# امنیت داده و شبکه

امضای دیجیتال و زیرساخت کلید عمومی

# فهرست مطالب

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

# امضای دیجیتال

- چرا به امضاء دیجیتال نیاز داریم؟ زیرا در صورت استفاده از رمز متقارن:

  - 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!

# امضای دیجیتال

## ویژگی‌ها:

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

# امضای دیجیتال

## 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.
- امضای دیجیتال 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.

# امضای دیجیتال

- **مولفه‌ها:**
  - 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.

# فهرست مطالب

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

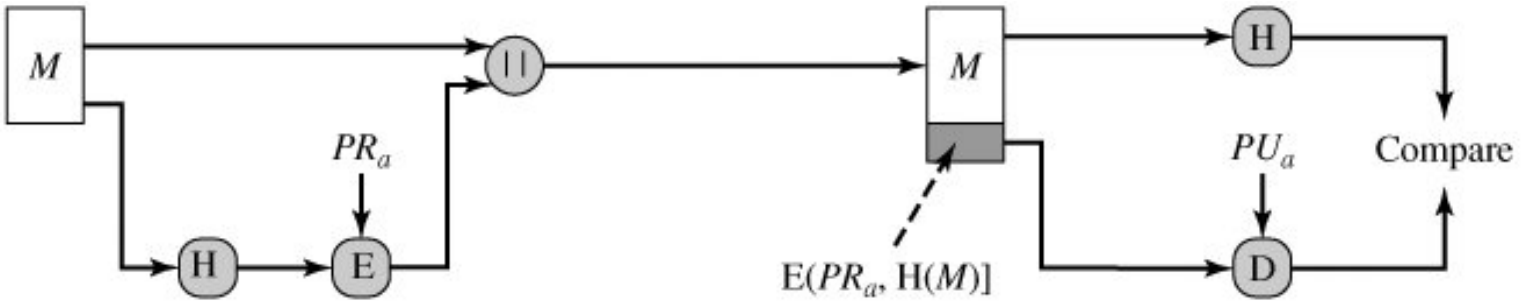
# استانداردهای امضای دیجیتال

- DSS : استانداردشده توسط NIST FIPS 186
  - مشهورترین استاندارد امضای دیجیتال محسوب می‌شود.

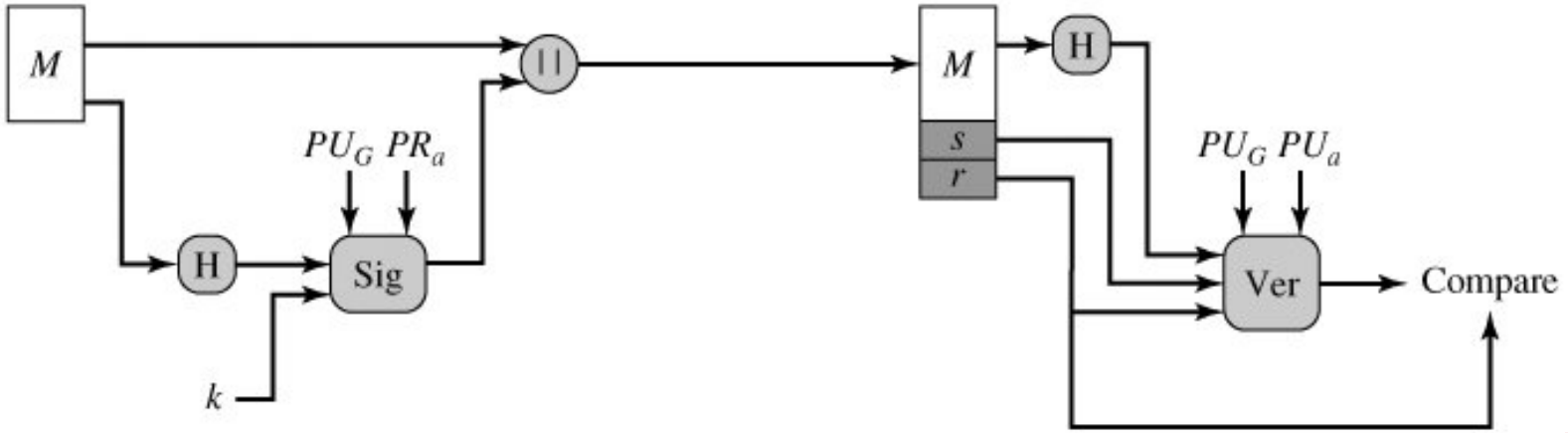
- RSA Digital Signature: استاندارد شده توسط
  - ISO 9776
  - ANSI X9.31
  - CCITT X.509

# DSS در قیاس با RSA

- امضای دیجیتال RSA




- امضای دیجیتال DSS



# استاندارد امضای دیجیتال DSS

- ویژگیهای DSS
  - پذیرفته شده توسط NIST به عنوان استاندارد امضاء دیجیتال
  - استفاده از الگوریتم SHA-1 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 امضای دیجیتال DSS

- پارامترهای الگوریتم
  - **p,q,g**: پارامترهای عمومی
    - p: عدد اول به طول L بیت ($2^{L-1}<p<2^{L}$)
    - q: عدد اول مقسوم‌علیه p-1 به طول N بیت ($2^{N-1}<q<2^{N}$)
  - **x**: کلید خصوصی کاربر (عددی تصادفی $0<x<q$ )
  - **y**: کلید عمومی کاربر ($y= g^{x} \bmod p$)
  - **k**: کلید مخفی به ازای هر پیام (عددی تصادفی $0<k<q$)
  - **$k^{-1}$**: معکوس k در پیمانه q ($k.k^{-1} \bmod q =1$)

طول p و q طبق استاندارد NIST

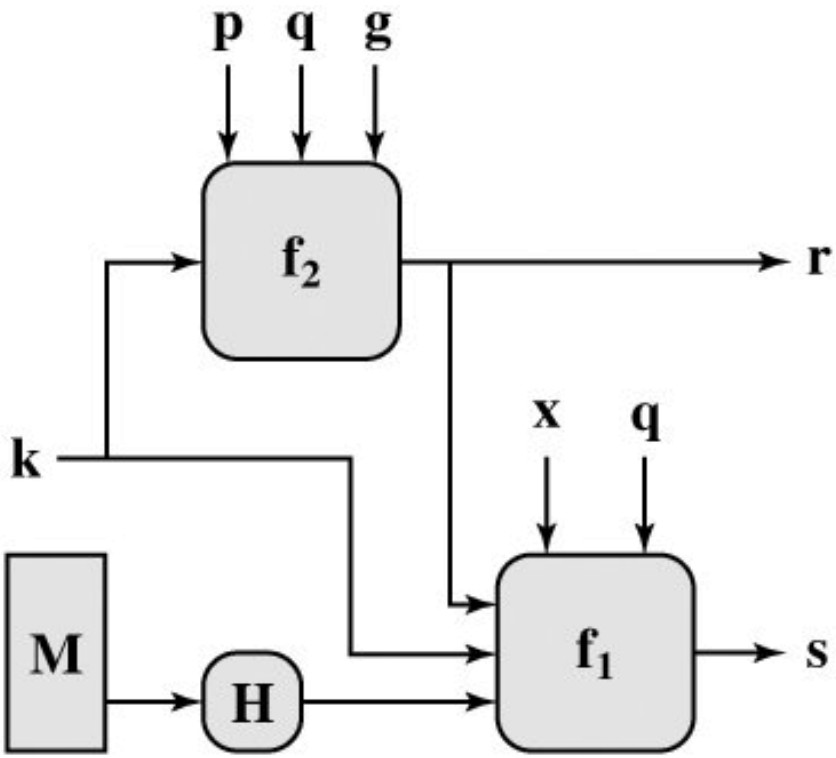
| L | N |
|---|---|
| 1024 | 160 |
| 2048 | 224 |
| 2048 | 256 |
| 3072 | 256 |

# استاندارد امضای دیجیتال DSS

## 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




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

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

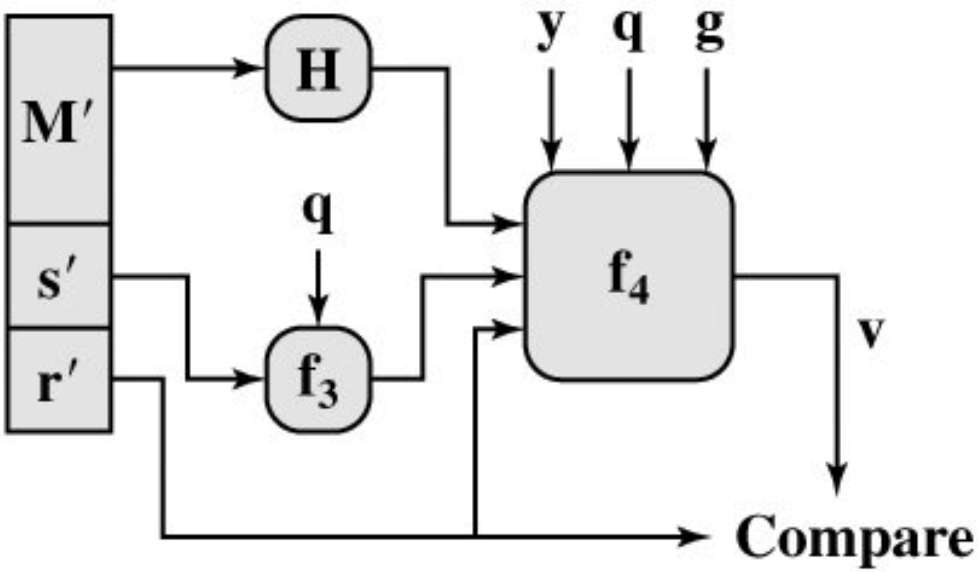
# استاندارد امضای دیجیتال

- 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 امضای دیجیتال

- 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 لگاریتم‌های گسسته
  - الگوریتم امضاء سریع است، چون خیلی از مقدارها از پیش قابل محاسبه هستند.
  - برای هر پیغام، یک مقدار سری k تولید و استفاده می‌شود. بنابراین امضای دو پیغام با محتوای یکسان، متفاوت خواهد بود.

# فهرست مطالب

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

# مباني PKI

- نکته اصلی در رمزنگاری نامتقارن:

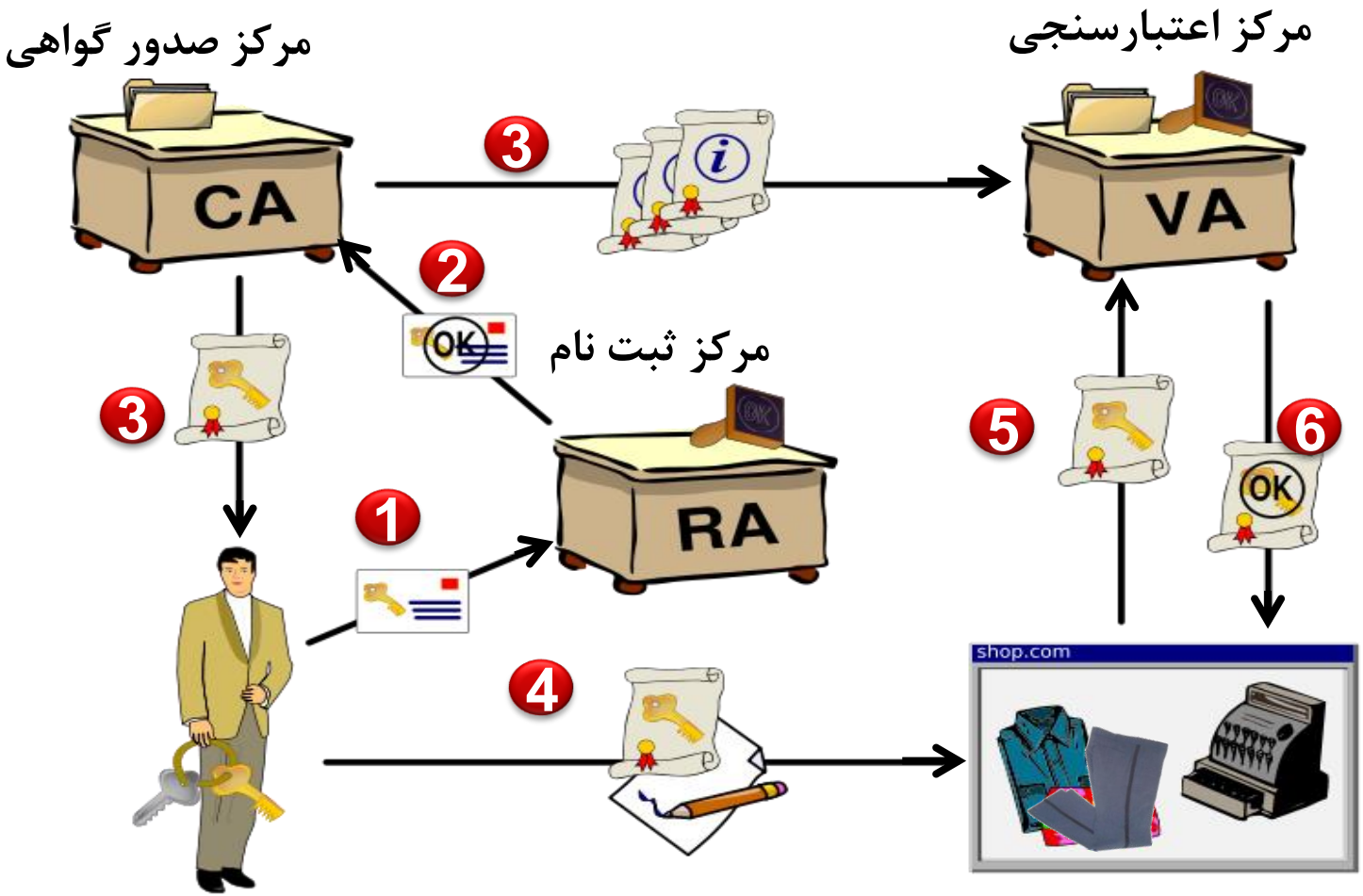
  "چه کسی کلید خصوصی متناظر با یک کلید عمومی را دارد؟"

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

# گواهي كليد عمومي

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

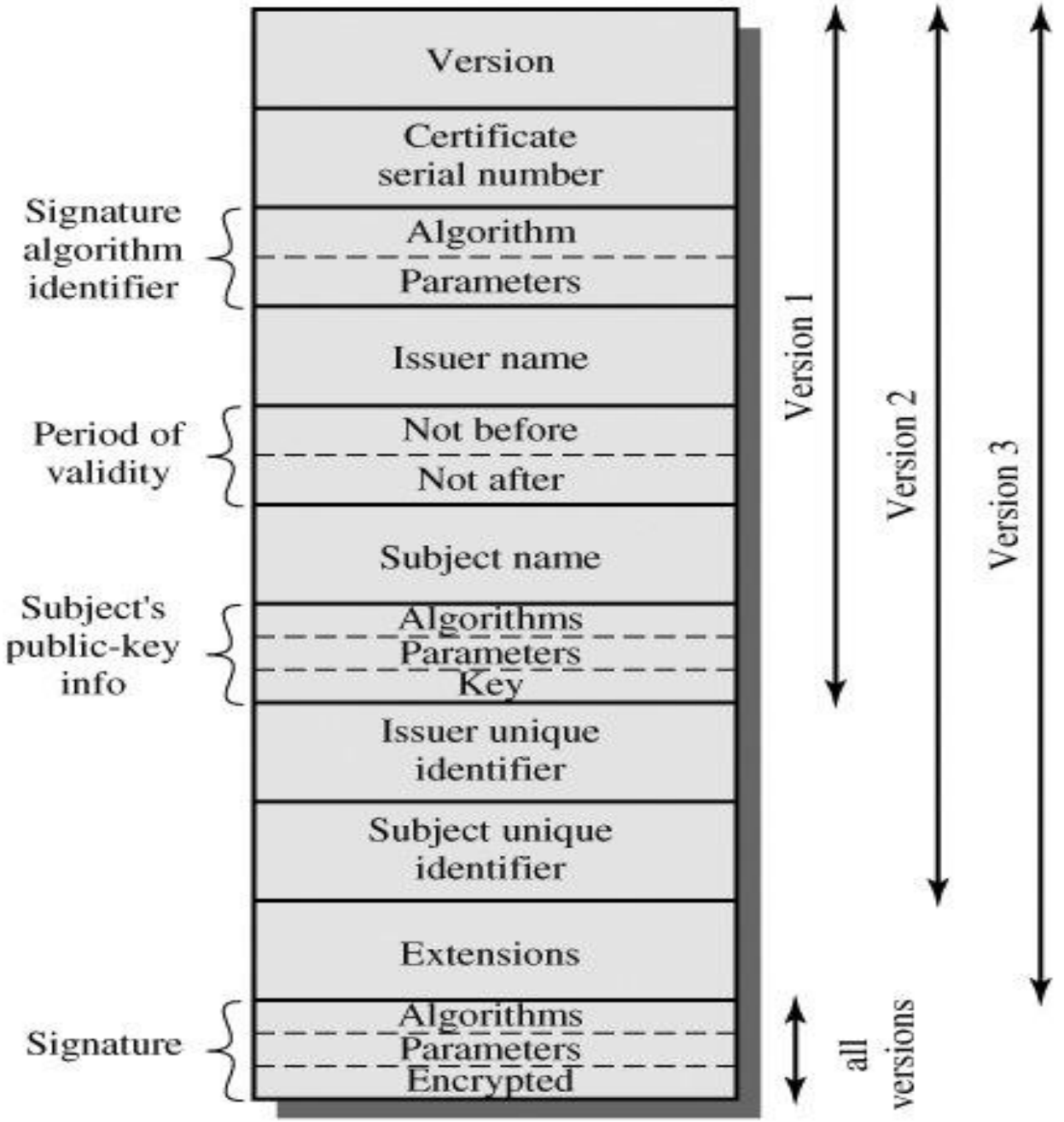
$$\text{Certificate:=} \left( \text{Public Key, ID, } \underbrace{E(PR_{CA}, \text{Certificate-Digest})}_{\text{امضای مرکز صدور گواهی CA بر روی گواهی}} \right)$$

# گواهي كليد عمومي

- صحت گواهی به راحتی قابل کنترل است.  هر تغییری در آن به سادگی کنترل می‌شود.
- ارسال و ذخیرهٔ گواهی به شکل رمز نشده می‌تواند صورت پذیرد.
- برای وارسی گواهی به کلید عمومی CA نیاز داریم.

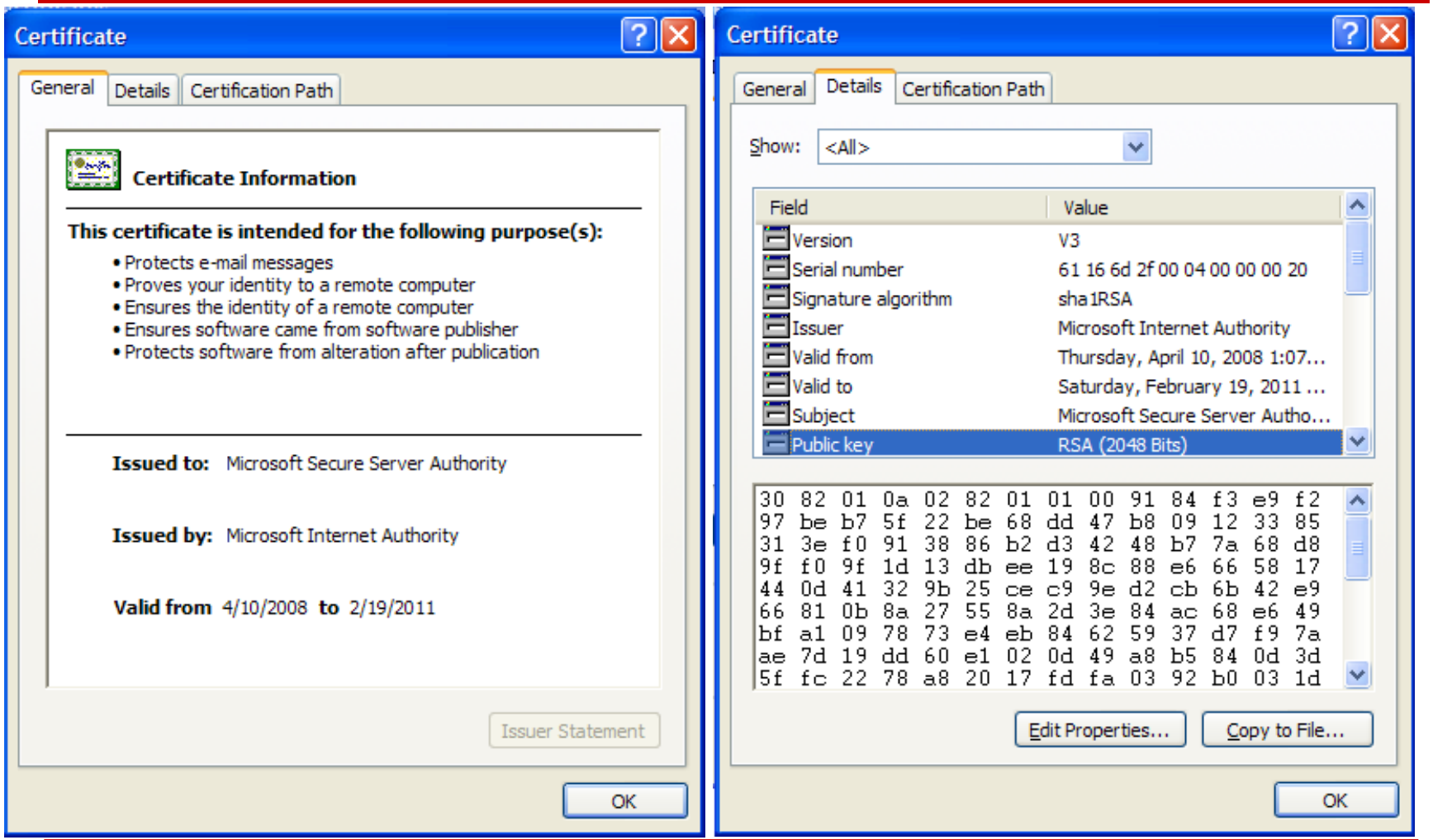
# X.509

- محصول ITU-T و بخشی از توصیه‌های سری X.500
- گواهی X.509 در S/MIME ، IPSec، SSL/TLS و SET استفاده شده است.
- قالب گواهی‌های کلید عمومی و قالب لیست گواهی‌های باطل‌شده در این استاندارد تعریف شده است.




# ساختار گواهی دیجیتال X.509

# گواهي كليد عمومي



# ابطال گواهي

- 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.

# ابطال گواهي

## دو رویکرد:

- با گم شدن، تغییر و یا لو رفتن کلید خصوصی لیستی از گواهی‌های منقضی نشده (از لحاظ زمانی) ولی باطل شده به همگان منتشر شود .

**استفاده از لیست CRL**

- هرکس هرگاه گواهی خواست، از مرکز مورد اعتماد درخواست کند. یا بررسی وضعیت گواهی به صورت برخط صورت پذیرد.

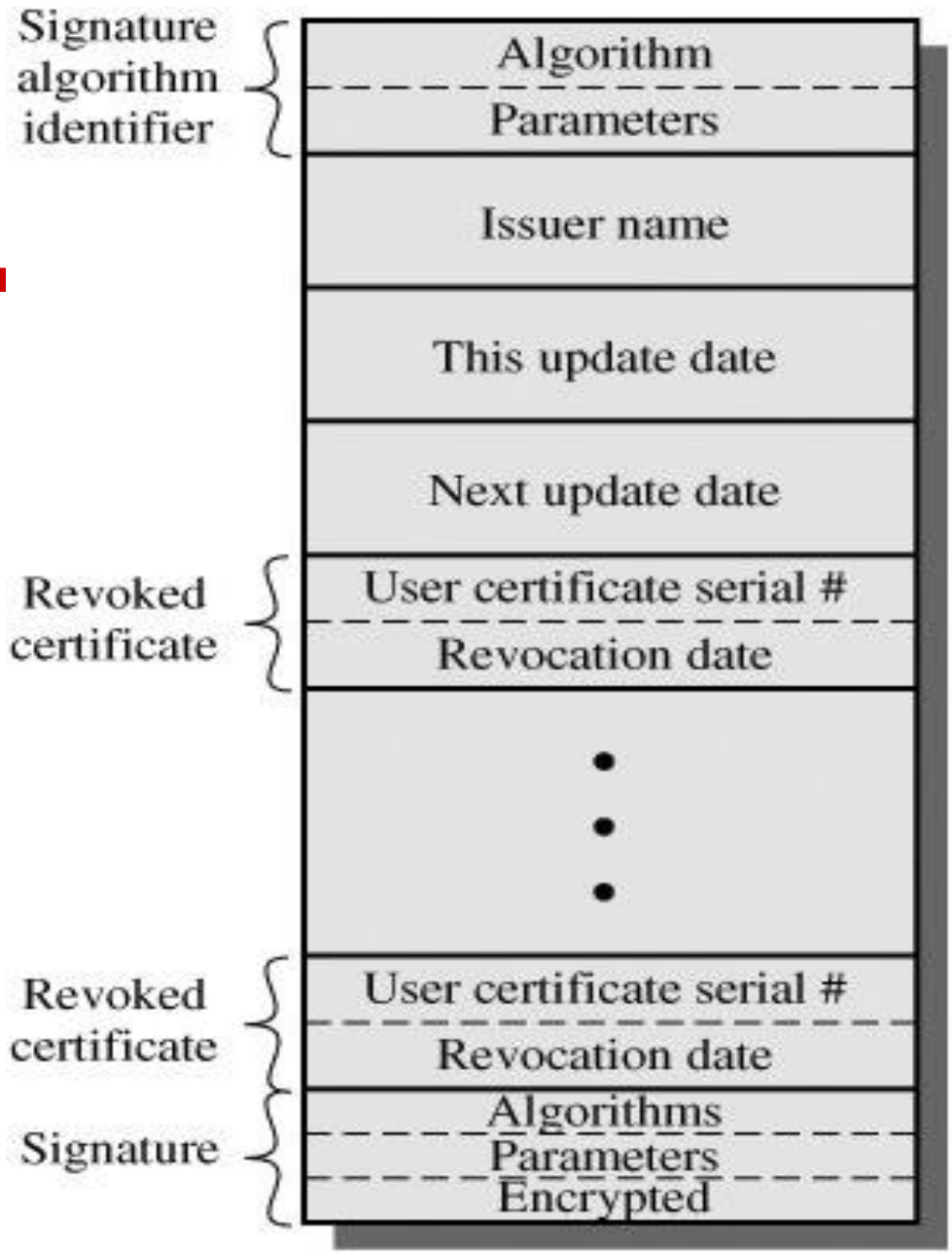
**استفاده از سرویس OCSP**

# ابطال گواهی - CRL

- به طور معمول برای اعلام عدم اعتبار گواهی از لیست گواهی‌های باطل شده (CRL) استفاده می‌شود.
  (**CRL**: Certificate Revocation List)

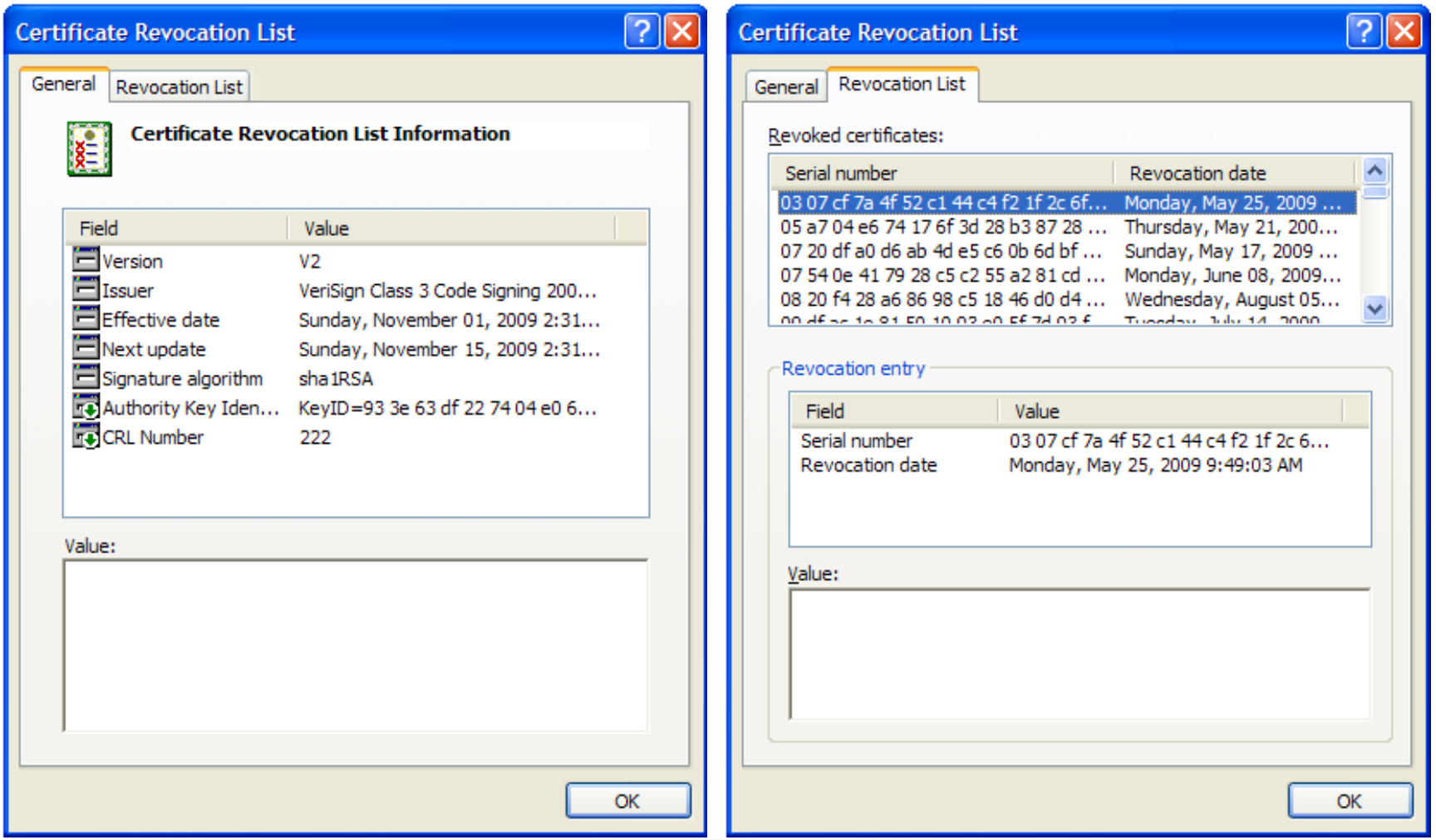
- تاریخ ابطال، شماره سریال گواهی‌های نامعتبر، به همراه امضاء صادرکننده در لیست گواهی نامعتبر (**CRL**) وجود دارد.

- **انواع CRL:**
  - **Full CRL** در دوره‌های زمانی مشخص، مرکز CA لیست کامل گواهی‌های نامعتبر را منتشر می‌کند.
  - **Delta CRL** اختلاف اخیرترین بروزرسانی و CRL جدید منتشر می‌شود.




## ساختار CRL در X.509

# ابطال گواهی - CRL



# ابطال گواهی - OCSP

## Online Certificate Status Protocol (OCSP)

- پروتکلی است که امکان بررسی برخط وضعیت گواهی (اعتبار یا ابطال آن) را فراهم می‌نماید.
- به کارگزار OCSP، اصطلاحاً OCSP Responder گفته می‌شود.
- مزیت نسبت به CRL: به دلیل برخط بودن اطمینان بیشتری را از وضعیت فعلی گواهی فراهم می‌نماید.
- عیب نسبت به CRL: کارگزار OCSP می‌تواند از گواهی‌هایی که یک فرد استفاده می‌نماید اطلاع یابد. لذا حریم خصوصی فرد خدشه‌دار می‌شود.

# نسخه‌برداري و بازيابي كليد

- 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.

# نسخه‌برداري و بازيابي كليد

- 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 دیجیتال.
  - عدم انکار مستلزم تولید و ذخیرهٔ امن کلید امضاء در محدوده تحت کنترل کاربر (در همه حالات) است و لذا در نگاهی بدبینانه، نباید از آن پشتیبان گرفت.
  - از نظر فنی هم ضرورت ندارد چرا که در صورت از دست رفتن کلید، یک زوج کلید دیگر تولید و استفاده می‌شود.

# گواهی های هر کاربر

- **بنابراین به لحاظ نظری بهتر است دو زوج کلید برای هر کاربر وجود داشته باشد:**
  - **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 رمزگشایی باشند. این کار توسط نرم‌افزار طرف کارفرما انجام می‌شود.
  - بروزآوری کلید و گواهی باید قبل از انقضاء صورت پذیرد.
  - در نقطه مقابل برای بروزرسانی کلیدهای امضاء باید کاملا کلید فعلی را نابود کرد!

# فهرست مطالب

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

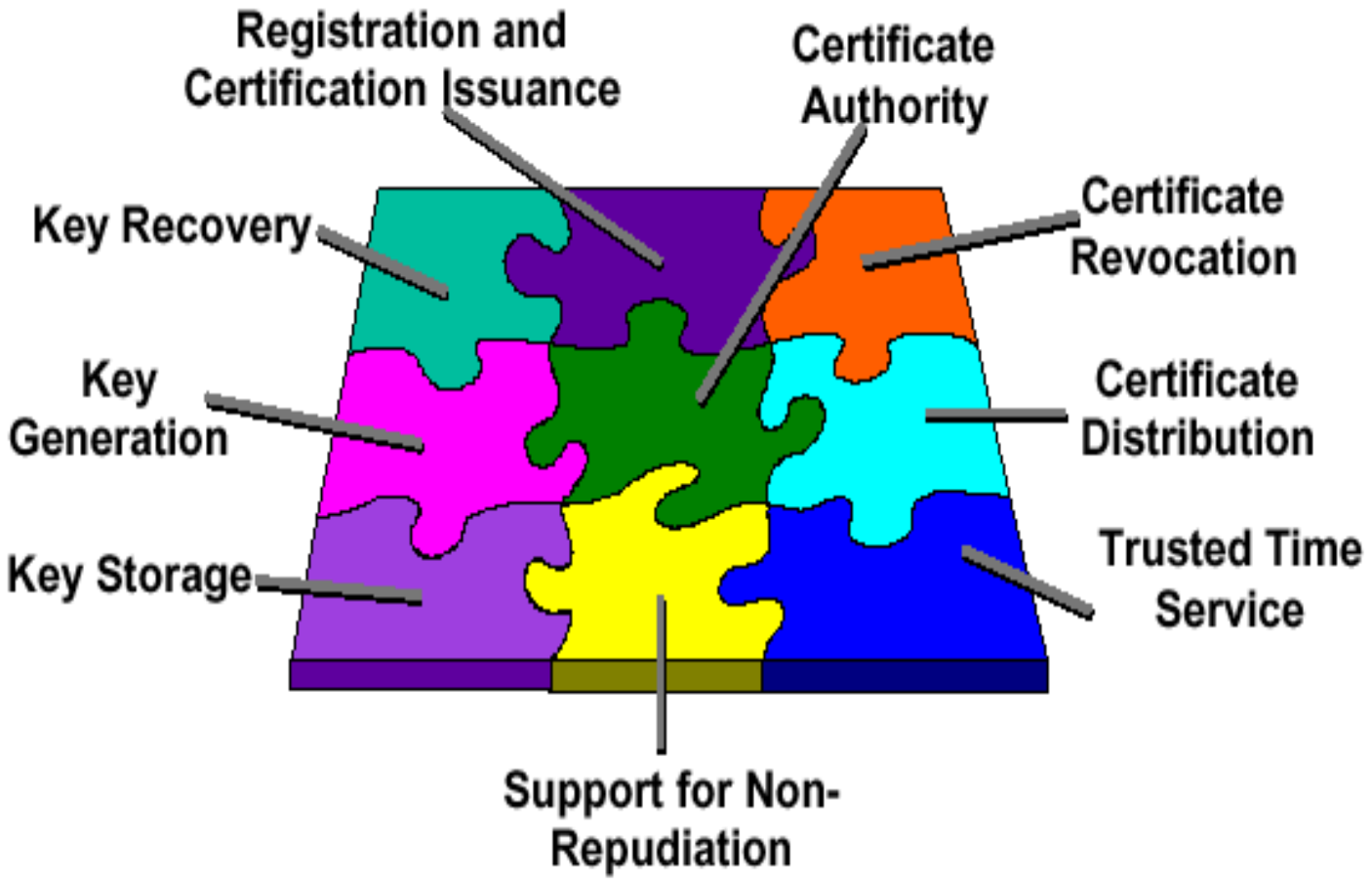
# مؤلفه‌هاي PKI

- 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 گواهي

- 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 درخواست 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.
- استاندارد ارایه درخواست صدور گواهی PKCS#10 است و درخواستها بر اساس این استاندارد در قالب فایل CSR به RA ارسال می‌شوند.
- **تمرین:** نحوه تولید زوج‌کلید و فایل CSR در سیستم‌عامل‌های مختلف به طور عملی بررسی شود.

# فهرست مطالب

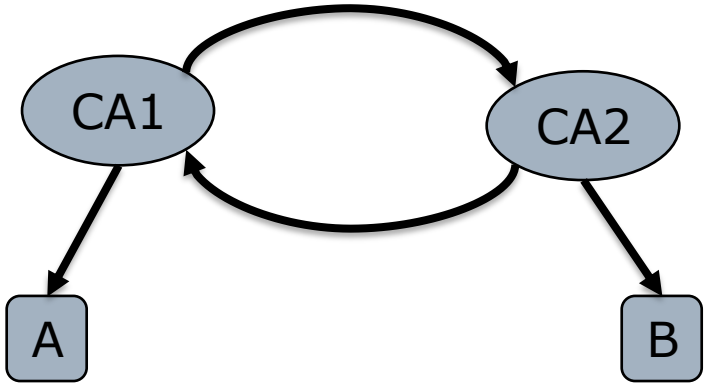
- مبانی امضای دیجیتال
- استانداردهای امضای دیجیتال
- **زیرساخت کلید عمومی (PKI)**
  - مبانی PKI
  - گواهی دیجیتال و مدیریت آن
  - مولفه‌های PKI
  - **معماری PKI، رویه‌ها و خط‌مشی‌ها**

# معماري 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 وSingle 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:



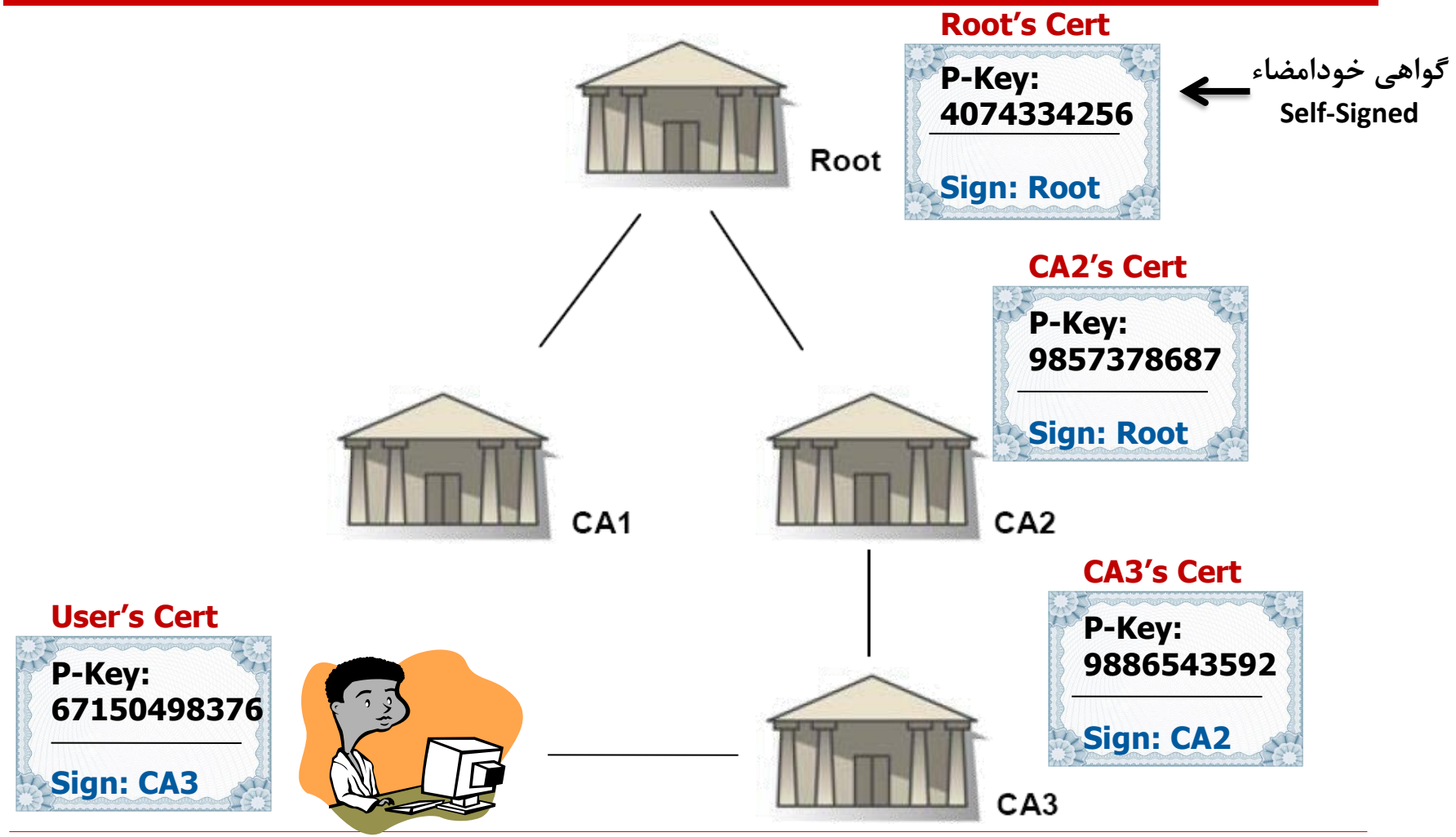

- CA1 <<CA2>> CA2 <<B>>
- CA2 <<CA1>> CA1 <<A>>

<< A >> CA به معنای گواهی صادره CA برای کاربر A است.

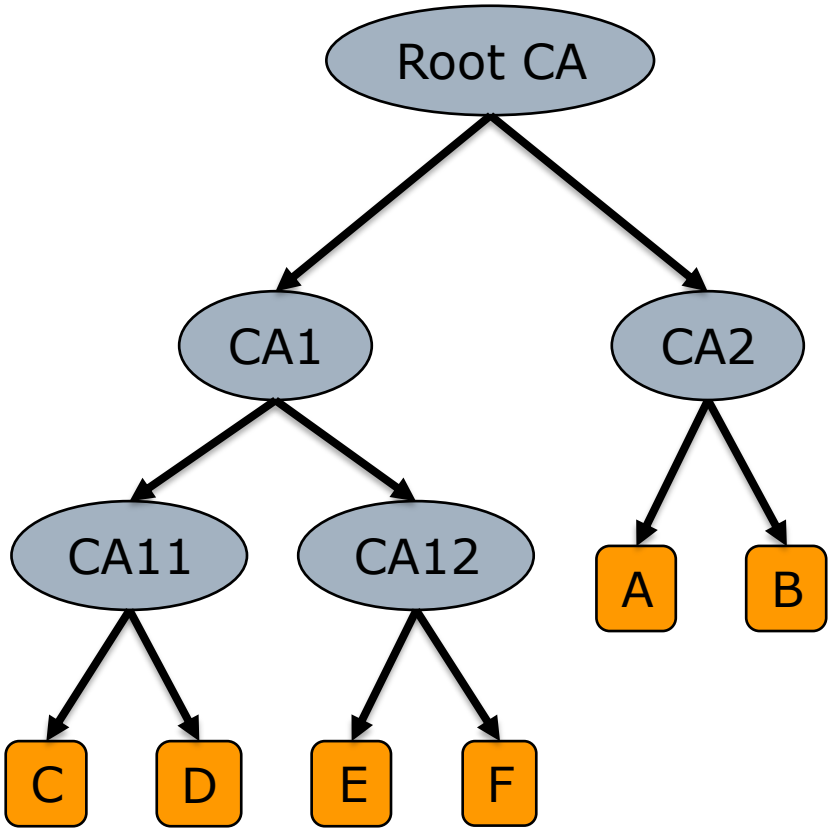
# Enterprise PKI

- دو معماری 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

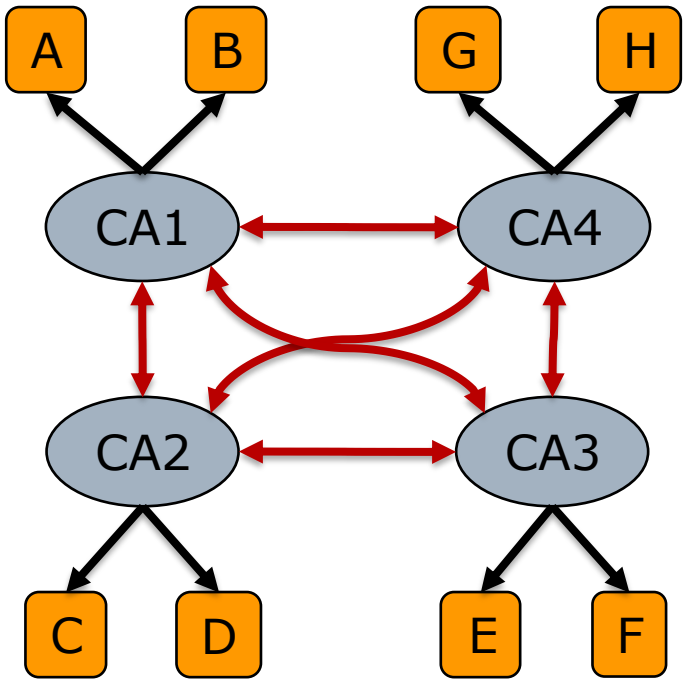


# مدل سلسله مراتبی




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

# مدل توری

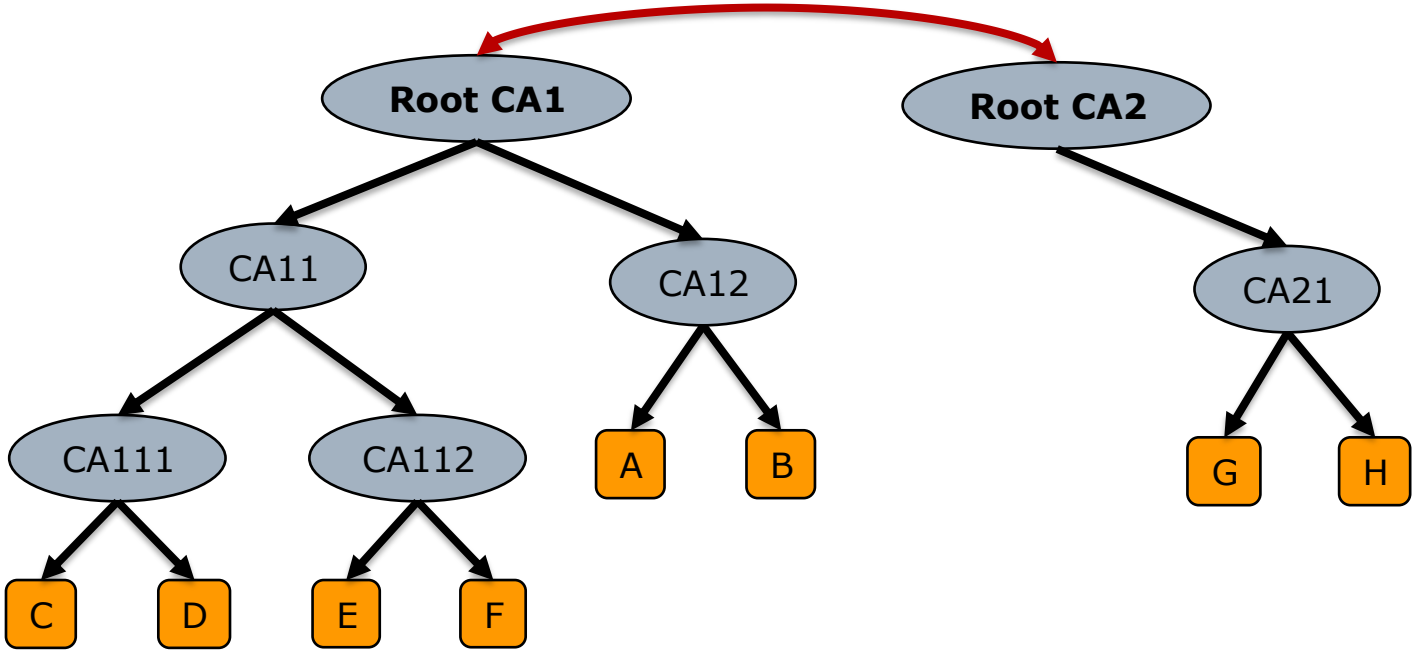



- هر دو CA به یکدیگر گواهی ضربدری بدهند.

- 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
- **در عمل از گواهی ضربدری استفاده چندانی نشده و لذا لازم است گواهی‌های همه مراکز ریشه را در همه سیستم‌ها داشته باشیم.**



# رویه‌ها و خط‌مشی‌ها

- برای داشتن PKI، وجود دو مستند ضروری است:
  - سیاست نامه گواهی دیجیتال (CP) Certificate Policy
  - آیین نامه اجرایی گواهی دیجیتال (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 متعلق به مرکز ریشه است که خط‌مشی 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 مرکز ریشه برای هر مرکز صدور گواهی (ریشه یا میانی) 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.
- مهم‌ترین این مستندات:
  - سند مراسم تولید کلید و گواهی مرکز
  - سند عملیات روزانه مرکز
  - سند سیاست نامه امنیتی

# پایان