امضاي ديجيتالي

الگوريتم كليد عمومي

- كليد عمومي يا رمز گذاري نامتقارن از دو كليد متفاوت كه به طور رياضي به هم وابسته هستند استفاده مي كنند . اگر چه تفاوتهايي در عملكرد آنها وجود دارد آنها را مي توان به دو روش معمول براي رمز گذاري و امضاي ديجيتالي تقسيم نمود.

رمز گذاري

- رمز گذاري
- RSA
- منحني بيضوي يا (ECDH) Diffic-Hellman (DH)
- امضاي ديجيتالي
- RSA
- الگوريتم امضاي ديجيتالي و يا منحني بيضوي DSA (ECDSA)

- وقتي الگوريتم كليد عمومي داخل سيستم وارد و تركيب مي شود با الگوريتم سريعتري تركيب مي شود كه سيستم را قادر به استفاده از مقادير زياد ديتا مي كند . ما ابتدا در خصوص رمز نگاري و سپس امضاء ديجيتالي بحث خواهيم نمود.

رمز نگاري

- رمز نگاري جنبه محرمانگي را ايجاد مي كند و اينكار از طريق جلو گيري از درك ديتا توسط افرادي بجز دريافت كننده انجام ميگرد رمز نگاري خوبي از كنترل دسترسي توسط خاصيت اختصاصي مديريت كليد صورت مي دهد. فقط دريافت كننده كليد لازم را براي بازگشايي رمز ديتا داشته و مي تواند به آن
- دسترسي پيدا كند.

دو روش عمومي در فناوري كليد عمومي براي پشتيباني رمزنگاري ديتا استفاده مي شود،RSA و Diffic-Hellman از اينجهت لفظ پشتيباني بكار برده شد كه الگوريتم كليد عمومي در محاسبه براي استفاده از رمز نگاري كردن ديتا بسيار گران است . اينست كه استفاده از (رمز گذاري كليد عمومي) براي رمز نگاري اتلاف وقت بوده و در اجرا مشكل خواهد داشت .

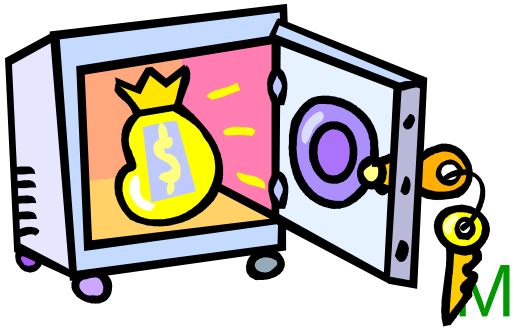
بنا بر اين به جاي رمز نمودن ديتابه طور مستقيم الگوريتم كليد عمومي با يك الگوريتم متقارن كليد براي محافظت ديتا بكار مي رود.

RSA

- RSA بر اساس نام Ronald Rivet, Adi shamir و Leonard Adlman نامیده شده که توسعه دهندگان الگوریتم مي باشند.که شناخته کد نشانه الگوریتم کلید عمومي است .
- هنگامي که مردم درباره رمز نگاري کلید عمومي سؤال مي کنند در واقع در مورد عملکرد RSA توضیح مي خواهند . کیفیت RSA برگشت پذیر بودن الگوریتم است. از لحاظ تکنیکي RSA یا هر الگوریتم کلید عمومي برگشت پذیر نیست. الگوریتم کلید عمومي تابع يك سويه است لیکن از آنجایي برگشت پذیر خوانده مي شود که دیتاي انتقال داده شده مي تواند با يك کلید متفاوت دیگري دوباره بدست بیاید .

- با RSA مي توان با استفاده از كليد خصوصي ديتايي را كه قبلاً با كليد عمومي رمز نگاري شده را دوباره بدست آورد . اين مفهوم در شكل A.1 توضيح داده شده است. با RSA كليد عمومي جهت رمز كردن ديتا استفاده مي شود و كليد خصوصي جهت بازگشايي رمز ديتا استفاده مي شود. از آنجايي كه كليد خصوصي هم دارد هر كسي مي تواند ديتا را براي صاحب كليد رمز نگاري كند اما فقط صاحب كليد مي تواند ديتا را بازگشايي رمز نمايد.
- در اجرا قسمتي از رمز نگاري نمودن سيستم با RSA براي رمز نگاري نمودن از يك كليد متقارن استفاده مي كند كه با ديتا را باب مي خواهد با روشي اطلاعاتي به آليس بفرستد كه فقط آليس قادر به فهميدن آن باشد.

- باب با ابجاد يك كليد متقارن شروع مي كند
- او از اين كليد جهت رمز گشايی نمودن ديتا با يك الگوريتم متقارن مانند DES استفاده مي كند
- با استفاده از كليد عمومي آليس او كليد متقارن را رمز گشايی مي كند كه به پيغام رمز گشايی شده اي مي شود. اين رمز گشايی مراقبت مي كند كه فقط آليس قادر به باز گشايی رمز نمودن و استفاده از كليد متقارن باشد.
- هنگامي كه پيغام مي رسد آليس كليد متقارن رمز گشايی شده را از پيغام بيرون آورده و با استفاده از كليد خصوصي خود باز گشايی رمز مي نمايد.
- با استفاده از كليد متقارن بدست آمده آليس تمام پيغام را باز گشايی رمز مي نمايد.



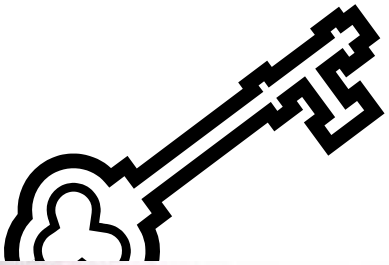
Diffiec- Hellman,Elliptic Curve Diffic – Hellman

- الگوريتم به افتخار Martin Hellman , Whit fiell Diffic نامگذاري شده كه توسعه دهندگان الگوريتم بودند. دركليد توافقي ، دو قسمت اطلاعاتي را تبادل مي كنند كه به آنها اجازه مي دهد يك بخش سري را shareشده را بدست آورند. قسمتهاي غير مجاز مي توانند اطلاعات تبادل شده را جدا كنند اما آنها قادر به تعيين shard secret نيستند: اين shard secret مي تواند به عنوان كليد الگوريتم متقارن استفاده شود. پروژه توافقي كليد DH در شكل A.B نشان داده شده است .

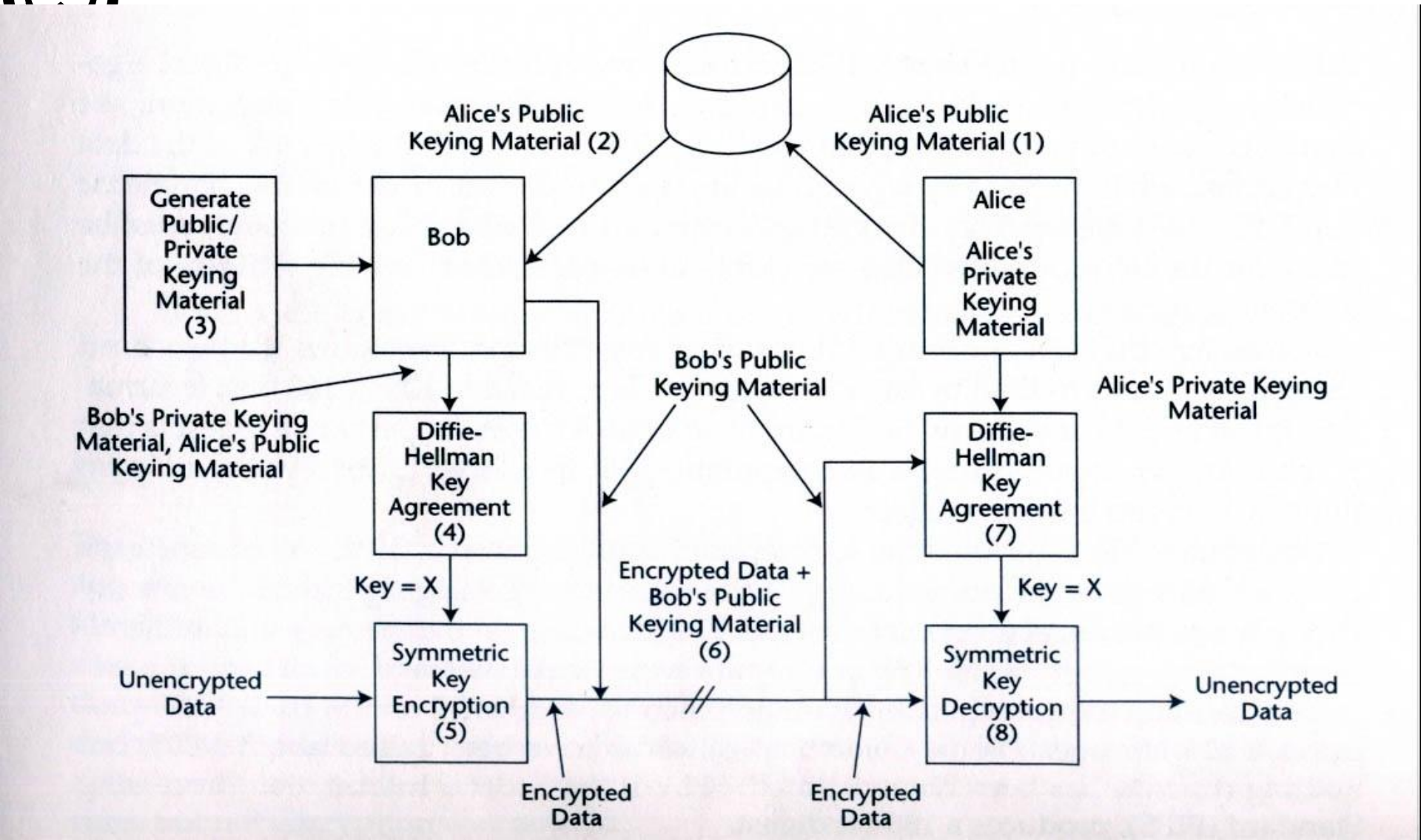
- (DH) و منحني بيضوي (DH) الگوريتم هاي توافقي كليدها مي باشد .

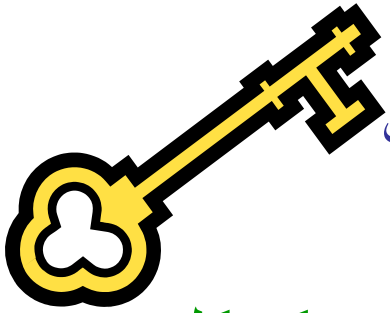
در شکل زیردو طرف باب و آلیس که مي خواهند تبادل اطلاعات کنند ازرمزنگاری استفاده مي کند.

- در شکل دو طرف باب و آلیس که مي خواهند تبادل اطلاعات کنند از رمز نگاری استفاده مي کند.
- باب به آلیس کلید شده عمومي اش را مي فرستد (این یك کلید نیست در واقع اطلاعاتي است که اجازه مي دهد که کلید بدست آید)
- آلیس به باب مطالب کلید عمومي خود را مي فرستد
- هر کدام با استفاده نمودن از این اطلاعات و الگوریتم DH یك Comman را بدست مي آورند.
- باب از secret براي بازگشایی رمز نمودن دیتا ارسالي باب استفاده مي کند

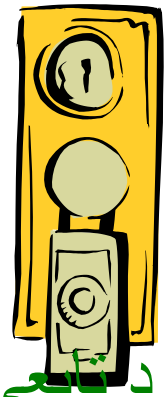


شکل A.4 نشان مي دهد كه DH چگونه مي تواند به عنوان سخت از يك سيستم رمزنگاری کننده استفاده شود.





- تبادل مطالب كليد شده مانند بحث قبلي به هم تأثير گذار نيستند مطالب كليد شده عمومي مي تواند در يك مكان شناخته شده ثبت شود.
- **يك مانع يا مشكل سيستم** Diffiec- Hellman آن است كه كليد متقارن draw back استفاده شده براي رمزنگاری نمودن به اطلاعات ارسالي از فرستنده و گيرنده وابسته است . اگر يك پيغام بايستي به چند دريافت كننده لازم مي شود بايستي چند بار encrtypt مي شود.
- يكبار براي هر دريافت كننده public را بكار مي برد.
- بحث قبلي از الگوريتم توافقي كليدDiffiec- Hellman استفاده كرده است اگرما از ECDH استفاده كنيم بسيار ساده تر مي گردد. به هر حال در Cryptography منحني بيضوي از نقاطس تعريف شده بوسيله يك منحني بيضوي درميان محدود ترجيحاً از محل ورود صحيح برخي اعداد درجه اول مانند آنچه در Diffiec- Hellman استفاده مي كنيم.



امضای دیجیتالی

- از آنجاييكه فقط صاحب كليد ، كليد خصوصي را نگه مي دارد تابعي كه از كليد خصوصي استفاده مي كند براي كار صاحب كليد استفاده مي شود نه كس ديگر. اين عمل راهي به سوي جهان رمزنگاری به مفهوم امضاء ديجيتالي خواهد بود.
- امضاء ديجيتالي بوسيله صاحب كليد خصوصي براي امضاءكردن اطلاعات الكترونيكي براي جلوگيري از جعل كردن بكار مي رود.یک طرف صاحب کلیدخصوصی می تواندبا امضاء دیجیتالی به خوبی فرم را تکمیل کند.
- امضاءديجيتالي از امضاء دست خط قوي تر است چرا كه امضاء به صورت رياضي به ديتا نشان(sign) شده گره خورده است.
- امضاء ديجيتالي نمي تواند از يك سند بريده شود وبه سند ديگر چسبانده شود.

- همچنين هر تغيير ديتاي Signed شده امضاء را بي اعتبار مي كند. يك امضاء ديجيتالي از ديتاي Sing شده و كليد خصوصي امضاء كننده ايجاد مي گردد. امضاء به پيغام ضميمه مي گردد. هر فردي كه پيغام را دريافت مي كند تابع وابسته ديگري و با استفاده از كليد عمومي و يا امضاء و يا ديتاي نهاده شده اجرا مي كند (كه بستگي به الگوريتم دارد). اگر اجراي اين تابع نتيجه مورد انتظار را تصديق كند، امضاء معتبر در نظر گرفته مي شود. امضاء ديجيتالي چند سرويس سري (امنيتي) توليد مي كند. آنها پيغام را از جهت اينكه فقط توسط صاحب كليد (كه صاحب كليد خصوصي مي باشد) و مي تواند پيغام را امضاء كند، sing شده باشد،اعتبار مي بخشند.

- يك امضاء ديجيتالي همچنين با چك نمودن صحت پيغام از تغييرات غيرمجاز جلوگيري مي كند.
- اگر يك امضاء ديجيتالي نتواند به عنوان يك امضاء كننده تائيد شود فرض مي شود كه متن پيغام تغيير كرده است. هنگامي كه يك امضاء ديجيتالي به خودي خود براي جلوگيری از تكرار مجدد كافی نباشد ، يک ساختمان ديجيتالي مي تواند نقش قسمت كليد براي جلوگيری از تكرار مجدد را بازي مي كند.

پيغام Digest

- قبل از اينكه در مورد الگوريتم هاي امضاء ديجيتالي بحث كنيم درخصوص الگوريتمهاي پيغام digest (كه به عنوان الگوريتمهاي hashing نيز ناميده مي شوند) بحث مي كنيم.

- در بحث رمز گشايی توضيح داديم كه چگونه الگوريتمهاي متقارن مانند DES به عنوان رمز نگاری كننده ديتا بكار مي روند و چگونه الگوريتم هاي كليد عمومي براي پشتيباني يا بدست آوردن كليد متقارن استفاده مي شود. اين عمل سرعت رمز نگاری را به صورت قابل قبول حفظ مي كند. يك همسازي مشابه بايد براي امضاء ديجيتالي ساخته شود اين همسازي شامل ايجاد يك digest از ديتاي sing شده مي باشد.

- يك الگوريتم پيغام digest شد. در هر اندازه ارائه مي شود و آن را داخل يك رشته با اندازه ثابت انتقال پيدا مي كند. از آنجايي كه يك ميليون byte و يا اطلاعات بيشتر به ۱۲۸ و يا ۱٦۰ بيت bit كاهش مي يابد اطلاعات از دست مي رود و انتقال قابل برگشت نيست.

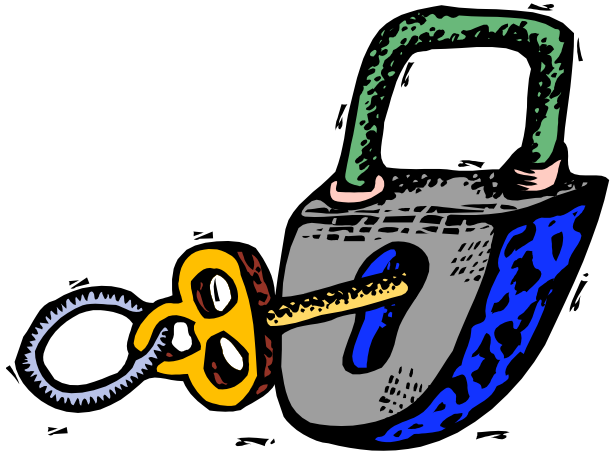
- يك خاصيت اصلي digest آن است كه يك input string شناخته شده با صدور محاسباتي قادر به كشف يا input string متفاوت با يك digest يكسان نيست.

- از آنجايي كه الگوريتم هاي كليد عمومي از نقطه نظرمحاسباتي گران هستند، به جاي پيغام كامل پيغام digest شده sign مي گردد. با الگوريتم digesting مناسب خواص امنيتي پيغام مسئله اي ساختگي نيست. امضاي روي پيغام هنوز پيغام را تصديق كرده و اعتبار امضاء هنوز تاييد مي كند كه يك پيغام هنوز تغيير نيافته است.

عموماً دو الگوريتم digest كردن پيغام استفاده مي شود. MD5 و SH1 .

MD5 يك Digest 128 بيتي را توليد مي كند.

- MD5 يك digest 128 بيتي ايجاد مي كند برخي از تئوريكي واقعي از MD5 برخواستهاند اما هيچكدام واقعاً اثبات نشده اند. SHA1 در استاندارد متحدسازي جريان اطلاعات يك digest 160 بيتي را توليد مي كند.



RSA

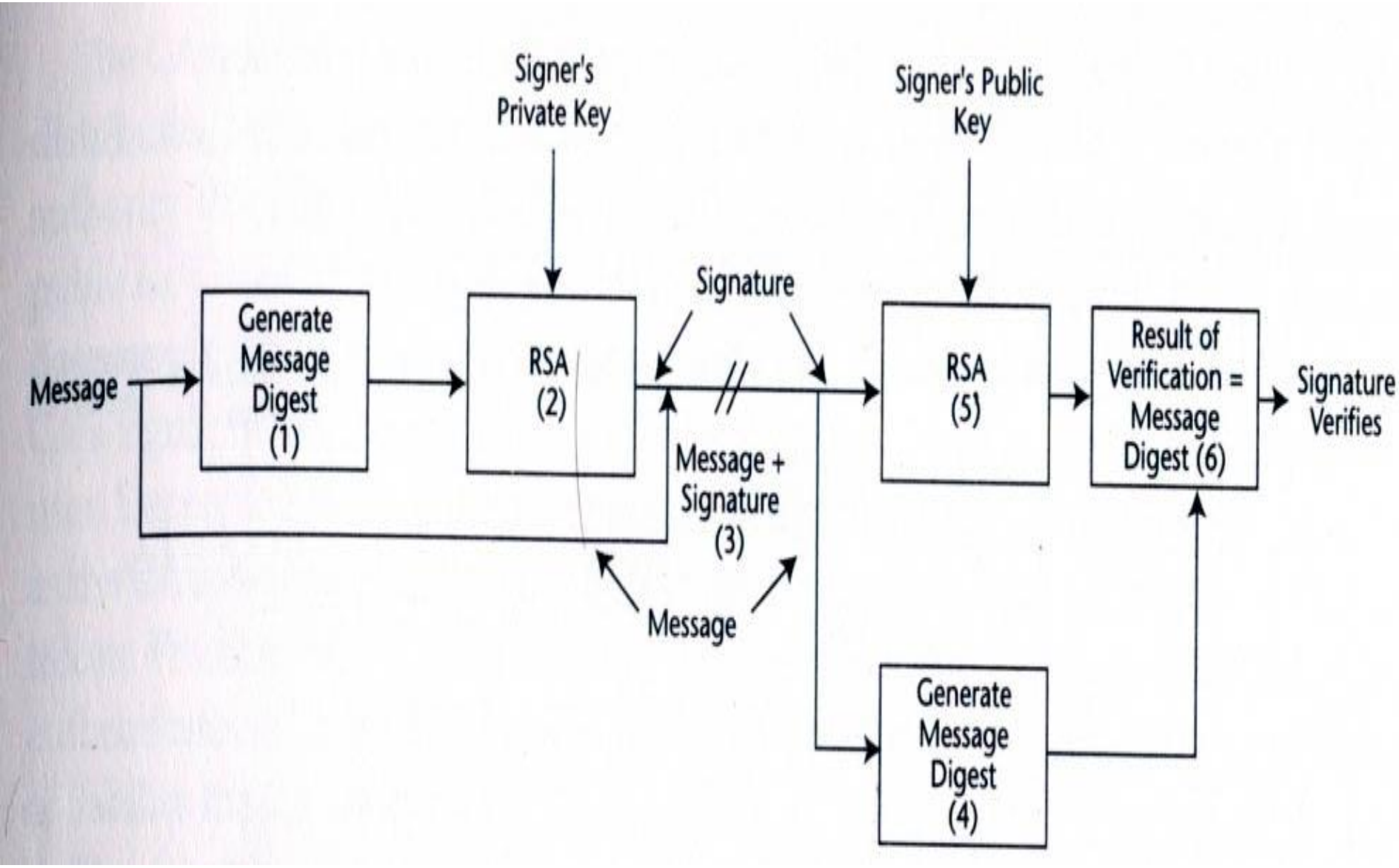
- دقيقاً همان الگوريتم RSA استفاده شده براي رمز نگاری ، مي تواند براي امضاء ديجيتالي استفاده شود. استفاده از RSA براي امضاء در شكل ٤٠٥ نشان داده شده است.

١. ابتدا يك پيغام Digest محاسبه مي شود.
٢. كليد خصوصي براي علامت گذاري پيغام digest شده استفاده مي شود.
٣. امضاء به پيغام پيوست مي شود و به دريافت كننده انتقال مي يابد.

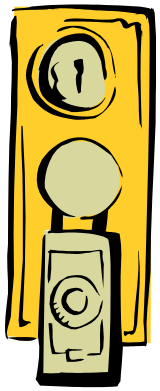
۴-دريافت كننده digest پيغام دريافتي را محاسبه مي كند.

۵-سپس لازمه تاييد امضاء خارج نمودن امضاء از پيغام و استفاده از RSA روي امضاء با كليد عمومي مي باشد .

۶-اگر نتيجه انتقال و digest محاسبه شده جديد برابر باشد، امضاء معتبر است.


Signer's
Private Key
Signer's Public
Key
Signature
Message
Generate
Message
Digest
(1)
RSA
(2)
Message +
Signature
(3)
RSA
(5)
Result of
Verification =
Message
Digest (6)
Signature
Verifies
Message
Generate
Message
Digest
(4)

DSA

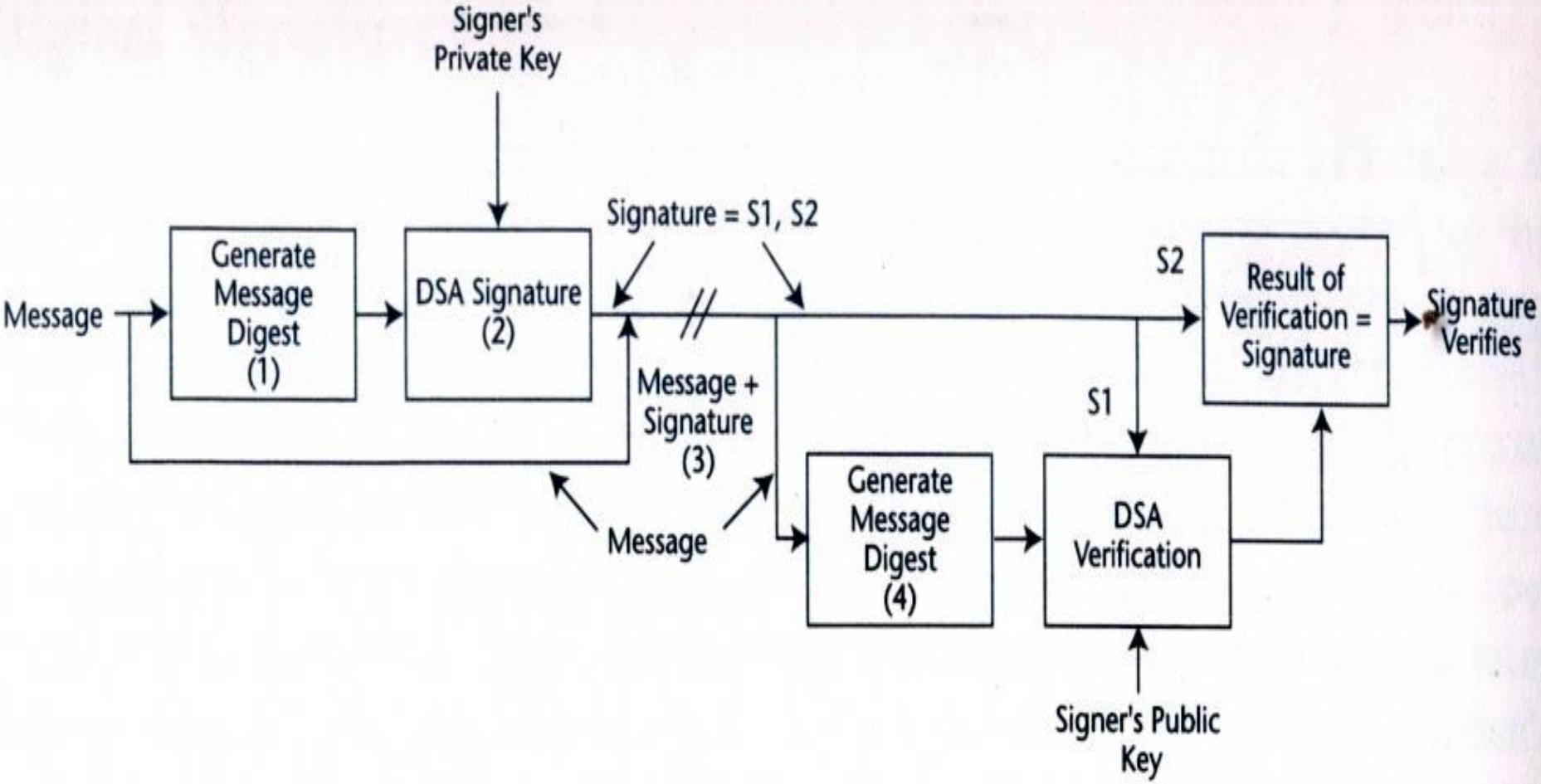


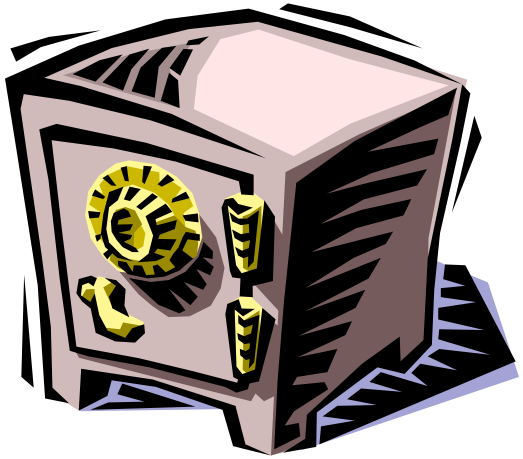
- انستيتو ملي استانداردها و تكنولوژي ،الگوريتم امضاء ديجيتالي را توسعه داده است. DSA
- (Digital signature Algorithm)
- دليل اين توسعه ايجاد يك شق ديگر براي RSA است كه بتواند براي امضاء استفاده شودو در رمز نگاری استفاده نشود .

- دولت U.S در استفاده بي رويه و غير قابل كنترل ازرمز نگاری متمركز شده است. موقعيت دولت اين بود كه رمز نگاری قوي فقط براي استفاده دولت يا ديگر شركت ها بوده است. استفاده از رمز نگاری بوسيله ديگران توانايي دولت را در استراق سمع بر فعاليت هاي قانون شكنان در بر خواهد داشت. يك شق ديگر RSA است كه مي تواند براي امضاء ديجيتالي استفاده شود اما به رمز نگاری شدن نيازي نيست.

الگوريتم DSA اين ملزومات را دربردارد. با شكل ٤٠٦ عملكرد آن را به توضيح داده شده است با DSA:

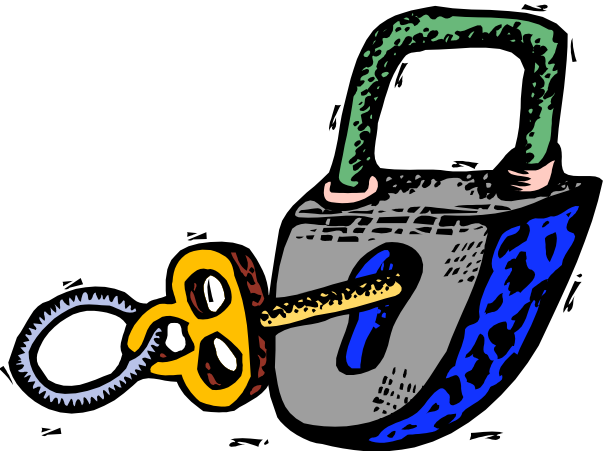
١. پيغام بايد يك پيغام digest را ايجاد كند.
٢. پيغام digest علامت زده مي شود امضاء به دو قسمت نوشته مي شود.
٣. سپس امضاء و ديگر اطلاعات پشتيباني كننده به پيغام ضميمه شده و به سمت دريافت كننده ارسال مي گردند.
٤. دريافت كننده digest پيغام را محاسبه كرده و يك تابع براساس كليد عمومي امضاء كننده، digest و امضاء اجرا مي كند. اگر نتيجه اين اجرا با قسمت امضاء برابر باشد امضاء معتبر است.


Signer's
Private Key
Signature = S1, S2
Message
Generate
Message
Digest
(1)
DSA Signature
(2)
S2
Result of
Verification =
Signature
Signature
Verifies
Message +
Signature
(3)
S1
Message
Generate
Message
Digest
(4)
DSA
Verification
Signer's Public
Key



گواهي نامه هاي كليد عمومي

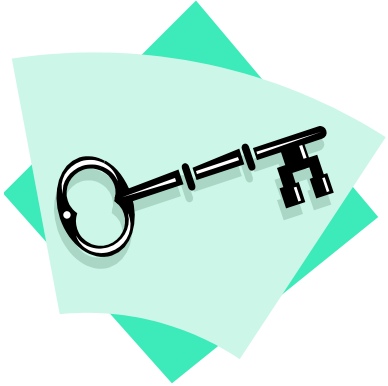
- هنگامي كه كليد عمومي مي تواند آزادانه منتشر و پخش شده و توسط هر كسي نگهداري شود، هنوز بايد براي اجتناب ازاينكه غيرواقعي نمايش داده شود ،امن گردد. براي اينكه سيستم كار كند، استفاده كنندگان كليد عمومي احتياج دارند كه اطمينان حاصل كنند كه مالك كليد كيست و آنكه كليد صحيح بوده و تغيير داده نشده باشد. اگر اين امكان وجود داشته باشد كه كليد عمومي يك نفر با شخص ديگري جايگزين گردد، استفاده كننده كليد مي تواند به هدايت شدن جهت انتقال با شخص ديگري بجز كسي كه او انتظار دارد، گول زده شود.



- در جامعه انساني ما از روش معرفي نمودن در موقعيت مشابه استفاده مي كنيم. كسي كه ما مي شناسيم و به او اعتماد داريم به ما شخص ديگري را كه نمي شناسيم معرفي مي نمايد. هنگامي كه اين روش بوسيله شخص واقعي نتواند انجام شود نامه هاي معرفي مي توانند مورد استفاده قرار گيرند. در اين روش يك شبكه معتمد ساخته مي شود.

- در دنياي الكترونيكي گواهي نامه هاي كليد عمومي نقش نامه هاي معرفي را بازي مي كنند. گواهي نامه ها به عنوان روشي در يك سازمان معتمد شناخته شده به عنوان (CA) تصديق كننده گواهي نامه[1]، براي معرفي ما به شخص منحصر به فردی توسط ضمانت كردن كليد عمومي آن فرد عمل مي كند.

[1]Certificate Authority



- گواهي نامه ها اين امكان را براي دريافت كننده كليد عمومي فراهم مي سازد كه با اطمينان كسي كه صاحب كليد است را بشناسد و مطمئن شود كه كليد تغيير نيافته است. اين روشي براي CA است كه به يك شخص منحصر به فردي با كليد عمومي اش متصل گردد از جهتي كه بدون اينكه كشف آن ممكن باشد تغييراتي را در آن انجام دهد.

- CA از يك ديتابيس مركزي (منطقي) ، براي تمام كليدهاي عمومي ثبت شده نگهداري مي‌كند و گواهي نامه هاي كليد عمومي را توزيع مي نمايذ. هر گواهي نامه لزوماً عبارتي است با تصديق توضيحات اصول كليد عمومي. CA براي يك كليد عمومي منحصر به فرد با استفاده از كليد خصوصي آن براي علامتگذاري گواهي نامه كليد عمومي، ضمانت مي كند كه سندی الكترونيكي است شامل نام استفاده كننده و كليد عمومي در كنار ديگر اطلاعات مي‌باشد.

- امضاء CA روي گواهي نامه نشان دهنده اينست كه كليد عمومي متعلق به نام استفاده كننده مي باشدكه بسته به سياستCA ، روش امضاء همچنين اطلاعات ديگر را مانند ضمانت CA براي اعتباربه استفاده كننده انتقال دهد. هر CA بايد يك عبارت معمول گواهي نامه[۱] (CPS) داشته باشد. CPS عملكرد CA را توضيح داده كه چطور يك سازمان و يا يك فرد منحصر به فرد را قبل از ثبت يك گواهي نامه تصديق كرده و اينكه چه نوع تعهد و مسئوليت CA مفروض است.
- گواهي نامه امضاء همچنين ازنفهميدن هر نوع تغيير كليد عمومي توسط استفاده كننده و جلوگيري مي كند. اگر نگهدارنده كليد عمومي به CA اعتماد كند و امضاء CA روي گواهي نامه متعلق داشته و اينكه كليد عمومي صحيح است. نگهدارنده ممكن است از گواهي نامه جهت تصديق پيغام كه بوسيله مشخص ناميده شده در گواهي نامه شده و متعلق با كليد خصوصي او علامت گذاري شده ، استفاده نمايد.

1]Certificate Practices Statement

- اينكه يك سازمان CA در يك كميته خيلي بزرگ براى تمام كساني كه مي خواهند به طور امن ارتباط برقرار كنند شناخته شود مشكل بزرگي است بنابراين ممكن است چندين CA وجود داشته باشد.CA ها داخل يك كميته بخصوص داخل يك دستگاه سلسله مراتبى[1] سازمان يافته هستند. براي مثال مي تواند يك سلسله مراتب از بانكها و يا شركتهاي بيمه كننده[٢] وجود داشته باشد. هركسي در سلسله مراتب مي تواند از يك گواهي نامه ثبت شده توسط CA داخل سلسله مراتب استفاده كند كه تبادلات با معني ديتاي محافظت شده با رمزنگاري با ديگر افراد منحصر به فرد در سلسله مراتب انجام دهد.
- در يك شخص منحصر به فرد مي توان تعلق داشتن به چندين سلسله مراتب را انتخاب نمايد. يك سلسله مراتب ممكن است نسبت به ديگر سلسله مراتب ها استانداردهاي سخت تري را براي شناسايي براي شخص منحصر به فرد قبل از ثبت گواهي نامه اختصاص وي بكار ببرد .

- [1] Hierarchy
- [2]Insurance

- گواهي نامه آن اعتبار بيشتري از ديگر سلسله مراتب كه سخت گيري كمتري دارند را در بر مي گيرد.يك دستگاه سلسله مراتب ممكن است استفاده كنندگان كاربرد خاصي را پشتيباني كند.
- گواهي نامه يك سازمان ممكن است براي انطباق هاي روزمره قابل قبول باشد ومعرفي اى از سازمان ديگري به بانك ممكن است به خريد چيزي نياز باشد. وقتي ما از يك مرورگر وب استفاده مي كنيم و يك پيغام POP روي صفحه بالا مي آيد از ما مي پرسدآياعلاقمند به پذيرفتن گواهي نامه CA هستيم. حتي اگر دستگاه سلسله مراتبي فقط يك CA داشته باشد می توانيم. به طور مؤثر به دستگاه سلسله مراتبي گواهي نامه بپيونديم.

ممكن است يك شخص منحصر به فرد دريك دستگاه سلسله مراتبي نياز داشته باشد با يك شخص منحصر به فرد در يك دستگاه سلسله مراتبي ديگر ارتباط برقرار كند. اين شخص منحصر به فرد ممكن است عضويت در هر دو دستگاه را در صورت امكان انتخاب كند .

- توسط نقطه مضاعف[۱] (ملتقي)دو دستگاه (احتمالاً نقاط مضاعف ريشه) همديگر را به طور متقابل تصديق[۲] نمايند. در طي تصديق متقابل ، نقاط مضاعف راهي براي گواهي كردن اشخاص دريافت كنند. در يك سازمان براي تأييد گواهي از سازمان ديگر را ايجاد مي نمايند.لازم است گواهي متقابل با دقت در تأمين كردن سياستهاي بكار برده شده توسط CAها و سازگاري آنها انجام گيرد.

شروع به كار يك دستگاه گواهي دهنده و CA ها لازم است به دقت انجام گردد.به طور معمول قيمتها ، اجرا، عمليات ثبت شركت براي اين سيستم ها وجود دارد. همچنين صدور تعهد وجود دارد كه بايستي دانسته شود. CAها ممكن است گواهي نامه هايشان را با ضمانت هاي مالي پشتيباني نمايند. امنيت ، بحران تصحيح آلت و افزار سيستم و ايجاد نشدن استرس به حد كافی می باشد. استاندارد طرز اجرا [1] ازCA می خواهد كه يك جمله طرز اجرا گواهي نامه را صادر كند كه طرز اجرا CA را توضيح داده و آنرا تعهد نمايد

- practice [1]

[1] Nodes

[2] Cross-certify

به عنوان دو محصول شناخته شدة CA مي توان Entrustو Versign را نام برد. Identrus كه يك شبكه جهاني انستيتو مالي مي باشد. مثالي از كنسرسيوم ضمانت شده CA مي باشد.

- Identrus استانداردهايي براي بانكها ايجاد كرده كه به عنوان معتمد سه بخشي براي تبادلات تجارت الكترونيكي بكار مي رود. چشم انداز Edentrus,Entrust,verisign
- ريشة CA را ايجاد كرده اند كه در قلة يك درخت معكوس دستگاه CA قرارد دارد. ريشة CA يك گواهي خود تأييد شده[۱] مي باشد . پس از ريشه CA هاي ديگر هستند كه گواهي خود تأييد شده توسط ريشه را دارند. self signed[1]
- ترازهای بعدي مي تواند براي ايجاد خالص نمودن اعضاء شريك و يا توزيع كاريمربوطه ايجاد شوند.CAهادرهرتراز گواهی نامه های تأييدشده تراز بالاتر را دارند. در نهايت به ترازي با CA هايي مي رسيم كه گواهي نامه هاي user را تأييد مي كنند. برخي دستگاهها شامل ريشه و گواهي نامه هاي user هستند. ممكن است برخی، چندين تراز به اضافه ريشه و نودهاي user را داشته باشند.

- راه حل ديگر مسئله توزيع كليد عمومي، اگر چه در اقدامات تجارتي خيلي محبوب نيست استفاده از يك فرم از شبكه هاي معتقد غير متمركز به عنوان محيط هاي براساس محرمانگي سطح بالا[1](PGP) مي باشد.
با PGP، user ها كليد خودشان را مستقيماً از طريق ابزار امني توزيع مي كنند كه با آنها ارتباط برقرار مي كنند. ابزار امن مي تواند گذاشتن گواهي نامه روي فلاپي و توسط شخصي به طور دستي به user ارتباط گيرنده داده شود
[1] Pretty Good Privacy .

كسي كه ما از قبل مي شناسيم و به او اعتماد داريم مي تواند يك گواهي نامه براي شخص منحصر به فرد ديگري كه مي خواهد براي ما شناخته شود را امضاء كند (تأييد كند) با دقت در پذيرش كليد و گواهي نامه ها يك شخص منحصر به فرد مي تواند حلقة ارتباطاتش را گسترش دهد.

روش گواهی نامه

- چندين روش متناوب براي گواهي كردن كليدهاي عمومي وجود دارد.بازگشايي كد ديتا، مدلهاي معتمد و مفاهيم اختصاصي مي تواند در تعداد اين تبادلها تغيير ايجاد كند در اين بخش ما روي خدمات گواهي نامه x.509 متمركز خواهيم شد. گواهي نامه x.509 به عنوان معمول ترين گواهي نامه كليد عمومي مورد بحث اند. در كنار كليد عمومي مالك يك گواهي نامه كليد عمومي شامل امضاي CA روي كليد عمومي و كليد عمومي صاحب CA مي باشد.
اطلاعات ديگر در گواهي نامه ها شامل version گواهي نامه ، نام صاحب كليد،تعيين نسب سازمانيصاحب كليد، نام CA ، مدت زمان اعتبار گواهی نامه ، الگوريتم استفاه شده براي امضاء گواهي نامه و پارامترهاي كليد مي باشد.

گواهي هاي كليد عمومي x.509 در Abstract syntax Notation1 (ASN.1) كدگذاري شده اند . كه با استفاده از استاندارد ISO x.400 email توسعه داده شده است .آن يك روش غير وابسته به plat form براي تشخيص نمايش دادن ديتا مي باشد.

- اهداف ASN1 وقتی که توسعه داده می شد بسیار شبیه بهXML 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[1] 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.
- Application [1]

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.