

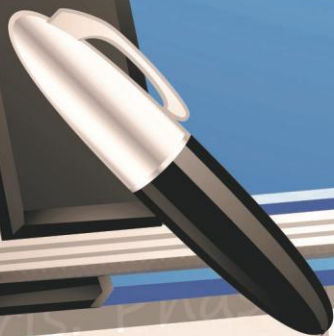
madsage
IRan Education
Research
NETwork
(IRERNET)

شبکه آموزشی - پژوهشی مادیج
با هدف بهبود پیشرفت علمی
و دسترسی راحت به اطلاعات
برای جامعه بزرگ علمی ایران
ایجاد شده است

مادیج

شبکه آموزشی - پژوهشی ایران

madsg.com
مادیج



porta. Lorem ipsum
dolor mauris e
goma. Lorem ipsum.

یادداشت‌های امن و ایمنی



امنیت داده و شبکه

امضای رقمی و زیرساخت کلید عمومی

مرتضی امینی - نیمسال اول ۹۰-۹۱



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 می تواند یک پیام جعلی را بسازد (با استفاده از کلید توافق شده) و آنرا به فرستنده نسبت دهد!

■ **انکار توسط فرستنده:** فرستنده می تواند 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 صرفاً 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 می کند.

■ الگوریتم تولید امضاء (Signature Alg)

□ پیام و کلید خصوصی فرستنده را به عنوان ورودی می گیرد و امضاء را تولید می کند.

■ الگوریتم تایید امضاء (Signature Verification Alg)

□ امضاء و کلید عمومی فرستنده را به عنوان ورودی می گیرد و تاییدیه امضاء را به عنوان خروجی برمی گرداند.



امضاء رقمی

■ مستقیم (Direct)

- فقط دو طرف ارتباط دخیل هستند.
- ضعف: به امنیت کلید خصوصی فرستنده وابسته است.
- فرستنده می تواند 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 می کند.
- امکان مراجعه به شخص سوم، در صورت بروز اختلاف



امضای رقمی با واسطه

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

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

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

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

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

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

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

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

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



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 : استاندارد شده توسط NIST FIPS 186
■ مشهورترین استاندارد امضاء رقمی محسوب می شود.

□ RSA Digital Signature : استاندارد شده توسط

■ ISO 9776

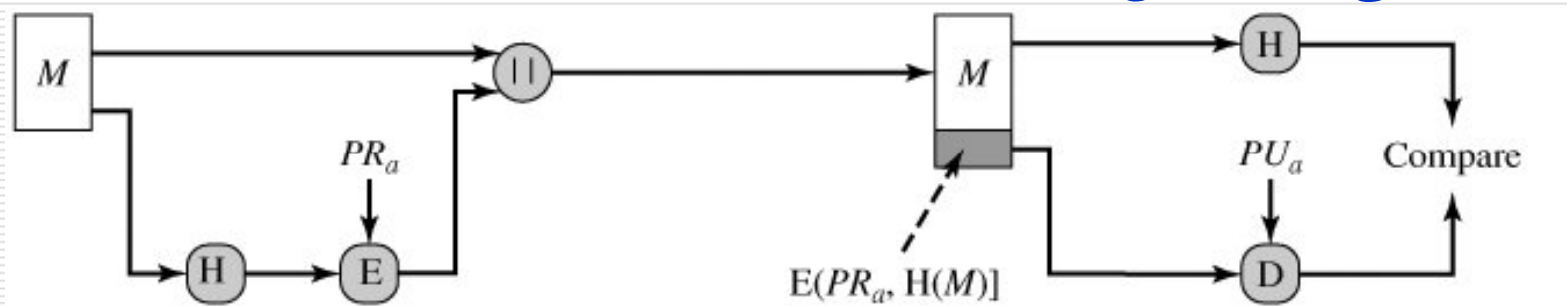
■ ANSI X9.31

■ CCITT X.509

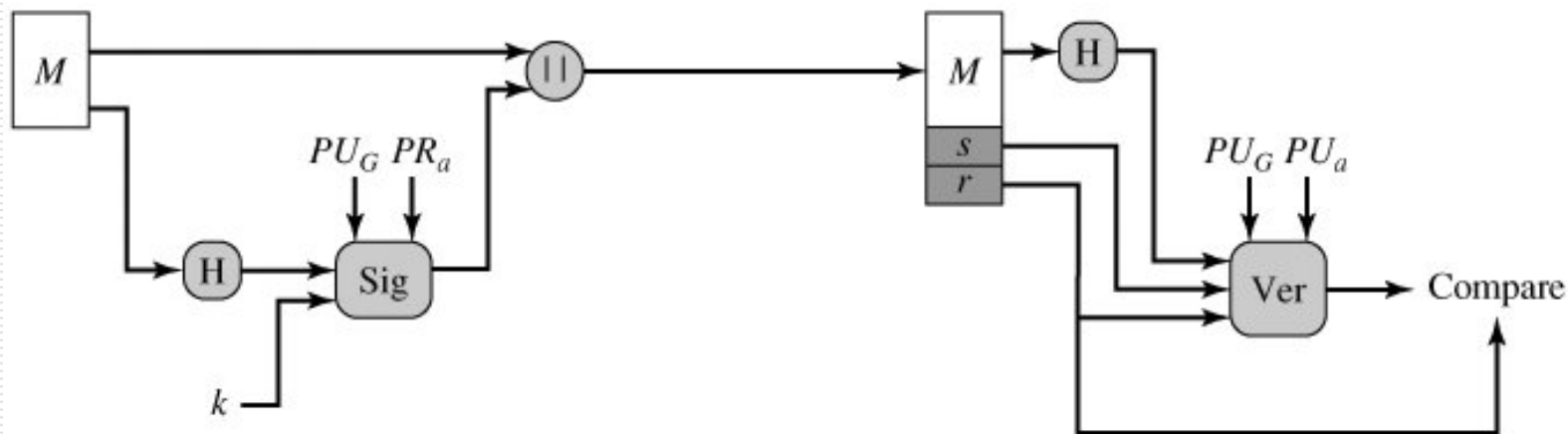


DSS در قیاس با RSA

□ 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-1 برای تولید چکیده پیام
- استفاده از الگوریتم DSA و کلید خصوصی فرستنده برای رمز کردن 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 ($y = g^x \text{ mod } p$)
- k : user per-message secret (a random such that $0 < k < q$)

- $r = (g^k \text{ mod } p) \text{ mod } q$
- $s = [k^{-1}(H(M) + xr)] \text{ mod } q$
- **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:

■ $r = (g^k \bmod p) \bmod q$

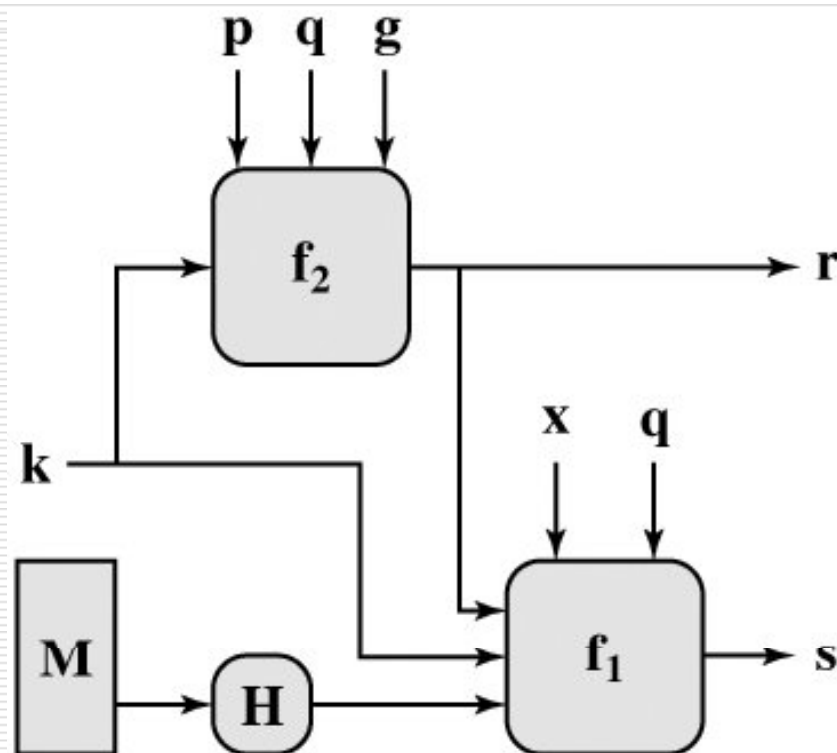
■ $s = [k^{-1}(H(M) + xr)] \bmod q$

□ $H(M)$: 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.

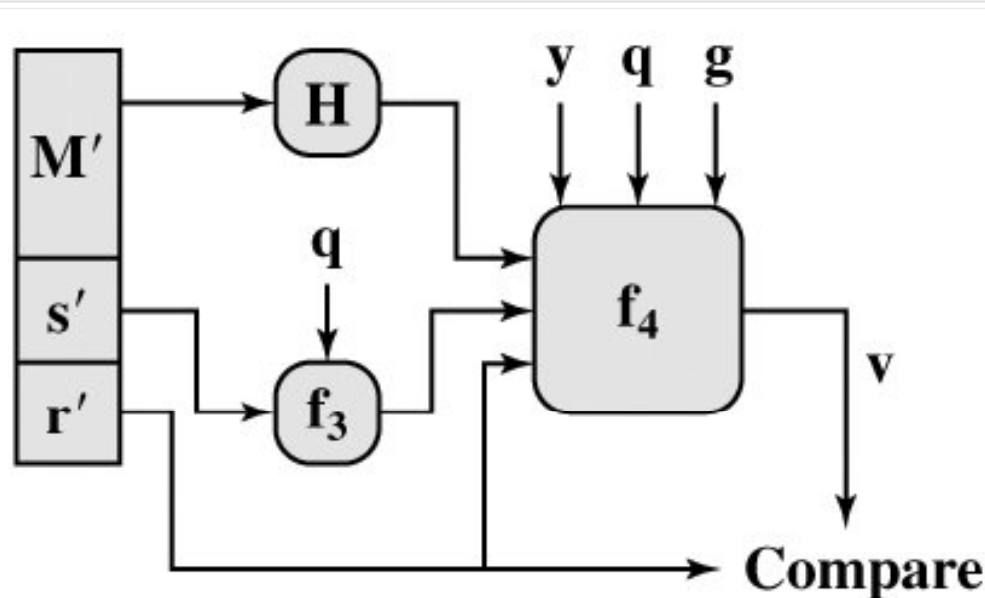
■ مقادیر زیر را محاسبه می کند:

- $w = (s')^{-1} \bmod q$
- $u_1 = [H(M')w] \bmod q$
- $u_2 = [(r')w] \bmod q$
- $v = [(g^{u_1}y^{u_2}) \bmod p] \bmod q$

■ اگر $v=r'$ ، امضاء معتبر است.



فرآیند واریسی امضاء در DSS



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

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

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



استاندارد امضاء رقمی

□ نکاتی درباره الگوریتم:

- مقدار r مستقل از پیام محاسبه می شود.
- به k و 3 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 مقادیرها 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، میسر نیست.
- استفاده از کلید سری جدید k برای هر پیام.



فهرست مطالب

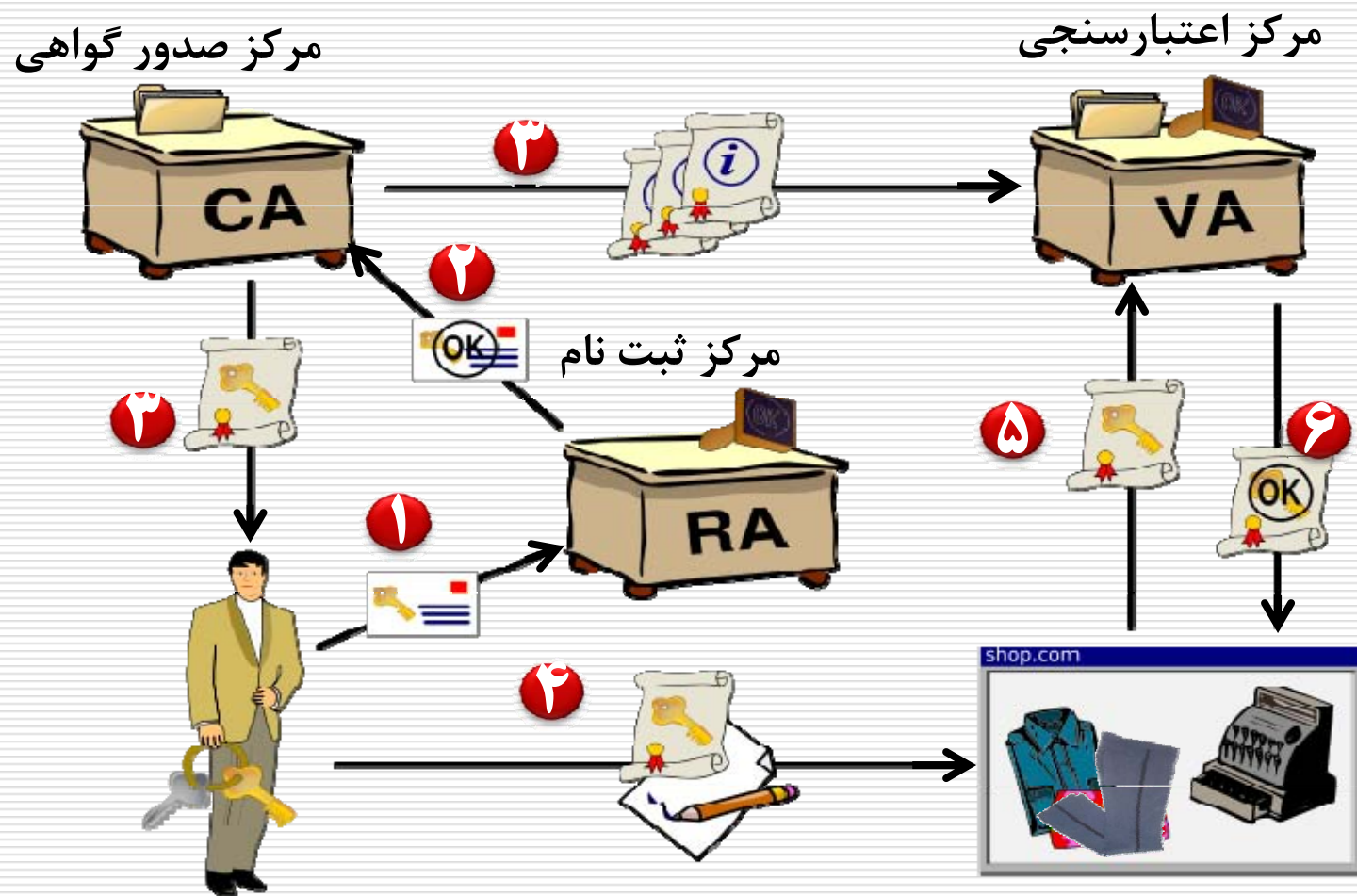
- مبانی امضای رقمی
- استانداردهای امضای رقمی
- زیرساخت کلید عمومی (PKI)
- مبانی PKI
- گواهی رقمی و مدیریت آن
- مولفه‌های PKI
- معماری PKI، رویه‌ها و خط‌مشی‌ها



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 دریافت کننده 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 واریسی 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 ایده آل

□ 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 ایده آل

- 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- ذکر شده باشد که 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) امضاء 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 می شود.
- ارسال و ذخیره گواهی به شکل رمز نشده.
- برای واریسی گواهی به کلید عمومی CA نیاز داریم.
- تقریباً همگی مشخصات گواهی ایده آل در گواهی کلید عمومی وجود دارد.



گواهی کلید عمومی

Certificate

General Details Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Protects e-mail messages
- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- Ensures software came from software publisher
- Protects software from alteration after publication

Issued to: Microsoft Secure Server Authority

Issued by: Microsoft Internet Authority

Valid from 4/10/2008 **to** 2/19/2011

Issuer Statement

OK

Certificate

General Details Certification Path

Show: <All>

Field	Value
Version	V3
Serial number	61 16 6d 2f 00 04 00 00 00 20
Signature algorithm	sha1RSA
Issuer	Microsoft Internet Authority
Valid from	Thursday, April 10, 2008 1:07...
Valid to	Saturday, February 19, 2011 ...
Subject	Microsoft Secure Server Autho...
Public key	RSA (2048 Bits)

```
30 82 01 0a 02 82 01 01 00 91 84 f3 e9 f2
97 be b7 5f 22 be 68 dd 47 b8 09 12 33 85
31 3e f0 91 38 86 b2 d3 42 48 b7 7a 68 d8
9f f0 9f 1d 13 db ee 19 8c 88 e6 66 58 17
44 0d 41 32 9b 25 ce c9 9e d2 cb 6b 42 e9
66 81 0b 8a 27 55 8a 2d 3e 84 ac 68 e6 49
bf a1 09 78 73 e4 eb 84 62 59 37 d7 f9 7a
ae 7d 19 dd 60 e1 02 0d 49 a8 b5 84 0d 3d
5f fc 22 78 a8 20 17 fd fa 03 92 b0 03 1d
```

Edit Properties... Copy to File...

OK



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:

■ هر کس هرگاه گواهی خواست از مرکز مورد اعتماد درخواست کند.

■ با گم شدن، تغییر و یا لو رفتن کلید خصوصی **لیستی از گواهی‌های منقضی نشده بی اعتبار** 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

Certificate Revocation List

General Revocation List

Certificate Revocation List Information

Field	Value
Version	V2
Issuer	VeriSign Class 3 Code Signing 200...
Effective date	Sunday, November 01, 2009 2:31...
Next update	Sunday, November 15, 2009 2:31...
Signature algorithm	sha1RSA
Authority Key Iden...	KeyID=93 3e 63 df 22 74 04 e0 6...
CRL Number	222

Value:

OK

Certificate Revocation List

General Revocation List

Revoked certificates:

Serial number	Revocation date
03 07 cf 7a 4f 52 c1 44 c4 f2 1f 2c 6f...	Monday, May 25, 2009 ...
05 a7 04 e6 74 17 6f 3d 28 b3 87 28 ...	Thursday, May 21, 200...
07 20 df a0 d6 ab 4d e5 c6 0b 6d bf ...	Sunday, May 17, 2009 ...
07 54 0e 41 79 28 c5 c2 55 a2 81 cd ...	Monday, June 08, 2009...
08 20 f4 28 a6 86 98 c5 18 46 d0 d4 ...	Wednesday, August 05...
00 df 2c 1e 81 50 10 03 e0 5f 7d 03 f...	Tuesday, July 14, 2000

Revocation entry

Field	Value
Serial number	03 07 cf 7a 4f 52 c1 44 c4 f2 1f 2c 6...
Revocation date	Monday, May 25, 2009 9:49:03 AM

Value:

OK



نسخه برداری و بازیابی کلید

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

□ دو دلیل برای نسخه برداری کلید

- فراموشی کلمه رمز: نابودی داده‌های حساس. حتی رمز نکردن به خاطر ترس از گم شدن کلمه رمز وجود دارد.
- گم شدن، دزدیده شدن، و یا خرابی رسانه‌ای که کلیدها روی آن ذخیره شده است.



نسخه برداری و بازیابی کلید

□ عدم انکار دلیلی بر عدم نسخه برداری کلید

■ انکار یعنی اعلام عدم دخالت در یک تراکنش.

□ در فرم کاغذی: امضای دستی این کار را کنترل می کند.

□ در فرم الکترونیکی: امضای رقمی.

■ عدم انکار مستلزم تولید و ذخیره 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 در صورت از دست رفتن کلید، یک زوج کلید دیگر تولید و استفاده می شود.



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 پشتیبان گیری



مدیریت سابقه 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 کاملاً 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 (Certificate Authority) CA: مسئول تولید، مدیریت، توزیع گواهی و CRL.
- مرکز ثبت نام (Registration Authority) RA: مسئول دریافت درخواست گواهی و کنترل محتوای گواهی و اطمینان از تعلق به دارنده آن.
- انبار (Repository): توزیع گواهی‌ها و CRL‌ها (حداکثر کارایی و دسترس پذیری را لازم دارد).
- آرشیو (Archive): انباره طولانی‌مدت و امن برای آرشیو اطلاعات.

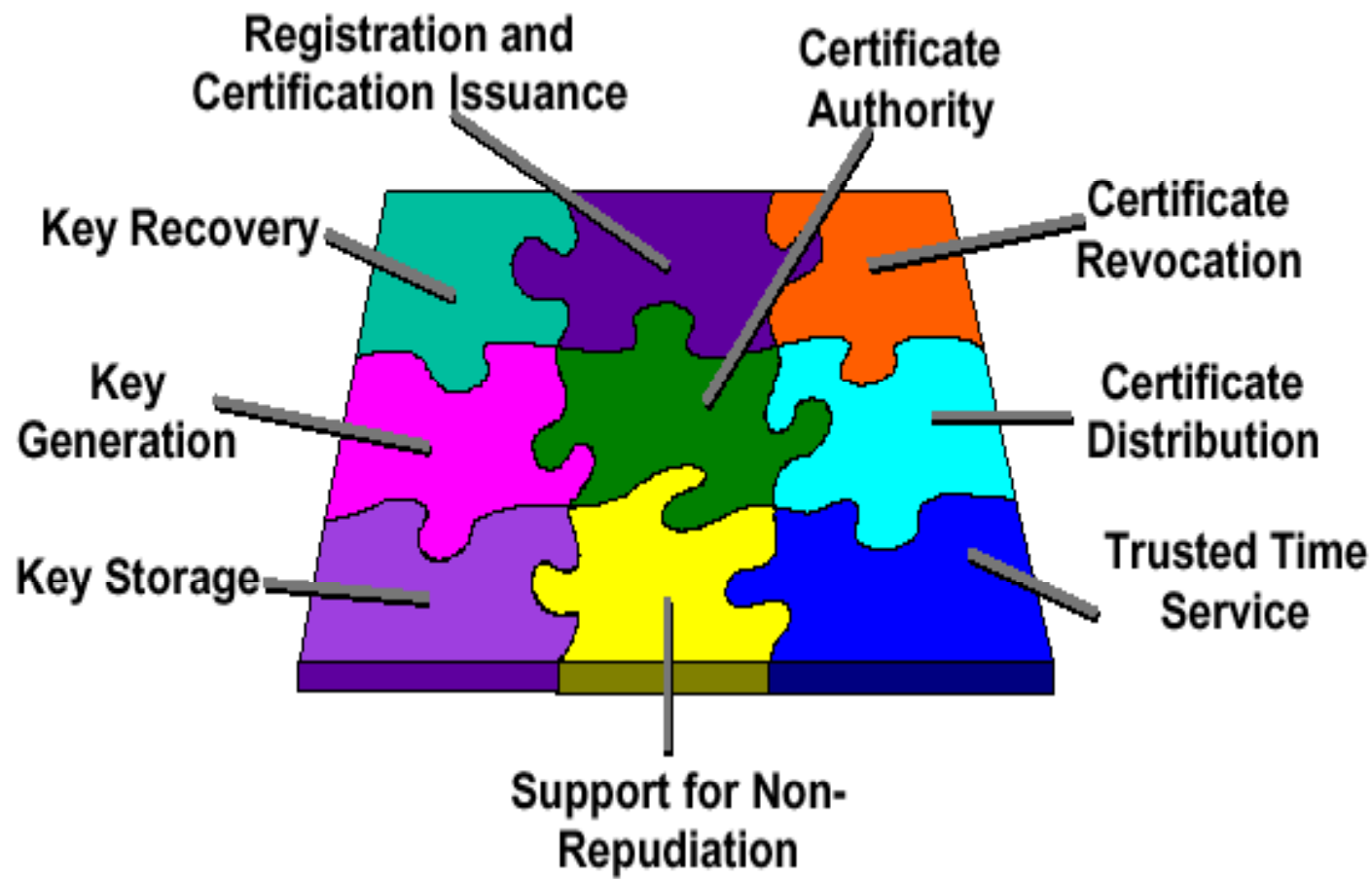


مرکز گواهی CA

- به عنوان آژانس اعتماد در PKI است و لذا طرف سوم امن نامیده می شود.
- مجموعه‌ای از سخت افزار، نرم افزار، و اپراتورها.
- با دو صفت شناخته می شود: 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 در حال پردازش است.
- وظیفه دیگر CA اطمینان از درستی گواهی و درستی ادعای درخواست‌کننده گواهی است.



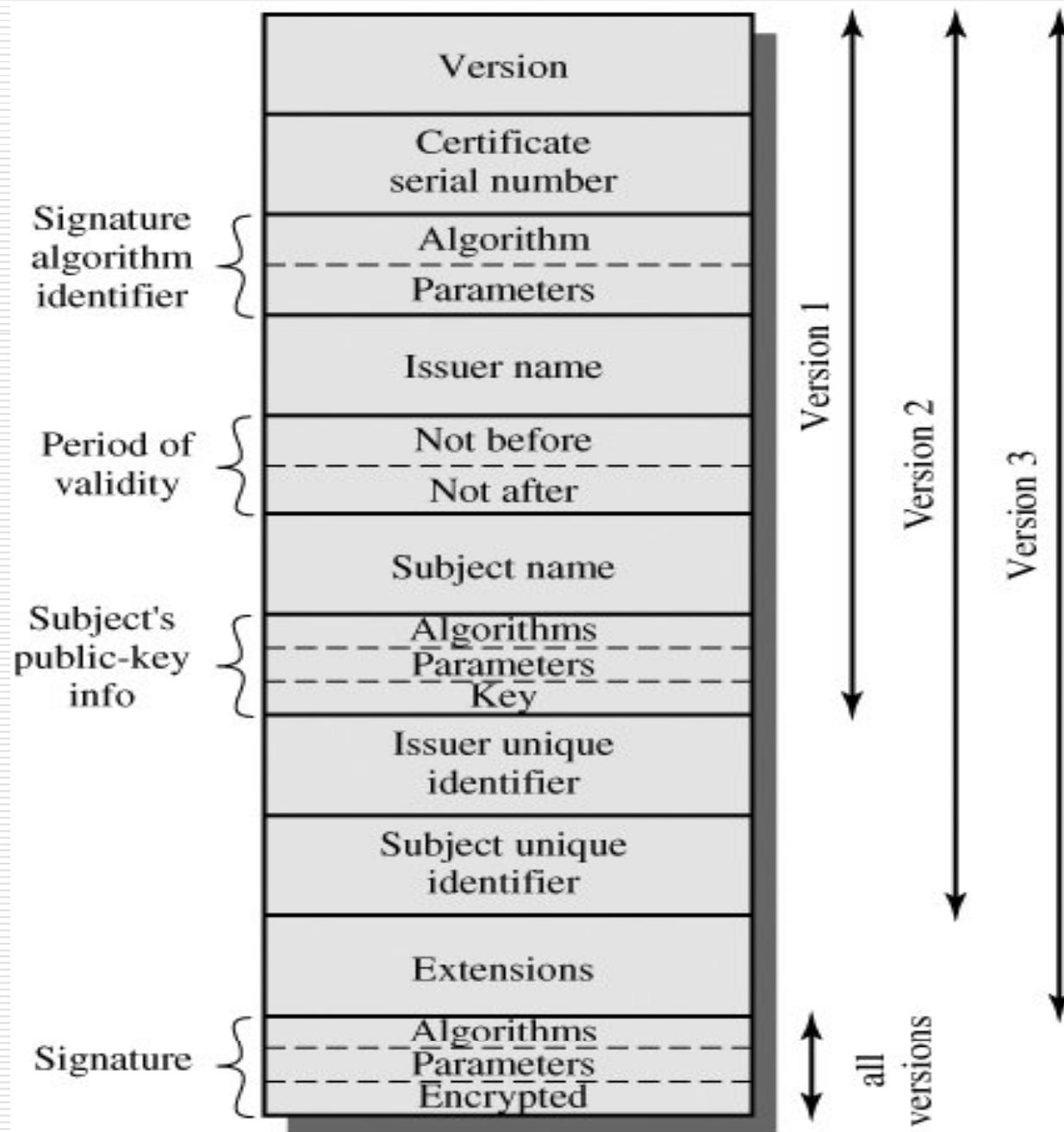
مرکز ثبت نام RA

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

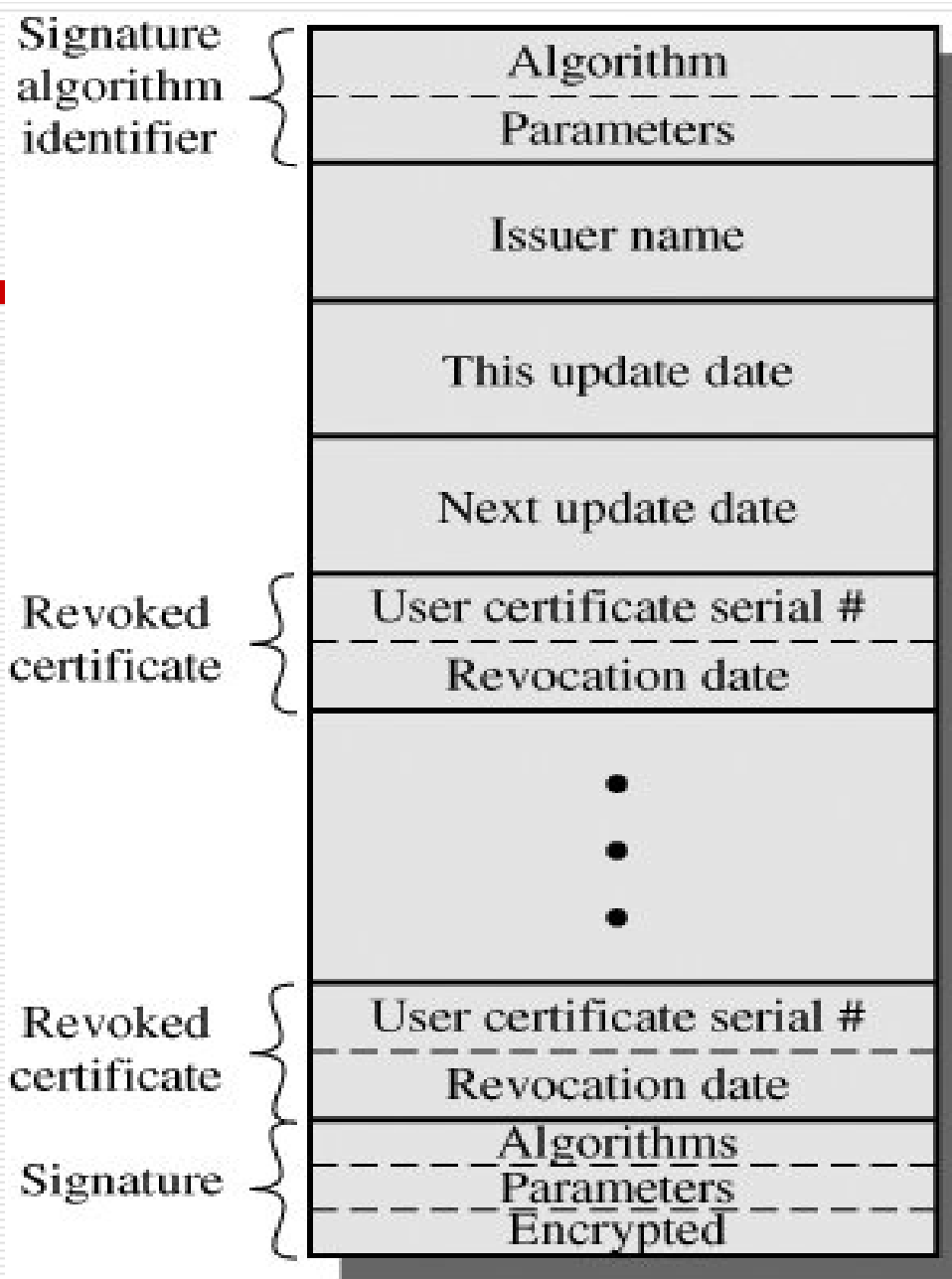


X.509

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



ساختار گواهی رسمی 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

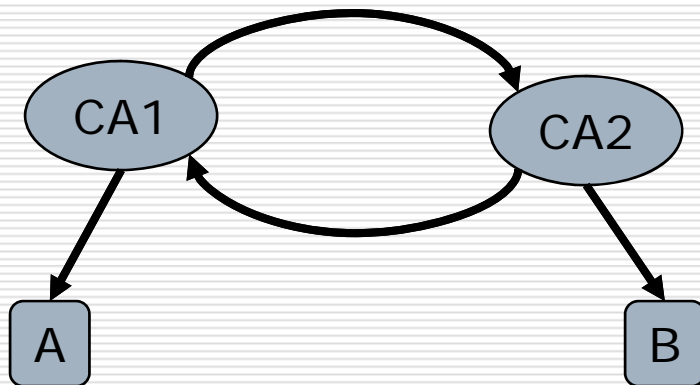
- مادام که دارندگان گواهی از یک CA گواهی گرفته باشند مسأله ساده است.
- وقتی که دارندگان گواهی از CAهای مختلف گواهی گرفته باشند چگونه اعتماد کنند؟
- معماری ساده PKI
- تنها یک CA در سازمان گلوگاه و Single point of failure هرگونه اشکال منجر به لطمه دیدن اعتماد و احتمالاً صدور مجدد گواهی‌ها.



گواهی ضربدري (Cross-Certificate)

□ گواهی ضربدري، گواهی ای است که یک CA برای CA دیگر صادر می کند تا گواهی های 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 <>

■ CA2 <<CA1>> CA1 <<A>>



Enterprise PKI

□ دو معماری مختلف برای PKI بزرگ

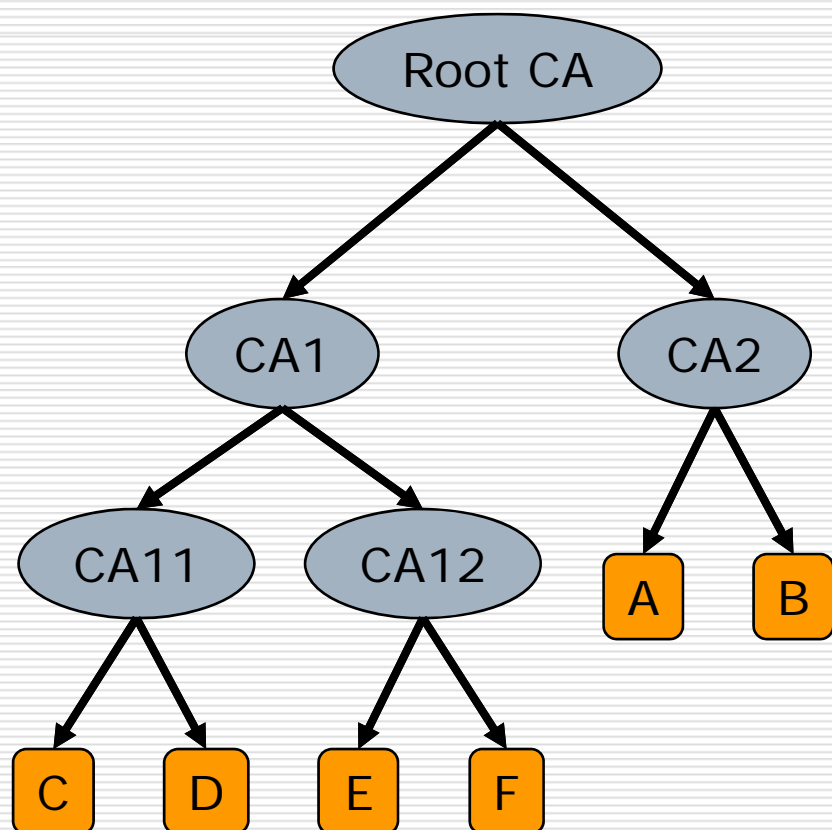
■ سلسله مراتبی: در یک ساختار درختی

■ توری (Mesh): ارتباط کامل ضربدیری CAها با یکدیگر

■ ترکیبی از دو مدل فوق: چند سلسله مراتب از CAها که ریشه آنها با یکدیگر ارتباط ضربدیری 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

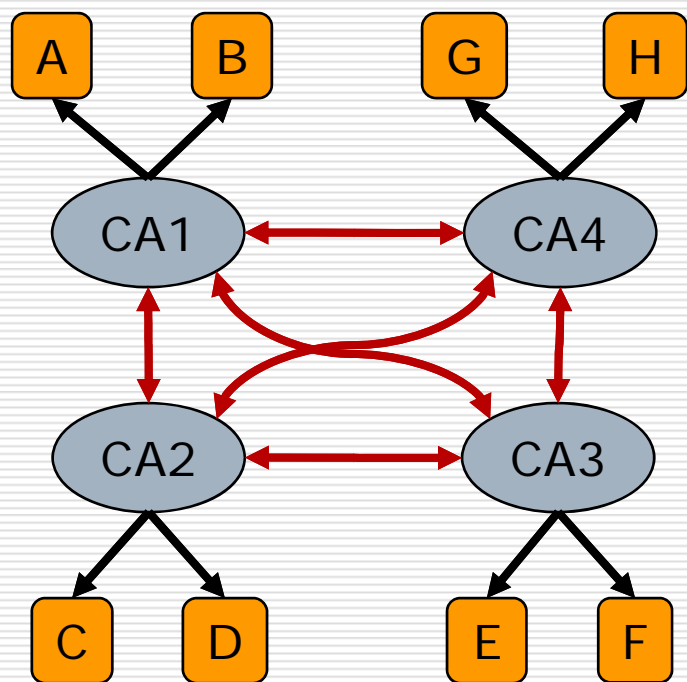
□ صرفاً برای ریشه امنیت بالا نیاز است.

□ 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

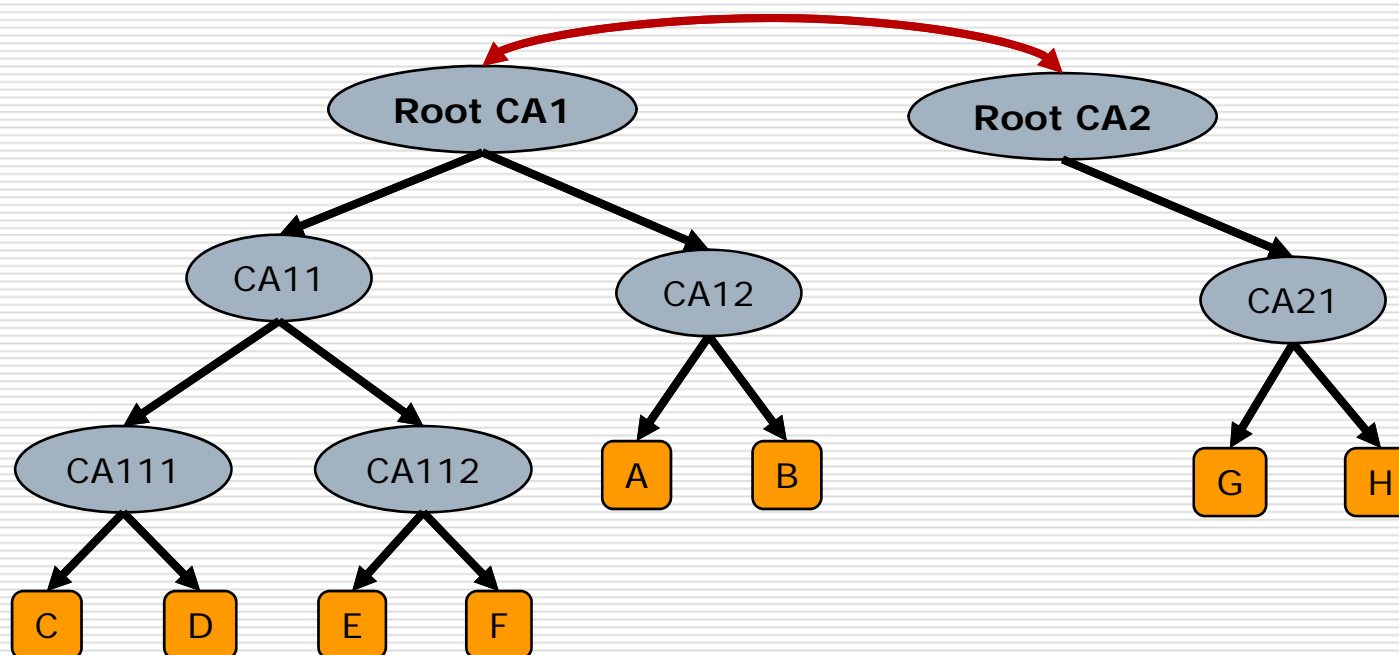
□ معایب:

■ 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 خط‌مشی امنیتی صدور گواهی و نگهداری اطلاعات گواهی را شرح می‌دهد.
 - شرح عملیات CA، مسئولیت‌های 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 داده و شبکه شریف

<http://dnsl.ce.sharif.edu>

پست الکترونیکی

m_amani@ce.sharif.edu

شبکه آموزشی - پژوهشی مادیج
با هدف بهبود پیشرفت علمی
و دسترسی راحت به اطلاعات
برای جامعه بزرگ علمی ایران
ایجاد شده است



madsg.com
مادیج

IRan Education & Research NETwork
(IRERNET)

