت کلید خودش را در حضور RA ایجاد نماید.

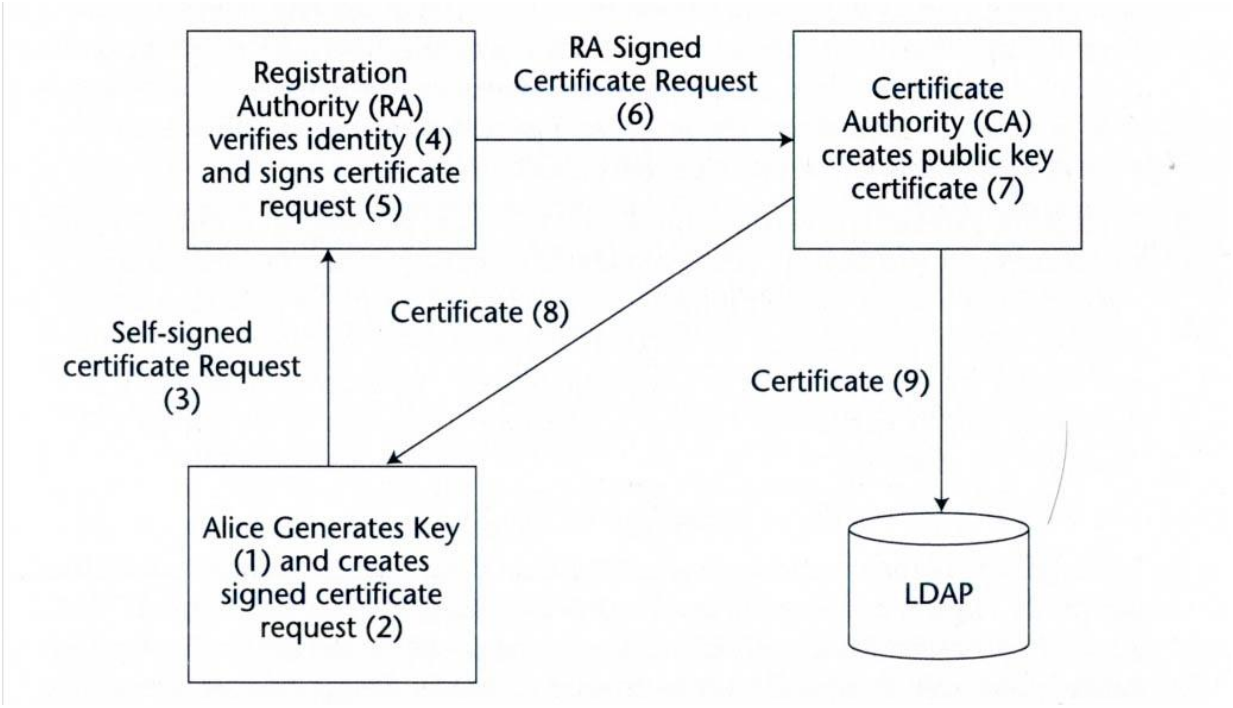
۶ -RA درخواست گواهی نامه را به CA می فرستد.

۷ -با دریافت درخواست گواهی نامه ، CA تصدیق می کند که امضای RA روی درخواست گواهی نامه بوده و تصدیق می کند که RA مستحق ساختن درخواست می باشد. با فرض اینکه RA مجاز شود، CA کلید عمومی داخل درخواست گواهی نامه را گرفته یک گواهی کلید عمومی با آن ایجاد می کند و گواهی نامه را Sign می نماید.

۸ -گواهی نامه ،آلیس پس فرستاده می شود و آلیس در آن یک signed- email , SSL ، یا هر جا که نیاز باشد امضایش تصدیق شود و پروتکل جهت مجاز نمودن آن کار گذاشته شود، را جایگذاری می کند.

۹ -همچنین ممکن است ، گواهی نامه را گرفته و آن را در یک کتابچه راهنما برای هرکسی که دوست دارد مطمئناً با آلیس ارتباط برقرار کند و یا می خواهد امضای آلیس را تصدیق کند گذاشته می شود که بتوان بدون وابستگی به هر نوع ارتباط مستقیم با آلیس ، گواهی کلید عمومی او را دوباره بدست آورد.

اگر بدلایلی کلیدهای آلیس بدلیل افتادن در دست کس دیگری ، به مخاطره بیافتد و یا گواهی نامه های او بدلیل تغییر یافتن به طور غیر مقتضی ، به مخاطره بیافتند ، CA بایستی اعلام نماید و گواهی آلیس باید لغو گردد. هنگامی که CA اعلام نماید که گواهی دیگر معتبر نیست، این گواهی نامه را به همراه تاریخ و زمان که نشان میدهد کی اعتبار گواهی نامه از بین رفته، داخل لیست گواهی نا مه های لغو شده [۱۸] (CRL) می گذارد.



[18] certificate revocation list

تبادلات کامل شده قبل از این زمان قابل قبول فرض می شود. تبادلات پس از این تاریخ می تواند مظنون واقع گردد. CA این لیست را در فواصل معین ایجاد کرده و آنرا به کتابچه راهنمای کم حجم دسترسی پروتکل[۱۹] (LDAP) پست می کند کتابچه راهنمایی که گواهی نامه ها و CRL ها در ساختمان درختی، سازمان سلسله مراتبی را درخود نگه می دارد. برای انجام ارتباطات مطمئن فردی و یا سازمانی با یک user در دستگاه سلسله مراتبی می توان گواهی نامۀ user را از کتابچه راهنما بدست آورده و اعتبار گواهی نامه را با کنترل کردن CAهای CRL تصدیق نمود. در تئوری هر کس که می خواهد از کلید آلیس استفاده کند بایستی قبل از استفاده از کلید به CA CRL او مراجعه نماید. درعمل از آنجایی که پیدا کردن کتابچه راهنمای CA و سپس دسترسی به آن مشکل می باشد(بیشتر Application هایی که از رمزنگاری کلید عمومی استفاده می کنند این طرح را پشتیبانی نمی کنند) ، بیشتر استفاده کنندگان گواهی نامه این کار را انجام نمی دهند و این مسئله امنیتی التزامی را بصورت باز رها می کنند.

هدف اصلی PKI ها این بود که دستگاه سلسله مراتبی CA ها جهانی و منفرد باشند. اعتبار CA می توانست تصدیق شود حتی اگر دریافت کنندۀ گواهی نا مه کلید عمومی به طور رسمی CA ویژه ای را نشناسد. واقعیت این است که بیشتر PKI ها به دیگر PKI ها بستگی ندارند . گواهی ها متقابل (یک CA برای CA دیگر معتبر نیست) گاهی اوقات وقتی که افراد در PKI های مختلف باید تبادل اطلاعات امنی داشته باشند مورد استفاده قرار می گیرد.

[19] Light weigh Directory Access protocol