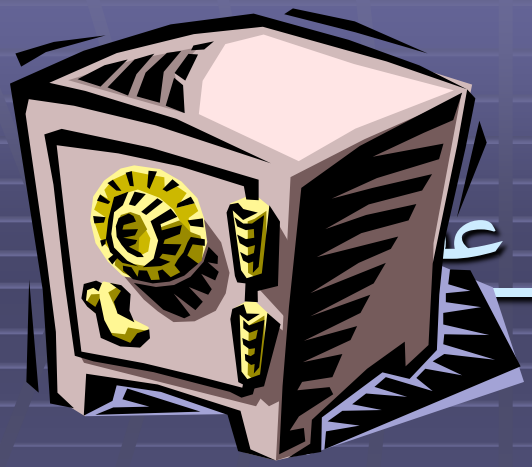
امضای دیجیتالی

۱-گواهي نامه هاي کليد عمومي

۲-زيرساخت کليد عمومي



گواهی نامه های کلید ع

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 [illegible] به عنوان (CA) تصديق كننده گواهي نامه[1]، براي معرفي [illegible] به فردی توسط ضمانت كردن كليد عمومي آن فرد عمل مي كند.

[1]Certificate Authority

- CA از يك ديتابيس (منطقي) ، براي تمام كليدهاي ثبت شده نگهداري مي‌كند و مديريت نامه هاي كليد عمومي را توزيع مي نمايد. 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.

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.

امضاء [illegible] گواهي نامه نشان دهنده اي [illegible] عمومي متعلق به نام است [illegible] باشدكه بسته به سياست CA [illegible] روش امضاء همچنين اطلاعات ديگر را مانند ضمانت CA براي اعتباربه استفاده كننده انتقال دهد. هر CA بايد يك عبارت معمول گواهي نامه[1] (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.

1]Certificate Practices Statement

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.

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 استاند
را بر
شخص
قبل از
اختصاص وي بكار ببرد .

Hierarchy [1]

[2]Insurance

گ ...يشتري از ديگر سلسله
م ...كمتري دارند را در بر
مي گيرد. يك 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 تامين 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 ، اجراء 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 الت و افزار سيستم و ايجاد نشدن استرس به حد كافي مي باشد. استاندارد طرز اجرا[1] ازCA مي خواهد كه يك جمله طرز اجرا گواهي نامه را صادر كند كه طرز اجرا CA را توضيح داده و آنرا تعهد نمايد.

[1] Nodes

[2] Cross-certify

[1] - practice

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 قرارهاي بعدي مي تواند براي ايجاد خالص نمودن اعضاء شريك و ريشة توزيع كار مربوطه ايجاد شوند. CA هادر هرتراز گواهی نامه های يك تأييدشده توسط بالاتر را دارد. دارد نهايت به ترازي با CA هايي مي رسيم كه خوهي نامه هي user را تأييد مي كنند. برخي دستگاهها ريشه و گواهي نامه هاي user هستند. ممكن است برخی، چندين ترازبه اضافه ريشه و توسط هاي user را داشته باشند. شده توسط ريشه را دارند.

[1] self signed

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(PGP)[1] مي باشد.

با PGP، user ها كليد خودشان را مستقيماً از طريق ابزار امني توزيع مي كنند كه با آنها ارتباط برقرار مي كنند. براي مثال، بسري كه ما از قبل مي شناسيم و به او اعتماد داريم مي تواند گواهي نامه اي را امضاء كند (تأييد كند) با دقت در پذيرش كليد و گواهي نامه ها يك شخص منحصر به فرد مي تواند حلقه ارتباطاتش را گسترش دهد.

براي ناظر امن مي تواند گواهي نامه اي را امضاء كند و توسط شخصي به طور دستي به user ارتباط گيرنده داده شود.

[1] . Pretty Good Privacy

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 و 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.

[1] Application

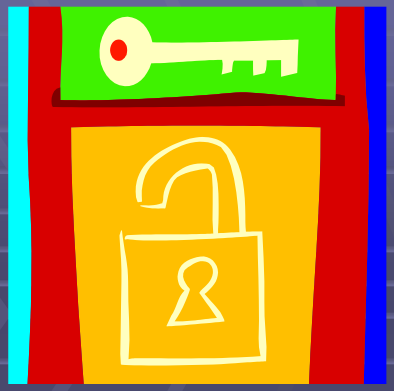
علی رغم مشکلات کار با ASN.1 بسیاری از کابردهای ساخته شده فرض گردید که آن فرمت کد گذاری می باشد.امروزه بسیاری از این کاربردها پشت سر گذاشته شده و توجهات روی XML به عنوان راه حلی برای نمایش دیتا بدون بستگی به Platform می باشد.اما گواهی نامه کلید عمومی هنوز به روش ASN.1 کد گزاری می شود.

عناصر ASN.1 شامل نوع ،طول و مقدار می باشد.چندین نوع پایه تعیین گردیده اند .آنها شامل زنجیره بیت ، هشت تایی [1] زنجیره Character وBooleans 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[2] (BER) و روش تشخیص داده کد[3] (DER)مورد استفاده می باشند.با BER تکه های یکسانی از دیتا می توانند از چندین راه مختلف نمایش داده شوند. این آنالوگ به1و1.0 و1.00 همه به یک مقدار نشان داده 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.

[1] Octets

[2] Basic encoding Rules

[3] Distinguished Encoding Rules

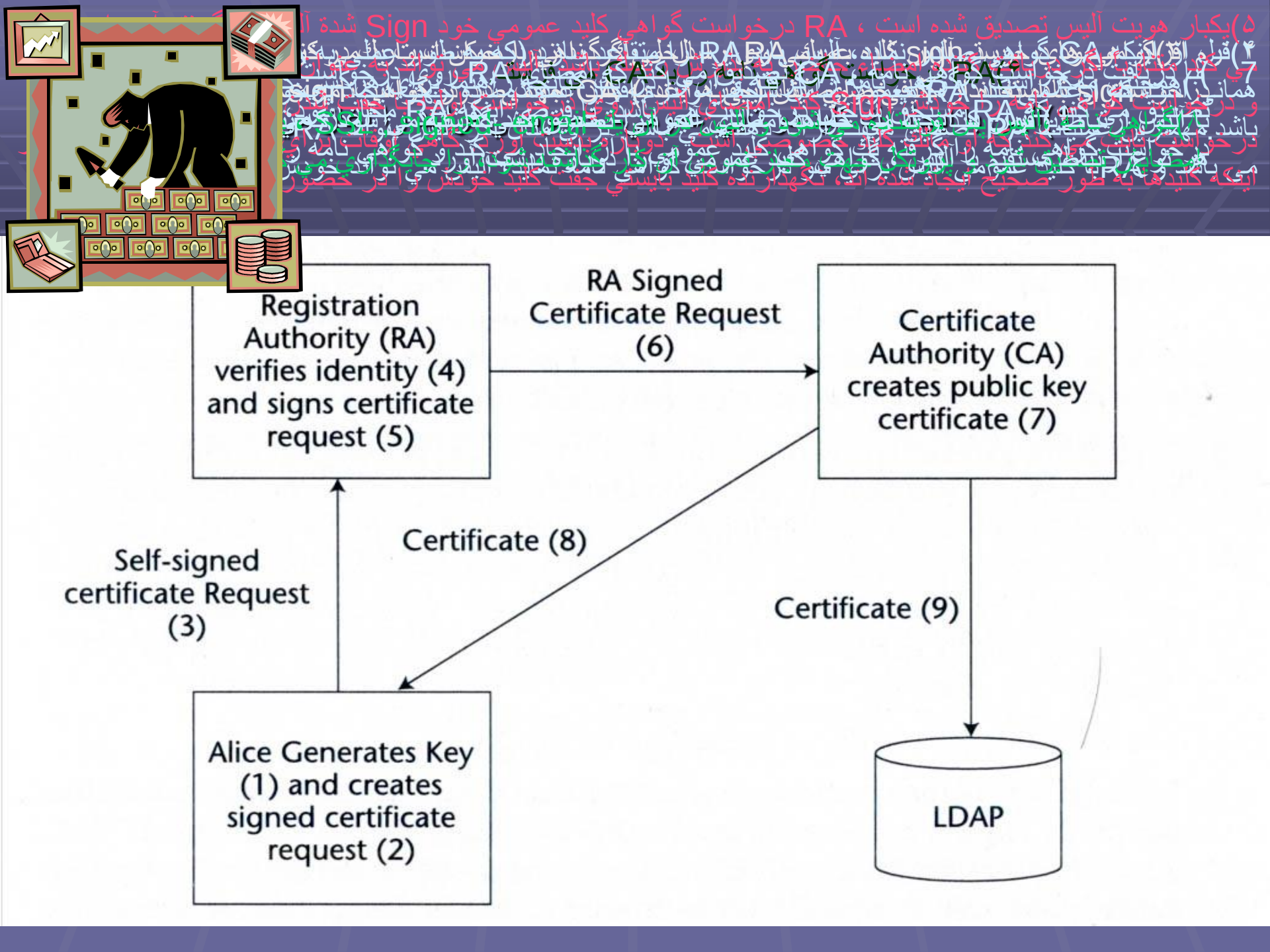


زیرساخت کلید عمومی

گواهي نامه هاي كليد عمومي به وجود يك زيرساخت مديريتي جهت پشتيباني ،توليد توزيع و فسخ گواهي نامه نياز دارد . اين زيرساخت، زيرساخت كليد عمومي[1] (PKI) ناميده مي شود. از آنجايي كه مديريت گواهي نامه اغلب به كليدها گره خورده ،PKI ها اغلب به خوبي شامل مديريت كليدها مي گردند. چندين اجزاي تركيبي براي PKI وجود دارد. CAكه قبلاً در موردش صحبت كرديم همچنين مي تواند سند نام نويسي[2] (RA) و يك كتابچه راهنما [3]باشد.

معمولاً بعلاوه اجزاي نرم افزاري يك جمله اجرايي گواهي نامه (CPS) وجود دارد كه عملكرد PKI، شاخص هاي امنيتي، 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.

[1] Public key Infrastructure
[2] Registration Authority
[3] Directory


Registration Authority (RA) verifies identity (4) and signs certificate request (5)
RA Signed Certificate Request (6)
Certificate Authority (CA) creates public key certificate (7)
Certificate (8)
Self-signed certificate Request (3)
Certificate (9)
Alice Generates Key (1) and creates signed certificate request (2)
LDAP

اگر بدلايلي كليدهاي آليس بدليل افتادن در دست كس ديگري ، به مخاطره بيافتد و يا گواهي نامه هاي او

بدليل تغيير يافتن به طور غير مقتضي ، به مخاطره بيافتند ، CA بايستي اعلام نمايد و گواهي آليس بايد لغو گردد. هنگامي كه CA اعلام نمايد كه گواهي ديگر معتبر نيست، اين گواهي نامه را به همراه تاريخ و زمان كه نشان ميدهد كي اعتبار گواهي نامه از بين رفته، داخل ليست گواهي نامه هاي لغو شده[1] (CRL) مي گذارد.

certificate revocation list [1]

در تئوري هر كس كه مي خواهد از كليد آليس استفاده كند بايستي قبل از استفاده از كليد به CA CRL او مراجعه نمايد. در عمل از آنجايي كه بيدا كردن كتابچه تبادلات كامل شده قبل از اين زمان قابل قبول فرض مي شود. تبادلات پس از اين تاريخ مي تواند مظنون واقع گردد. CA اين ليست را در فواصل معين ايجاد كرده و آنرا به كتابچه راهنماي كم حجم دسترسي پروتكل (LDAP) پست مي كند. كتابچه راهنمايي شكل گواهي نامه (بوشت Application [1] ساز مانايي سلسله مراتبي مي تواند گواهي نامه user را از كتابچه راهنما بدست آورده و اعتبار گواهي نامه را با كنترل كردن CA هاي CRL تصديق نمود.

[1] Light weigh Directory Access protocol

هدف اصلي PKI ها اين بود كه دستگاه سلسله مراتبي CA ها جهاني و منفرد باشند.

اگراعتبار CA مي توانست تصديق می شد حتي اگر دريافت كنندة گواهي نامه كليد عمومي به طور رسمي CA ويژه اي را نشناسد. واقعيت اين است كه بيشتر PKI ها به ديگر PKI ها بستگي ندارند . گواهي ها متقابل (يك CA براي CA ديگر معتبر نيست) گاهي اوقات وقتي كه افراد در PKI هاي مختلف بايد تبادل اطلاعات امني داشته باشند مورد استفاده قرار مي گيرد.

پایان