یا ذاالامن والامان

امنیت داده و شبکه

امضای رقمی و زیرساخت کلید عمومی

مرتضی امینی - نیمسال اول ۹۰-۸۹

مرکز امنیت شبکه شریف
http://nsc.sharif.edu

فهرست مطالب

- مبانی امضای رقمی
- استانداردهای امضای رقمی
- زیرساخت کلید عمومی (PKI)
  - مبانی PKI
  - گواهی رقمی و مدیریت آن
  - مولفه‌های PKI
  - معماری PKI، رویه‌ها و خط‌مشی‌ها

امضاء رقمی

- چرا به امضاء رقمی نیاز داریم؟

  - جعل توسط گیرنده: گیرنده می‌تواند یک پیام جعلی را بسازد (با استفاده از کلید توافق شده) و آنرا به فرستنده نسبت دهد!

  - انکار توسط فرستنده: فرستنده می‌تواند سناریوی فوق را بهانه قرار دهد و پیام فرستاده شده را منکر شود!

امضاء رقمی

- ویژگی‌ها:
  - امکان تصدیق هویت فرستنده، زمان و تاریخ ارسال
  - تضمین عدم تغییر محتویات پیام
  - امکان تصدیق توسط طرف سوم (در صورت بروز اختلاف)

امضاء رقمی

نیازمندی‌ها:

- رشته بیتی تولید شده وابسته به پیام اصلی باشد.
- از اطلاعات منحصر به فرستنده استفاده شود (جلوگیری از جعل و انکار)
- به سادگی محاسبه شود و فضای کمی برای ذخیره نیاز داشته باشد.
- تشخیص و تایید (verify) آن آسان باشد.
- جعل آن از نظر محاسباتی دست نیافتنی باشد.
- امضاء رقمی صرفا بر رمزنگاری نامتقارن (کلید عمومی) مبتنی است. در واقع برای پشتیبانی از سرویس عدم انکار، فرستنده و گیرنده نمی‌توانند از یک کلید مشترک استفاده کنند.

امضاء رقمی

- **مولفه ها:**
  - الگوریتم تولید کلید (Key Generation Alg)
    - بصورت تصادفی یک زوج کلید عمومی تولید می‌کند.
  - الگوریتم تولید امضاء (Signature Alg)
    - پیام و کلید خصوصی فرستنده را به عنوان ورودی می‌گیرد و امضاء را تولید می‌کند.
  - الگوریتم تایید امضاء (Signature Verification Alg)
    - امضاء و کلید عمومی فرستنده را به عنوان ورودی می‌گیرد و تاییدیه امضاء را به عنوان خروجی برمی‌گرداند.

امضاء رقمی

- مستقیم (Direct)
  - فقط دو طرف ارتباط دخیل هستند.
  - ضعف: به امنیت کلید خصوصی فرستنده وابسته است.
    - فرستنده می‌تواند ارسال پیام را انکار کند.
    - استفاده از مُهر زمانی (timestamp) به تنهایی کافی نیست. ممکن است در زمان T، کلید خصوصی فرستنده لو رفته باشد.
    - در این صورت مهاجم می تواند برای قبل از زمان T پیام جعل کند.
- باواسط (Arbitrated)
  - وجود یک سوم شخص مشکل تعلق پیام به فرستنده را برطرف می‌کند.
  - امکان مراجعه به شخص سوم، در صورت بروز اختلاف

امضای رقمی با واسطه

سناریوی ۱: رمزنگاری متقارن، پیام برای واسط آشکار است.

(1) $X \rightarrow A: M \| E(K_{xa}, [ID_X \| H(M)])$

(2) $A \rightarrow Y: E(K_{ay}, [ID_X \| M \| E(K_{xa}, [ID_X \| H(M)]) \| T])$

سناریوی ۲: رمزنگاری متقارن، پیام از دید واسط مخفی است.

(1) $X \rightarrow A: ID_X \| E(K_{xy}, M) \| E(K_{xa}, [ID_X \| H(E(K_{xy}, M))])$

(2) $A \rightarrow Y: E(K_{ay}, [ID_X \| E(K_{xy}, M)]) \| E(K_{xa}, [ID_X \| H(E(K_{xy}, M)) \| T])$

سناریوی ۳: رمزنگاری کلید عمومی، پیام از دید واسط مخفی است.

(1) $X \rightarrow A: ID_X \| E(PR_x, [ID_X \| E(PU_y, E(PR_x, M))])$

(2) $A \rightarrow Y: E(PR_a, [ID_X \| E(PU_y, E(PR_x, M)) \| T])$

امضاء رقمی

- ضعف سناریوی اول:
  - عدم رعایت محرمانگی پیغام
  - امکان تبانی واسط با فرستنده یا گیرنده
- ضعف سناریوی دوم:
  - امکان تبانی واسط با فرستنده یا گیرنده
- مزایای سناریوی سوم:
  - نیاز به هیچ توافقی قبل از ارتباط نیست.
  - در صورت لو رفتن کلید خصوصی x، برچسب زمانی درست است.
  - متن پیام در معرض دید واسط یا شخص دیگر نیست.

فهرست مطالب

- مبانی امضای رقمی
- **استانداردهای امضای رقمی**
- زیرساخت کلید عمومی (PKI)
  - مبانی PKI
  - گواهی رقمی و مدیریت آن
  - مولفه‌های PKI
  - معماری PKI، رویه‌ها و خط‌مشی‌ها

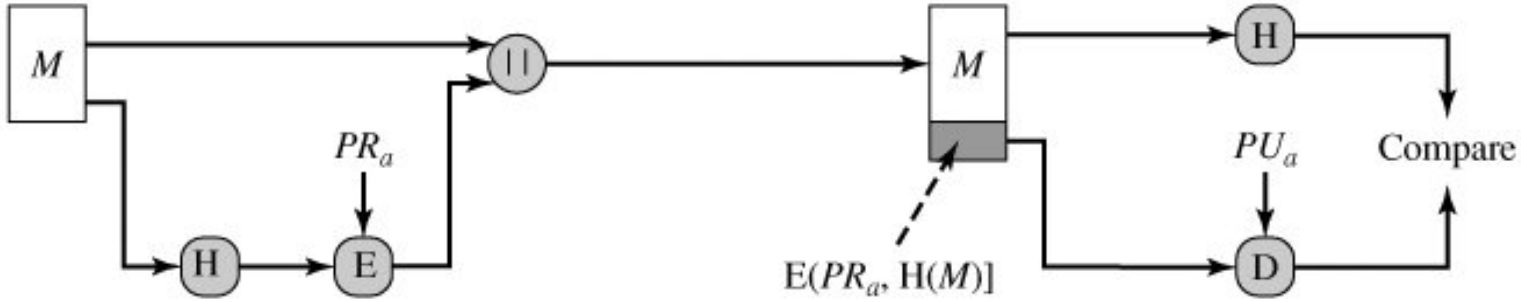
استانداردهای امضاء رقمی

- DSS : استانداردشده توسط NIST FIPS 186
  - مشهورترین استاندارد امضاء رقمی محسوب می‌شود.

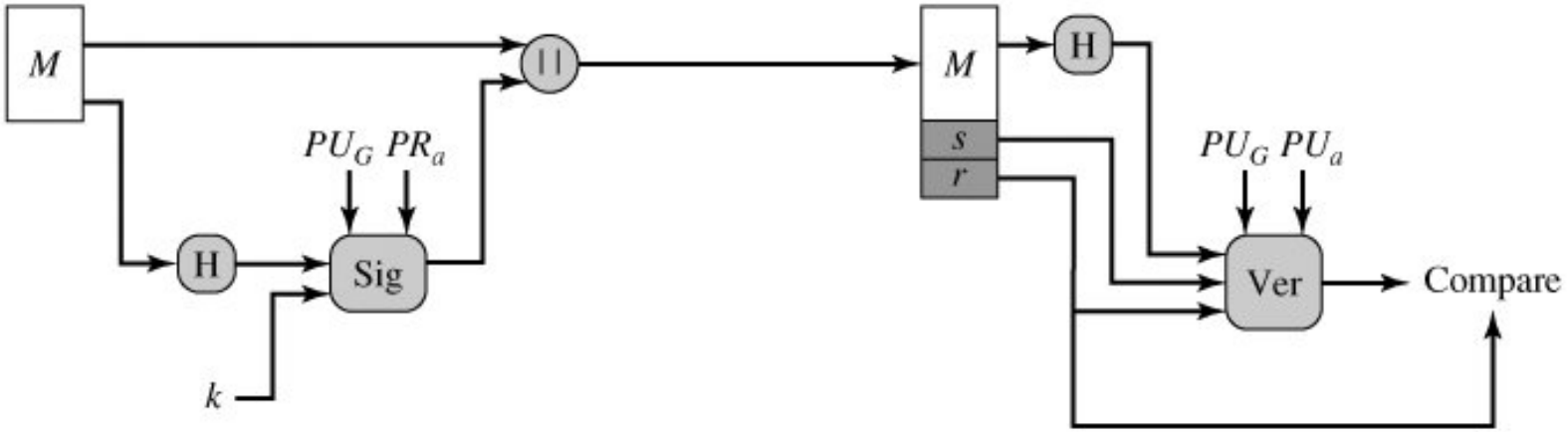
- RSA Digital Signature: استاندارد شده توسط
  - ISO 9776
  - ANSI X9.31
  - CCITT X.509

DSS در قیاس با RSA

امضای دیجیتال RSA



امضای دیجیتال DSS



استاندارد امضاء رقمی DSS

- ویژگیهای DSS
  - پذیرفته شده توسط NIST به عنوان استاندارد امضاء رقمی
  - استفاده از الگوریتم SHA برای تولید چکیده پیام
  - استفاده از الگوریتم DSA و کلید خصوصی فرستنده برای رمزکردن چکیده تولید شده
  - عدم پشتیبانی از رمزنگاری و تبادل کلید (در مقایسه با RSA)
  - سرعت اجرای DSA از RSA کمتر است.
  - امنیت آن به دشوار بودن محاسبه لگاریتم‌های گسسته مرتبط است.

استاندارد امضاء رقمی

- پارامترهای الگوریتم

- **p,q,g:** global public-key components
- **x:** user private key (a random such that 0<x<q)
- **y:** user public key ($y= g^x \bmod p$)
- **k:** user per-message secret (a random such that 0<k<q)

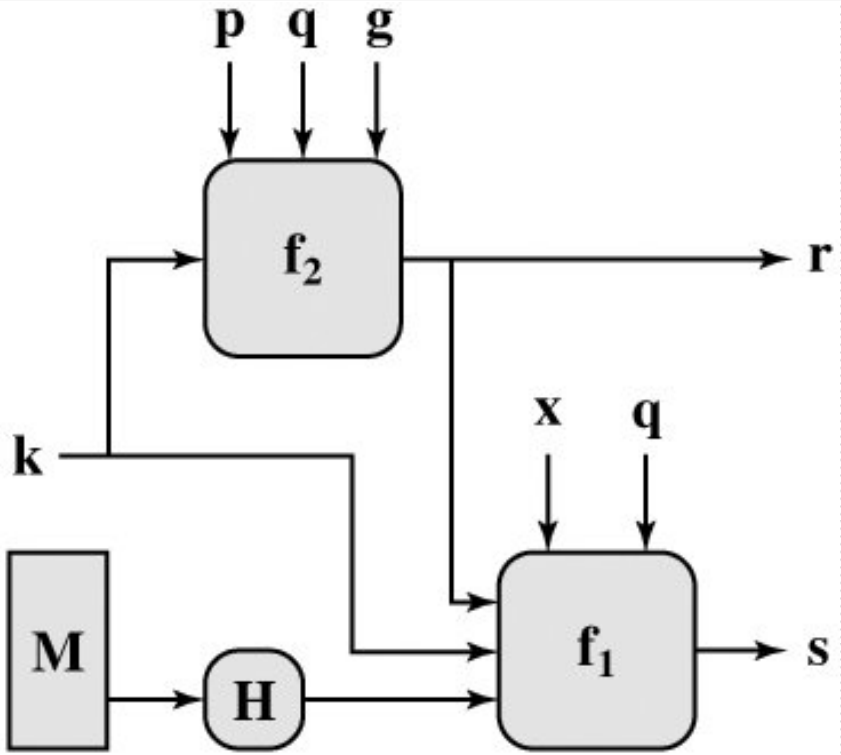
- $r = (g^k \bmod p) \bmod q$
- $s = [k^{-1}(H(M) + xr)] \bmod q$
- **Signature = (r, s)**

استاندارد امضاء رقمی

الگوریتم تولید امضاء

- تولید یک کلید تصادفی k، که باید بعد از یکبار استفاده از بین رفته و دیگر مورد استفاده قرار نگیرد.
- سپس زوج مرتب امضاء (r,s) بصورت زیر محاسبه می‌شوند:
  - $r = (g^k \bmod p) \bmod q$
  - $s = [k^{-1}(H(M) + xr)] \bmod q$
    - H(M) : مقدار درهم تولید شده از M با استفاده از الگوریتم SHA-1
- (r,s) به پیام M الحاق شده و فرستاده می‌شود.

فرآیند امضاء در DSS



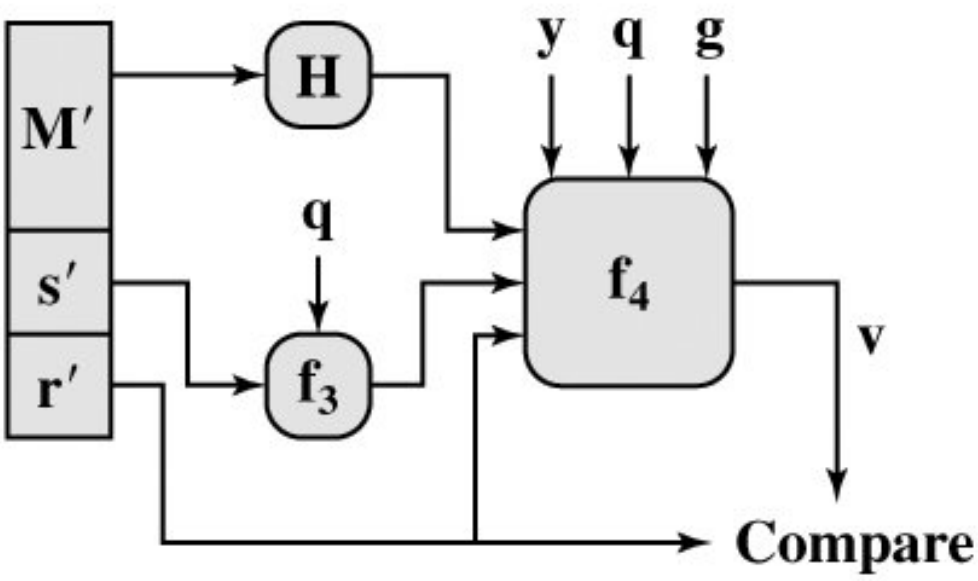
$$s = f_1(H(M), k, x, r, q) = (k^{-1} (H(M) + xr)) \bmod q$$

$$r = f_2(k, p, q, g) = (g^k \bmod p) \bmod q$$

استاندارد امضاء رقمی

- تصدیق امضاء
  - گیرنده M’ و (r’,s’)را دریافت می کند.
  - مقادیر زیر را محاسبه می کند:
    - $w = (s')^{-1} \bmod q$
    - $u1 = [H(M')w] \bmod q$
    - $u2 = [(r')w] \bmod q$
    - $v = [(g^{u1}y^{u2}) \bmod p] \bmod q$
  - اگر v=r’ ، امضاء معتبر است.

فرآیند وارسی امضاء در DSS



$$w = f_3(s', q) = (s')^{-1} \bmod q$$

$$v = f_4(y, q, g, H(M'), w, r')$$

$$= ((g^{(H(M')w) \bmod q} y^{r'w \bmod q}) \bmod p) \bmod q$$

استاندارد امضاء رقمی

- نکاتی درباره الگوریتم:
  - مقدار r مستقل از پیام محاسبه می‌شود.
    - به k و ۳ پارامتر عمومی بستگی دارد.
  - محاسبه k از روی r یا محاسبه x از روی s از نظر محاسباتی دست نیافتنی است.
    - دشواری محاسبه لگاریتم های گسسته
  - الگوریتم امضاء سریع است، چون خیلی از مقدارها از پیش قابل محاسبه هستند.

استاندارد امضاء رقمی

- دلایل امنیت DSA
  - کلید خصوصی x هیچ‌گاه فاش نمی‌شود.
  - امکان جعل امضاء بدون داشتن x میسر نیست.
  - امکان ایجاد پیام دیگری که با امضاء مطابق باشد، نیست.
  - استفاده از کلید سری جدید k برای هر پیام.

فهرست مطالب

- مبانی امضای رقمی
- استانداردهای امضای رقمی
- **زیرساخت کلید عمومی (PKI)**
  - **مبانی PKI**
  - گواهی رقمی و مدیریت آن
  - مولفه‌های PKI
  - معماری PKI، رویه‌ها و خط‌مشی‌ها

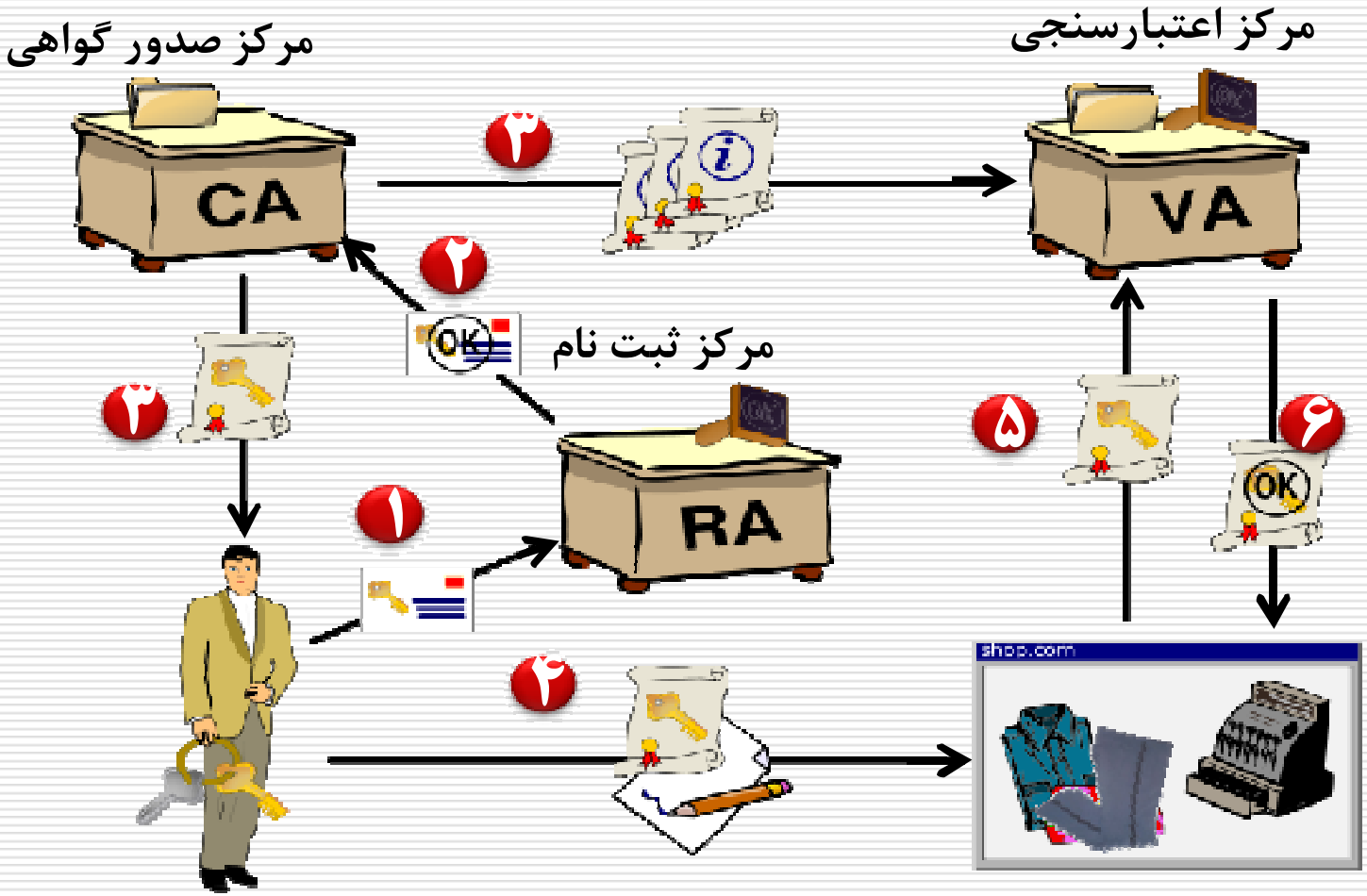
مبانی PKI

- نکته اصلی در رمزنگاری نامتقارن:

  "چه کسی کلید خصوصی متناظر با یک کلید عمومی را دارد؟"

- در پاسخ به یک پیام، باید مطمئن بود که دریافت‌کننده همان است که مورد نظر ما است.
- برای هر کلید عمومی باید یک گواهی از یک مرجع معتبر وجود داشته باشد که متضمن تعلق آن به یک فرد باشد.
- بنابراین نیاز به زیرساختی برای صدور گواهی و وارسی آن داریم که زیرساخت کلید عمومی (PKI) نام دارد.

PKI در یک نگاه



فهرست مطالب

- مبانی امضای رقمی
- استانداردهای امضای رقمی
- **زیرساخت کلید عمومی (PKI)**
  - مبانی PKI
  - **گواهی رقمی و مدیریت آن**
  - مولفه‌های PKI
  - معماری PKI، رویه‌ها و خط‌مشی‌ها

گواهی ایده‌آل

- **ویژگی‌ها:**

۱- شیئی دیجیتالی باشد که توزیع آن ساده باشد.

۲- حاوی نام و مشخصات کاربری که دارنده کلید خصوصی متناظر است، باشد.

۳- تاریخ تولید گواهی را دارا باشد.

گواهی ایده‌آل

۴- صادرکننده گواهی معتبر باشد.

۵- گواهی صادره بین گواهی‌های تولید شده توسط صادرکننده، منحصر بفرد باشد.

۶- منقضی نشده باشد.

۷- اطلاعات گواهی قابل تغییر و جعل نباشد.

۸- به سرعت بتوان اعلام کرد که منبع گواهی معتبر نیست.

۹- ذکرشده باشدکه گواهی به چه کاربردهایی تناسب دارد.

گواهی کلید عمومی

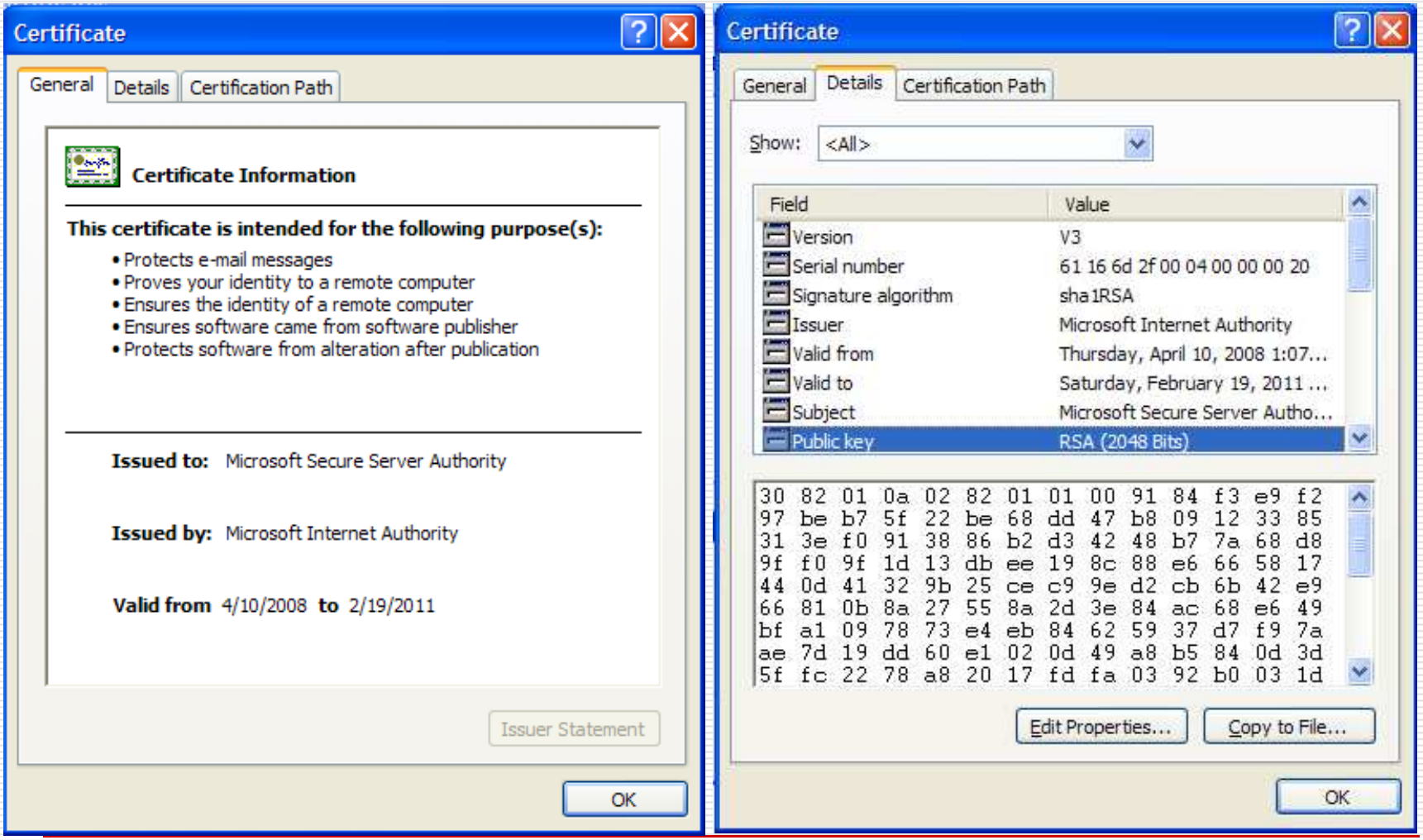
- گواهی (Certificate) مستند رسمی برای تضمین تعلق شناسه به کلید عمومی.
- گواهی به وسیله یک مرکز مطمئن (CA) امضا، شده است.

Certificate:= (Public Key, ID, $E(PR_{CA}$,Certificate-Signature))

گواهی کلید عمومی

- صحت گواهی به راحتی قابل کنترل است. هر تغییری در آن به سادگی کنترل می‌شود.
- ارسال و ذخیرهٔ گواهی به شکل رمز نشده.
- برای وارسی گواهی به کلید عمومی CA نیاز داریم.
- تقریبا همگی مشخصات گواهی ایده‌آل در گواهی کلید عمومی وجود دارد.

گواهی کلید عمومی



عدم اعتبار گواهی

- دلایل ابطال گواهی:
  - تغییر شغل،
  - گم شدن و یا لو رفتن کلید خصوصی،
  - عدم تبعیت از سیاستهای مرکز صدور گواهی توسط کاربر
- نیاز به تغییر کلید عمومی، ضرورت اطمینان از اطلاع همه دنیا از این تغییر.

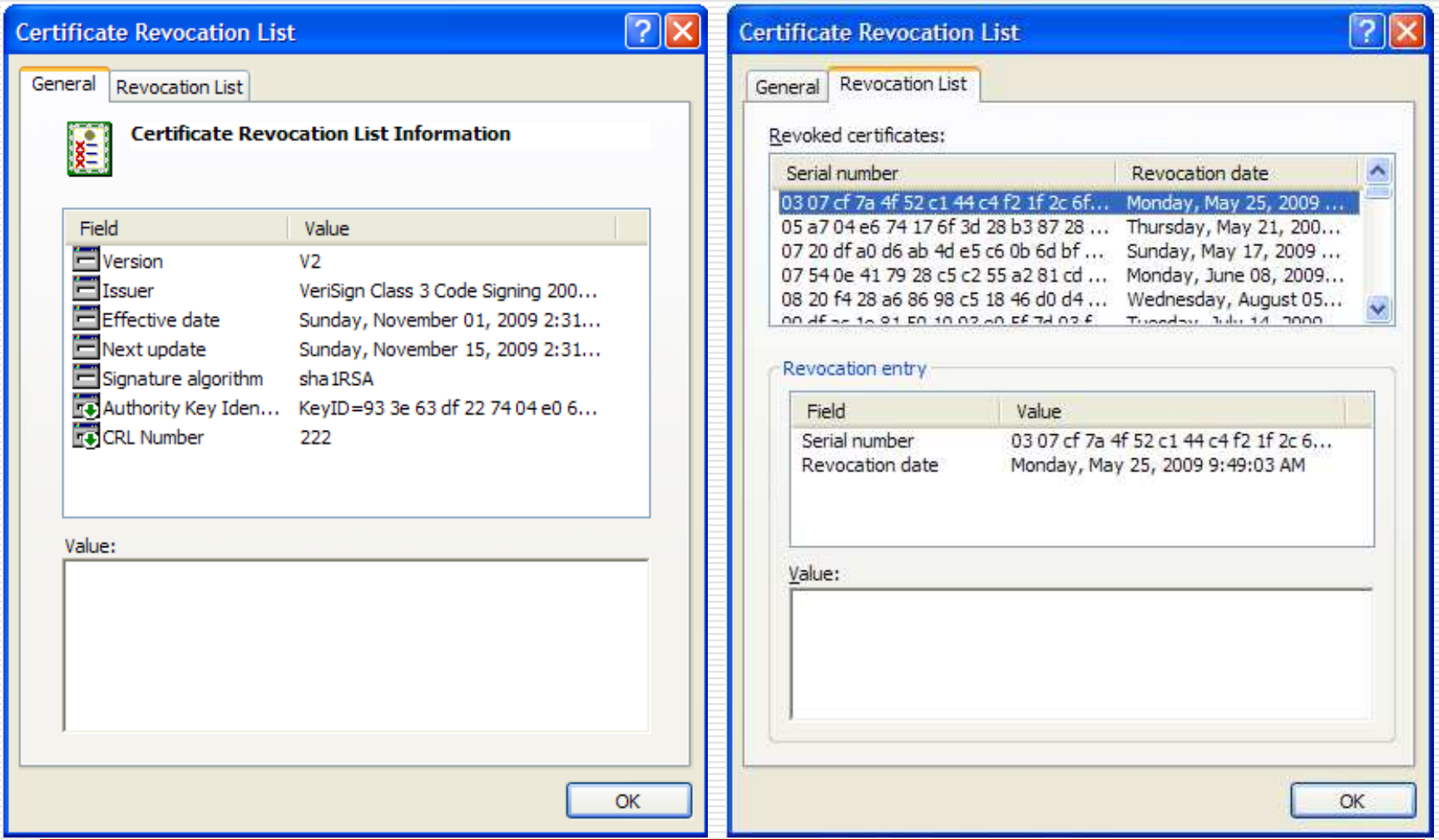
عدم اعتبار گواهی

- **دو رویکرد:**
  - هرکس هرگاه کلید عمومی خواست از مرکز مورد اعتماد درخواست کند.
  - با گم شدن، تغییر و یا لو رفتن کلید خصوصی لیستی از گواهی‌های منقضی نشده بی‌اعتبار به همگان منتشر شود .
- به طور معمول برای اعلام عدم اعتبار گواهی از لیست گواهی‌های نامعتبر(CRL) استفاده می‌شود.
  (**CRL**: Certificate Revocation List)
- تاریخ انقضاء، شماره سریال گواهی‌های نامعتبر، به همراه امضاء صادرکننده در لیست گواهی نامعتبر (**CRL**) وجود دارد.

انواع CRL

- **Full CRL** در دوره‌های زمانی مشخص یک CA لیست کامل گواهی‌های نامعتبر را منتشر می‌کند.
- **Delta CRL** اختلاف اخیرترین بروز رسانی و CRL جدید.

عدم اعتبار گواهی



نسخه‌برداری و بازیابی کلید

- کلید ممکن است گم شود! داده‌ها غیر قابل دسترس می‌شوند. باید مرکزی برای بازیابی کلید وجود داشته باشد.

- دو دلیل برای نسخه‌برداری کلید
  - فراموشی کلمهٔ رمز: نابودی داده‌های حساس. حتی رمز نکردن به خاطر ترس از گم‌شدن کلمهٔ رمز وجود دارد.
  - گم شدن، دزدیده شدن، و یا خرابی رسانه‌ای که کلیدها روی آن ذخیره شده است.

نسخه‌برداری و بازیابی کلید

- عدم انکار دلیلی بر عدم نسخه‌برداری کلید
  - انکار یعنی اعلام عدم دخالت در یک تراکنش.
    - در فرم کاغذی: امضای دستی این کار را کنترل می‌کند.
    - در فرم الکترونیکی: امضای رقمی.
  - عدم انکار مستلزم تولید و ذخیرهٔ امن کلید امضاء در محدوده تحت کنترل کاربر (در همه حالات) است و لذا نباید از آن پشتیبان گرفت.
  - از نظر فنی هم ضرورت ندارد چرا که یک زوج کلید دیگر تولید و استفاده می‌شود.

گواهی های هر کاربر

- بنابراین دو زوج کلید برای هر کاربر لازم است.
  - **زوج کلید امضاء:** عدم نیاز به پشتیبان
  - **زوج کلید رمزنگاری:** نیازمند پشتیبان‌گیری

مدیریت سابقهٔ کلیدها

- نباید کلیدها ابدی باشند. پس باید:
  - کلیدها را بروز آورد.
  - سابقه زوج کلیدهای (رمزنگاری) قبلی را نگه داشت تا داده‌های رمز شده با زوج قبلی قابل رمزبرداری باشند. این کار توسط نرم‌افزار طرف کارفرما انجام می‌شود.
  - بروزآوری کلید باید قبل از انقضاء صورت پذیرد.
  - در نقطه مقابل برای بروزرسانی کلیدهای امضاء باید کاملا کلید فعلی را نابود کرد!

فهرست مطالب

- مبانی امضای رقمی
- استانداردهای امضای رقمی
- **زیرساخت کلید عمومی (PKI)**
  - مبانی PKI
  - گواهی رقمی و مدیریت آن
  - **مولفه‌های PKI**
  - معماری PKI، رویه‌ها و خط‌مشی‌ها

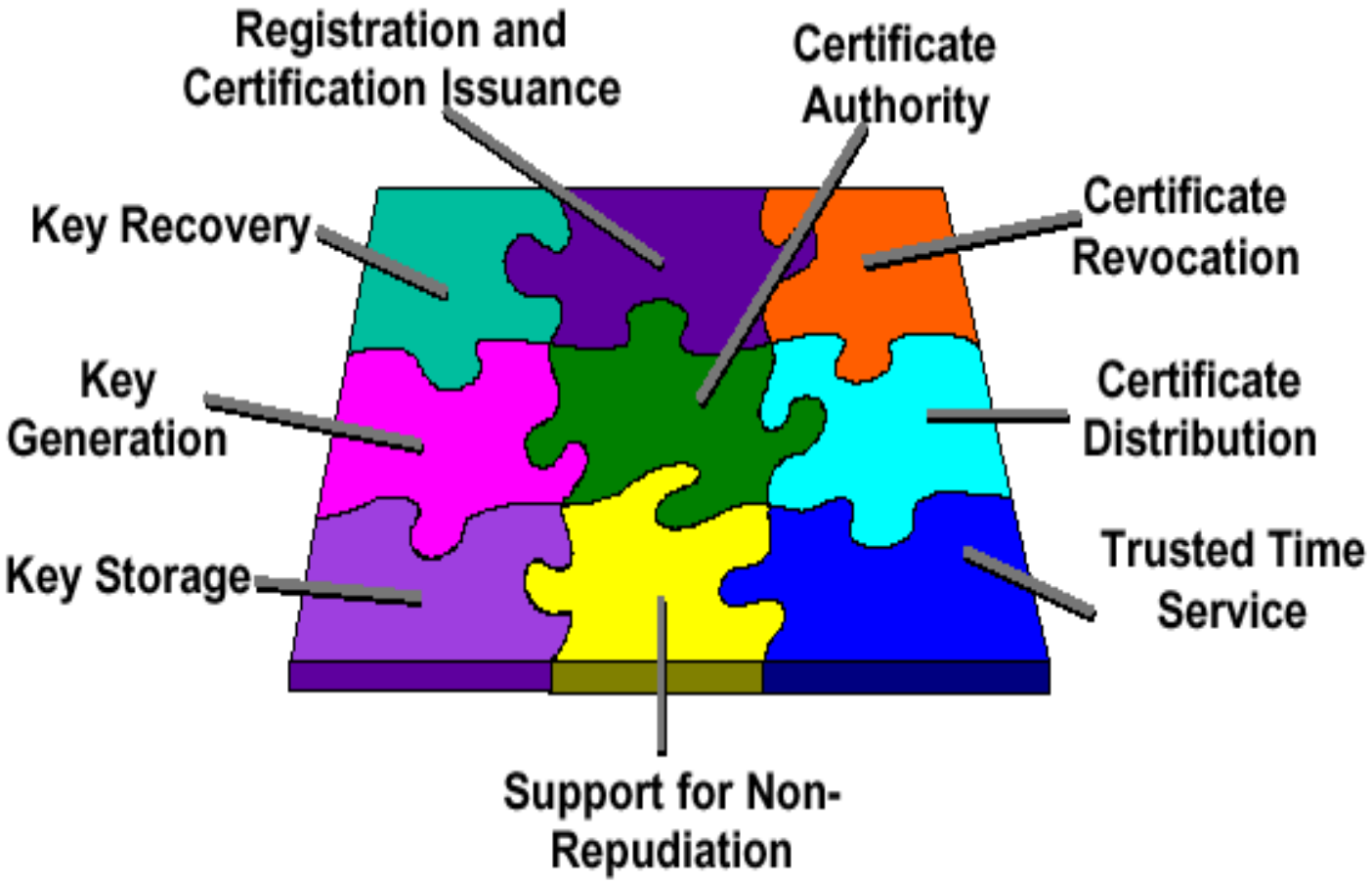
مؤلفه‌های PKI

- کاربران یا دارندگان گواهی (End Users or Certificate Holders):
  کاربران انسانی، تجهیزات و هر آنچه که می‌تواند از گواهی استفاده نماید.
- مرکز گواهی CA (Certificate Authority): مسئول تولید، مدیریت، توزیع گواهی و CRL.
- مرکز ثبت نام RA (Registration Authority): مسئول دریافت درخواست گواهی و کنترل محتوای گواهی و اطمینان از تعلق به دارنده آن.
- انباره (Repository): توزیع گواهی‌ها و CRLها (حداکثر کارآیی و دسترس پذیری را لازم دارد).
- آرشیو (Archive): انباره طولانی‌مدت و امن برای آرشیو اطلاعات.

مرکز گواهی CA

- به عنوان آژانس اعتماد در PKI است و لذا طرف سوم امن نامیده می‌شود.
- مجموعه‌ای از سخت افزار، نرم افزار، و اپراتورها.
- با دو صفت شناخته می‌شود: نام و کلید عمومی.

اجزای تشکیل دهنده CA



وظایف CA

- صدور گواهی (تولید و امضاء) به کاربران و یا دیگر CAها.
- نگهداری وضعیت گواهی‌ها و صدور CRL.
- انتشار گواهی‌ها و CRL موجود.
- نگهداری آرشیو اطلاعات وضعیتی از گواهی‌های صادره منقضی یا ابطال شده، به منظور تعیین اعتبار گواهی‌ها پس از انقضاء.

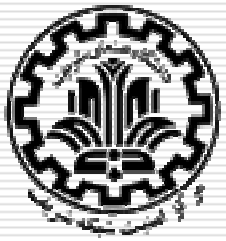
صدور گواهی

- تأیید اینکه فاعل (دارنده گواهی) کلید خصوصی متناظر با کلید عمومی موجود در گواهی را دارد.
- اگر کلید خصوصی CA لو برود، همه گواهی‌های صادره‌اش در معرض شک است.
- پس اولین وظیفه CA حفاظت از کلید خصوصی خودش است، حتی وقتی درحال پردازش است.
- وظیفه دیگر CA اطمینان از درستی گواهی و درستی ادعای درخواست‌کننده گواهی است.

مرکز ثبت نام RA

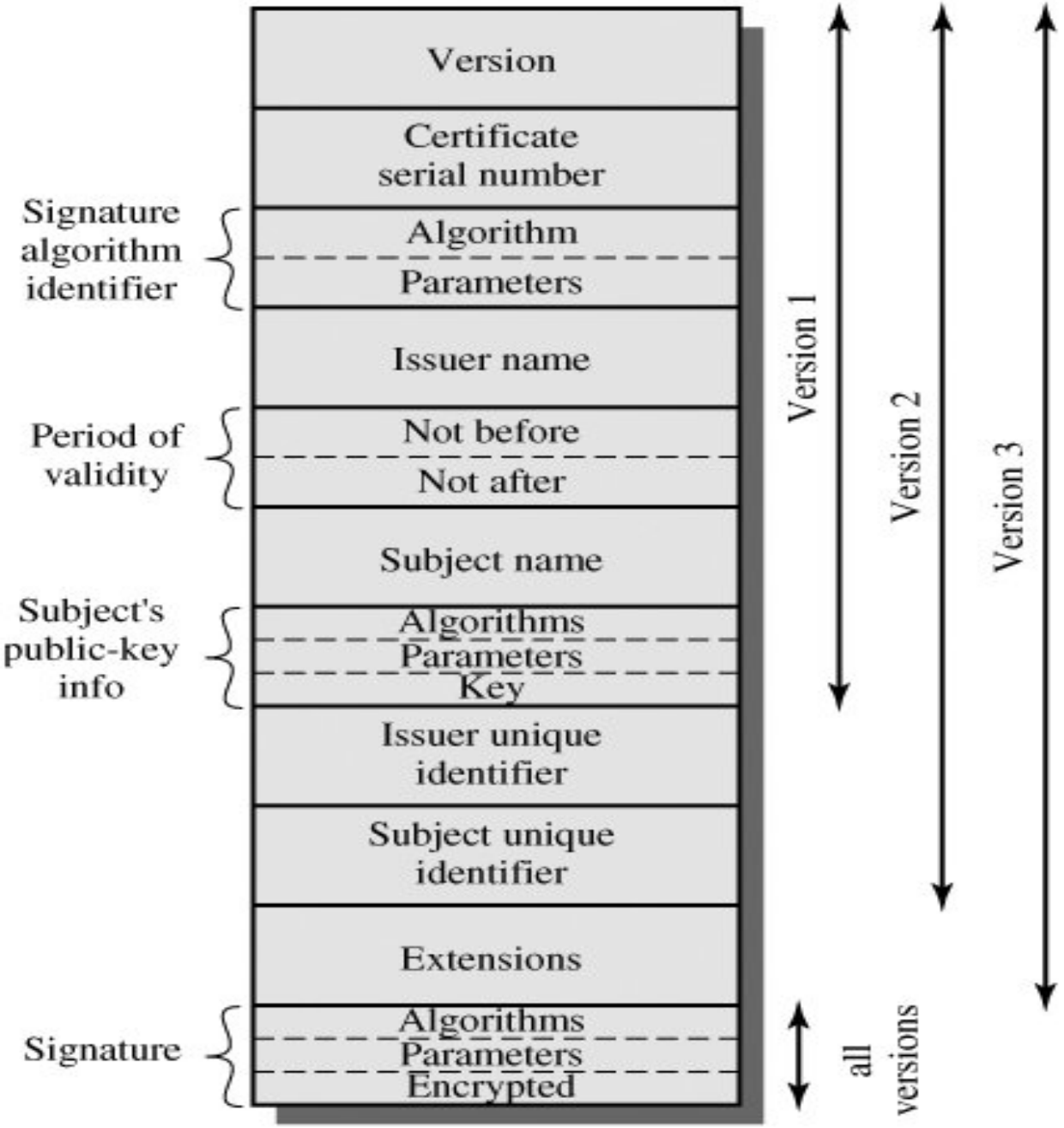
- RA قبل از ارائه در خواست به CA اطلاعات لازم را جمع‌آوری و کنترل می‌کند: مراجعه شخص، احراز هویت.
- اگر قبلاً زوج کلید تولید کرده باشد که همان به CA ارسال می‌شود.
- در غیر این صورت RA و (یا CA) می تواند زوج کلید لازم را در حضور متقاضی تولید نمایند.

X.509

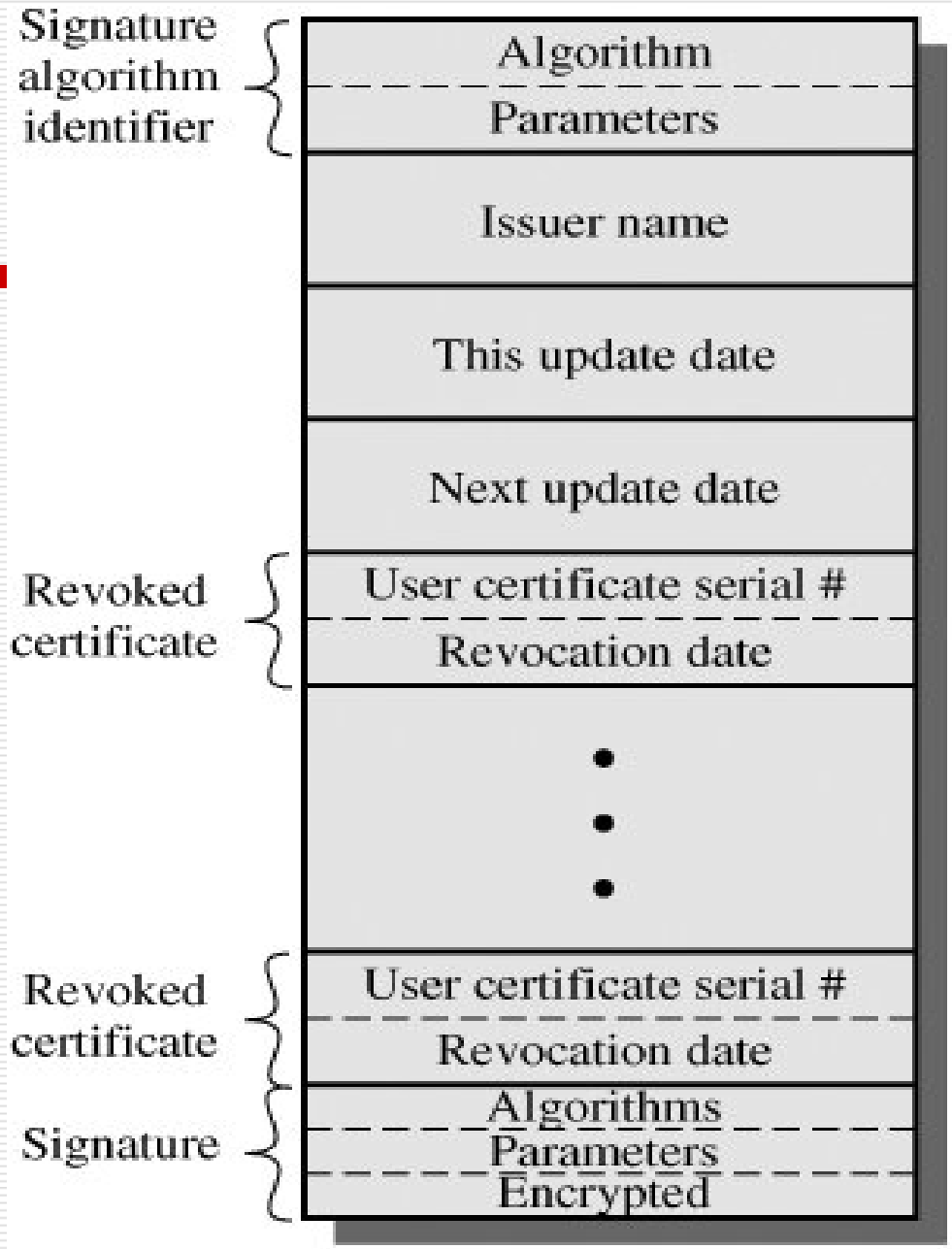


- محصول ITU-T و بخشی از توصیه‌های سری X.500
- گواهی X.509 در S/MIME ، IPSec، SSL/TLS و SET استفاده شده است.
- <<A>> CA به معنای گواهی صادره CA برای کاربر A است.
- همه کاربران در محدودهٔ یک CA: وجود اعتماد مشترک و امکان وارسی گواهی صادره.

ساختار گواهی رقمی X.509



ساختار CRL در X.509



فهرست مطالب

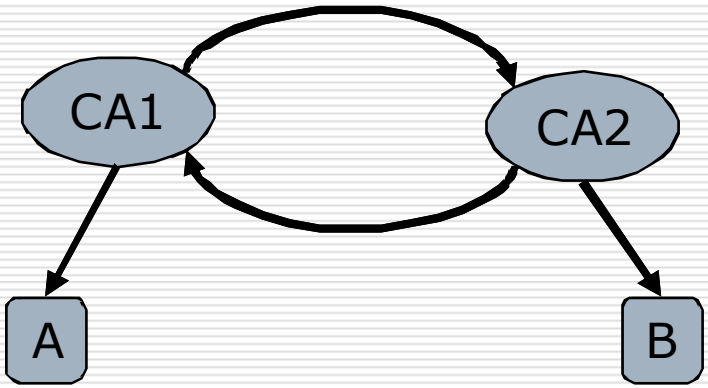
- مبانی امضای رقمی
- استانداردهای امضای رقمی
- **زیرساخت کلید عمومی (PKI)**
  - مبانی PKI
  - گواهی رقمی و مدیریت آن
  - مولفه‌های PKI
  - **معماری PKI، رویه‌ها و خط‌مشی‌ها**

معماری PKI

- مادام که دارندگان گواهی از یک CA گواهی گرفته باشند مسأله ساده است.
- وقتی که دارندگان گواهی از CAهای مختلف گواهی گرفته باشند چگونه اعتماد کنند؟
- معماری ساده PKI
  - تنها یک CA در سازمان گلوگاه و Single point of failure هرگونه اشکال منجر به لطمه دیدن اعتماد و احتمالاً صدور مجدد گواهی‌ها.

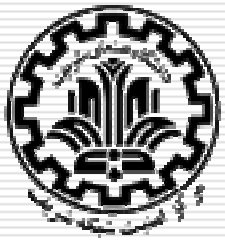
گواهی ضربدری (Cross-Certificate)

- گواهی ضربدری، گواهی‌ای است که یک CA برای CA دیگر صادر می‌کند تا گواهی‌های صادره توسط CA دوم توسط کاربران CA اول معتبر شناخته شوند.
- با فرض صدور گواهی A و B توسط دو CA مختلف CA1 و CA2:



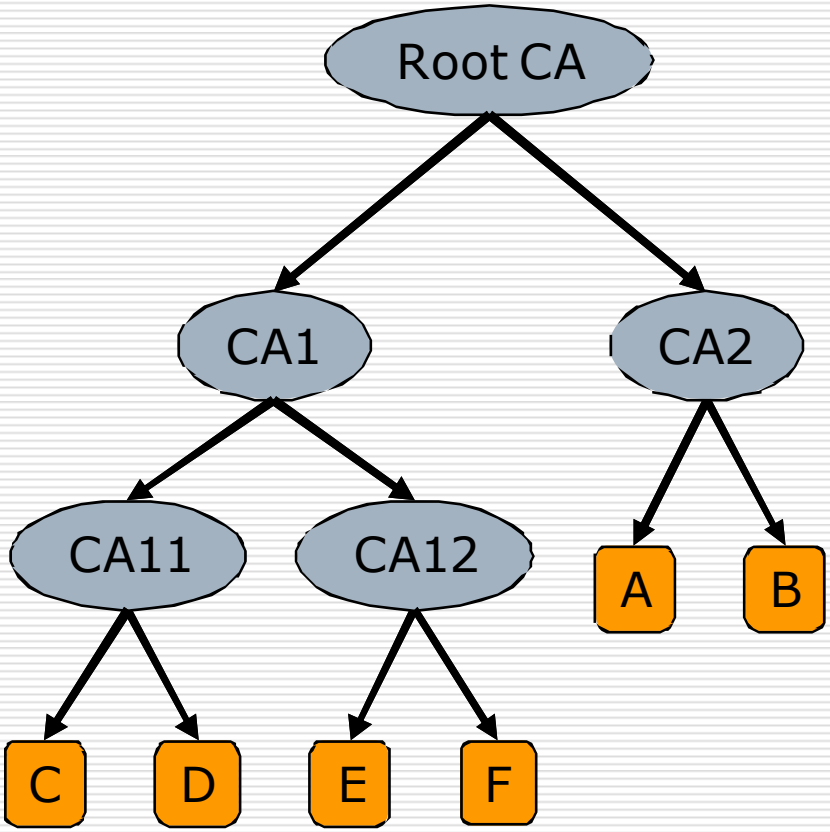
- CA1 <<CA2>> CA2 <<B>>
- CA2 <<CA1>> CA1 <<A>>

Enterprise PKI



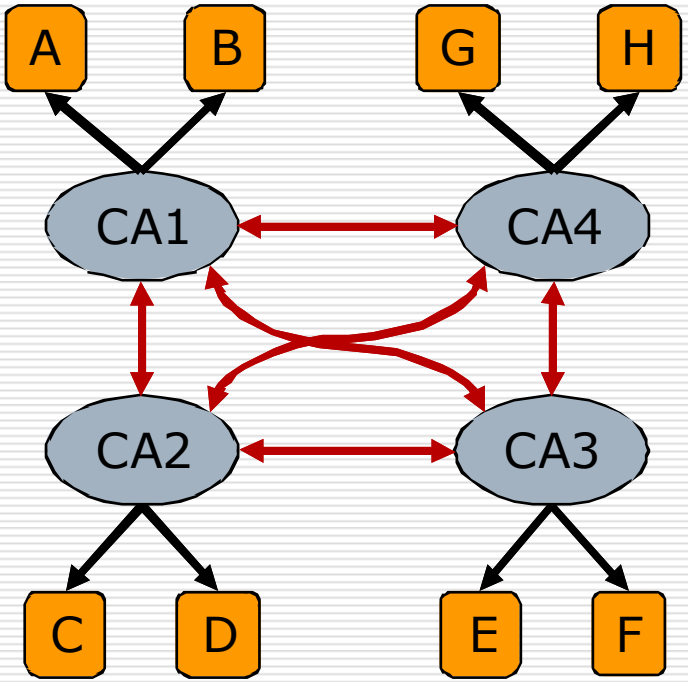
- دومعماری مختلف برای PKI بزرگ
  - سلسله مراتبی: در یک ساختار درختی
  - توری (Mesh): ارتباط کامل ضربدری CAها با یکدیگر
  - ترکیبی از دو مدل فوق: چند سلسله مراتب از CAها که ریشه آنها با یکدیگر ارتباط ضربدری دارند.

مدل سلسله مراتبی



- ساختار درختی از CAها
- CA ریشه و مجموعه‌ای CA میانی
- مزایا:
  - توزیع کار و کاهش ریسک
  - کاهش هزینه برقراری امنیت فیزیکی
    - صرفاً برای ریشه امنیت بالا نیاز است.
- معایب:
  - همه CAها را نمی توان در یک سلسله مراتب جای داد.

مدل توری

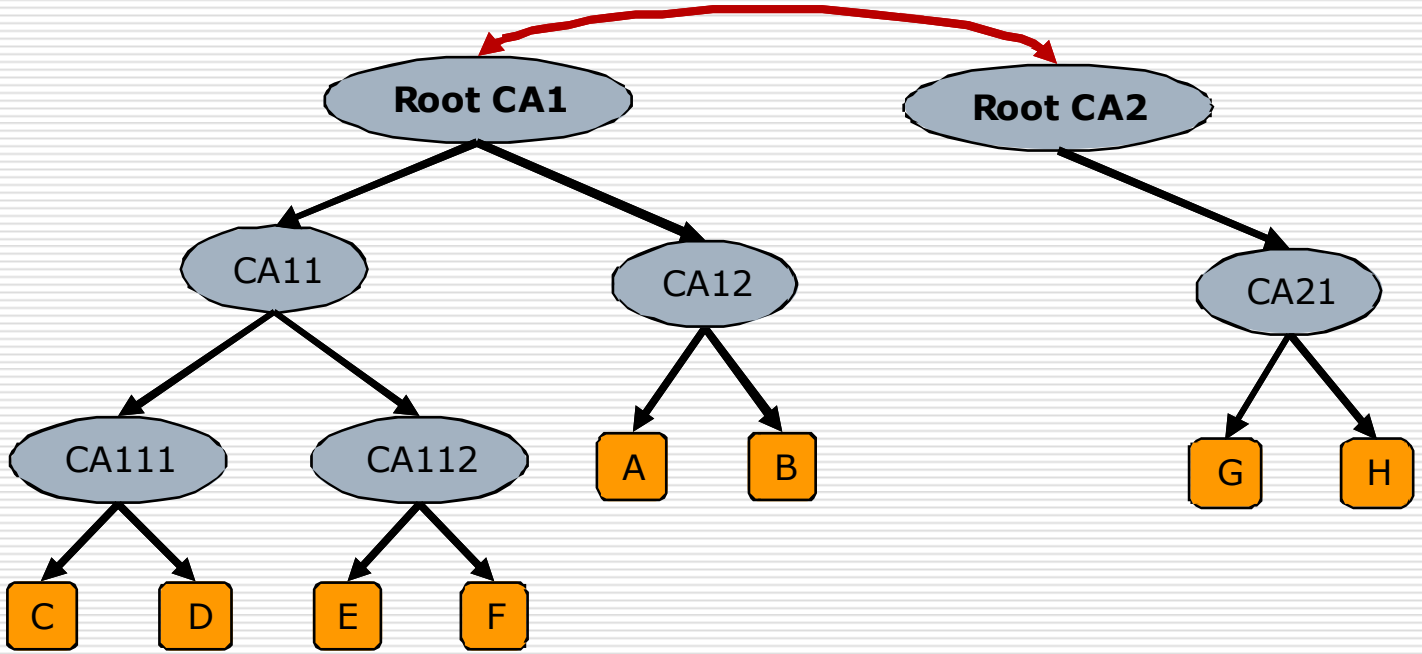


- هر دو CA به یکدیگر گواهی ضربدری بدهند.

- مزایا:
  - استقلال CAها از یکدیگر
- معایب:
  - نیاز به صرف منابع و هزینه زیاد

مدل ترکیبی

- ساختار درختی برای هر بخش
- ارتباط درختها با یکدیگر از طریق گواهی ضربدری در سطح ریشه



رویه‌ها و خط‌مشی‌ها

- برای داشتن PKI، وجود دو مستند ضروری است:
  - سیاست نامه گواهی رقمی (CP) Certificate Policy
  - آیین نامه اجرایی گواهی رقمی (CPS) Certificate Practices Statement
- این دو مستند قالب مشترک دارند ولی شنونده متفاوت و هدف متفاوتی دارند.
- استاندارد فعلی برای این دو مستند RFC 3647 است.

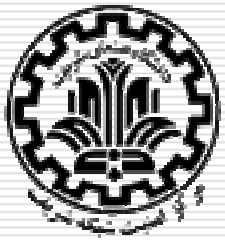
رویه‌ها و خط‌مشی‌ها

- CP یک مستند سطح بالا است که خط مشی امنیتی صدور گواهی و نگهداری اطلاعات گواهی را شرح می‌دهد.
  - شرح عملیات CA، مسئولیت های کاربر برای درخواست، استفاده، و مدیریت کلیدها و گواهی‌ها را دارد.
  - عمر این خطمشی از مرحله تولید تا انقضاء گواهی است.

- CPS مستندی است که مطابق با CP یک مرکز تدوین شده و نحوه اجرایی شدن CP را بیان می‌کند.

رویه‌ها و خط‌مشی‌ها

- علاوه بر CP و CPS در عمل مستندات دیگری نیز لازم است.
- مهم ترین این مستندات:
  - سند مراسم تولید کلید و گواهی مرکز
  - سند عملیات روزانه مرکز
  - سند سیاست نامه امنیتی



پایان

مرکز امنیت شبکه شریف

http://nsc.sharif.edu

پست الکترونیکی

m_amini@ce.sharif.edu