



یاد‌الامن والامان

امنیت داده و شبکه

امضای دیجیتال و زیرساخت کلید عمومی

مرتضی امینی - سیدمهدی خرازی

نیم‌سال دوم ۱۴۰۴-۱۴۰۳



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 خط مشی‌ها



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 خط مشی‌ها



امضای دیجیتال

□ ویژگی‌ها:

- امکان تصدیق هویت فرستنده (و در صورت نیاز زمان و تاریخ ارسال)
- تضمین عدم تغییر محتویات پیام
- تضمین عدم انکار فرستنده در ارسال پیام (امضاء شده)
- 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 (همان کلید خصوصی برای 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 نیافتندی باشد.
- **امضای دیجیتال صرفا بر رمزنگاری نامتقارن مبتنی است.** در واقع برای پشتیبانی از سرویس عدم انکار، فرستنده و گیرنده نمی‌توانند از یک کلید مشترک استفاده کنند.



امضای دیجیتال

□ چرا برای امضاء دیجیتال نمی‌توان از رمز متقارن استفاده کرد؟

- **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

□ 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)
 - پیام و 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 خط مشی‌ها



استانداردهای امضای دیجیتال

NIST FIPS 186: استانداردشده توسط **DSS** □

■ مشهورترین استاندارد امضای دیجیتال محاسب می‌شود.

: استاندارد شده توسط **RSA Digital Signature** □

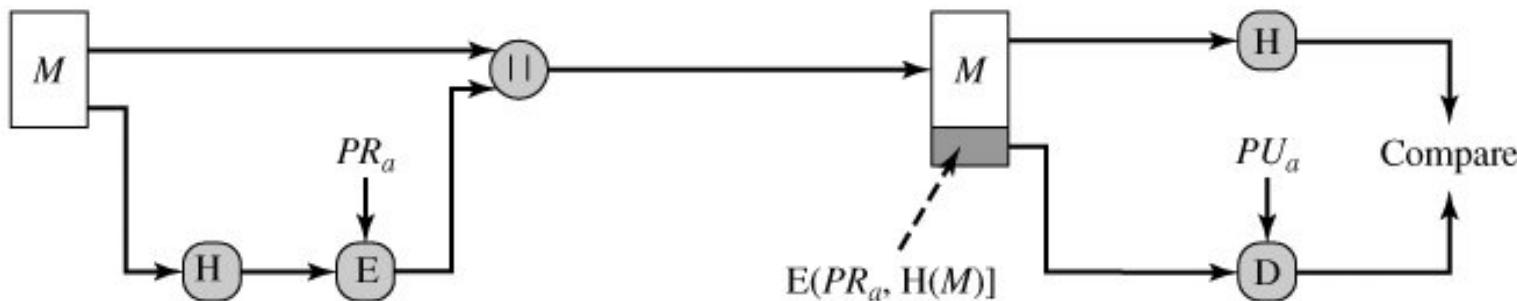
ISO 9776 ■

ANSI X9.31 ■

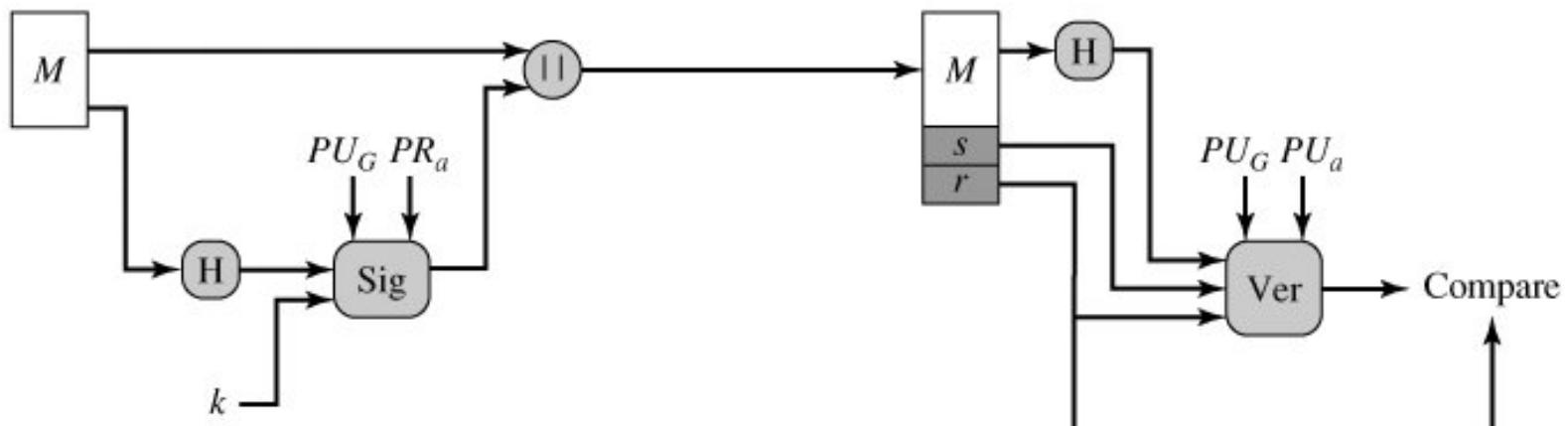
CCITT X.509 ■

RSA در قیاس با DSS

□ 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 کاربرد در حفظ محرمانگی و تبادل کلید (در مقایسه با RSA)
- سرعت اجرای DSA از RSA کمتر است.
- امنیت آن به دشوار بودن محاسبه لگاریتم‌های گستته مرتبط است.



استاندارد امضای دیجیتال DSS

□ پارامترهای الگوریتم

NIST طول p و q طبق استاندارد

L	N
1024	160
2048	224
2048	256
3072	256

■ پارامترهای عمومی : p, q, g

□ p : عدد اول به طول L بیت ($2^{L-1} < p < 2^L$)

□ q : عدد اول مقسم علیه $p-1$ به طول N بیت ($2^{N-1} < q < 2^N$)

■ x : کلید خصوصی کاربر (عددی تصادفی $0 < x < q$)

■ y : کلید عمومی کاربر ($y = g^x \text{ mod } p$)

■ k : کلید مخفی به ازای هر پیام (عددی تصادفی $0 < k < q$)

■ k^{-1} : معکوس k در پیمانه q ($k \cdot k^{-1} \text{ mod } q = 1$)

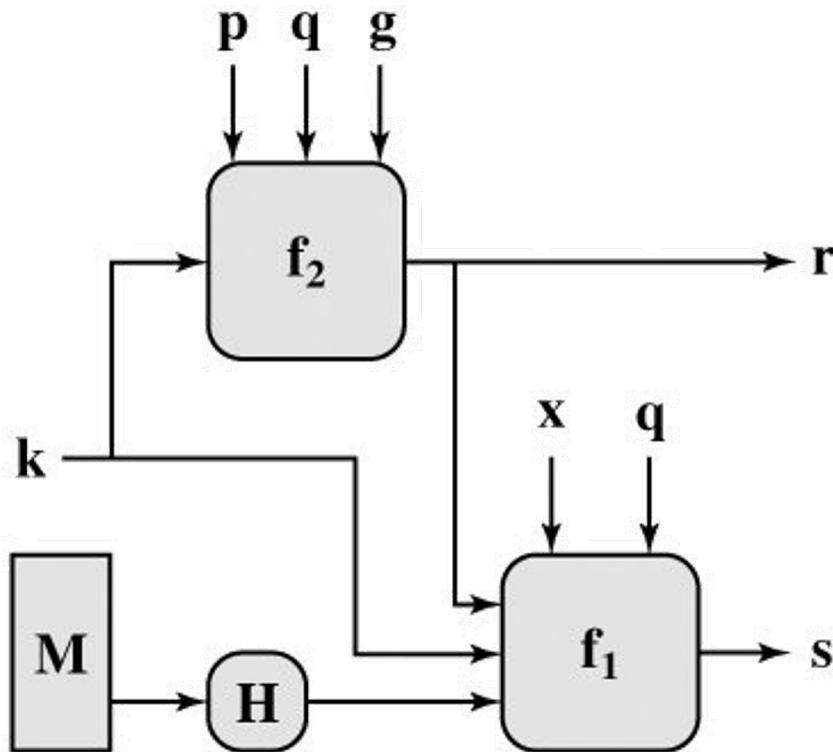


استاندارد امضای دیجیتال DSS

□ 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

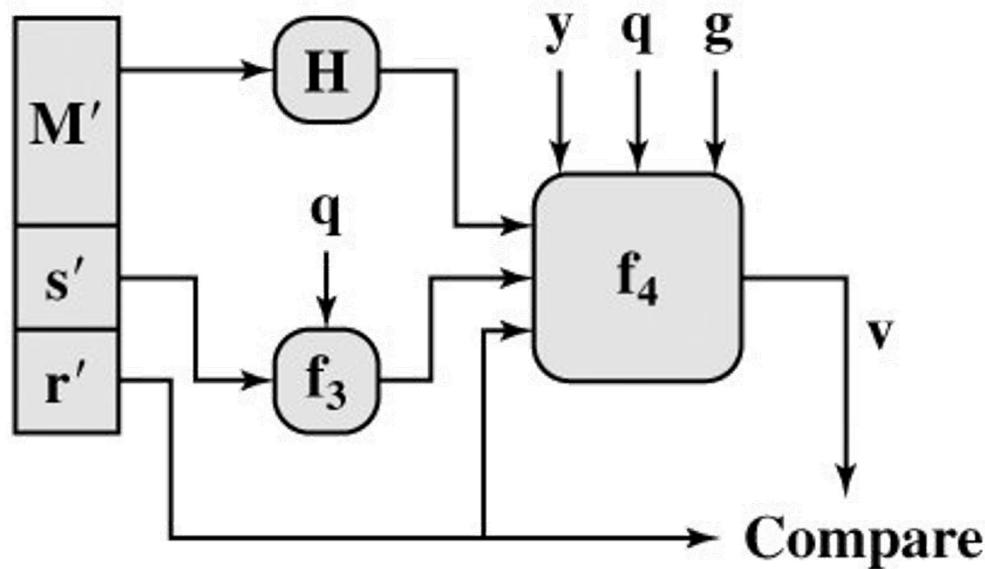
□ وارسی و تصدیق امضاء

- گیرنده M و (r,s) را دریافت می کند.
- مقادیر زیر را محاسبه می کند:
 - $w = s^{-1} \text{ mod } q$
 - $u1 = [H(M).w] \text{ mod } q$
 - $u2 = [r.w] \text{ mod } q$
 - $v = [(g^{u1}y^{u2}) \text{ mod } p] \text{ mod } q$

↑
کلید عمومی

■ اگر $v=r$ ، امضاء معتبر است.

فرآیند وارسی امضاء در DSS



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

$$\begin{aligned} v &= f_4(y, q, g, H(M'), w, r') \\ &= ((g^{(H(M'))w} \bmod q)^{r'w \bmod q}) \bmod p \bmod q \end{aligned}$$



استاندارد امضای دیجیتال

□ نکاتی درباره الگوریتم:

- مقدار ۲ مستقل از پیام محاسبه می‌شود.
- به k و ۳ پارامتر عمومی بستگی دارد.
- محاسبه k از روی ۲ و محاسبه X از روی ۵ از نظر محاسباتی دست نیافتنی است.
- دشواری محاسبه لگاریتم‌های گسته
- 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 خط مشی‌ها

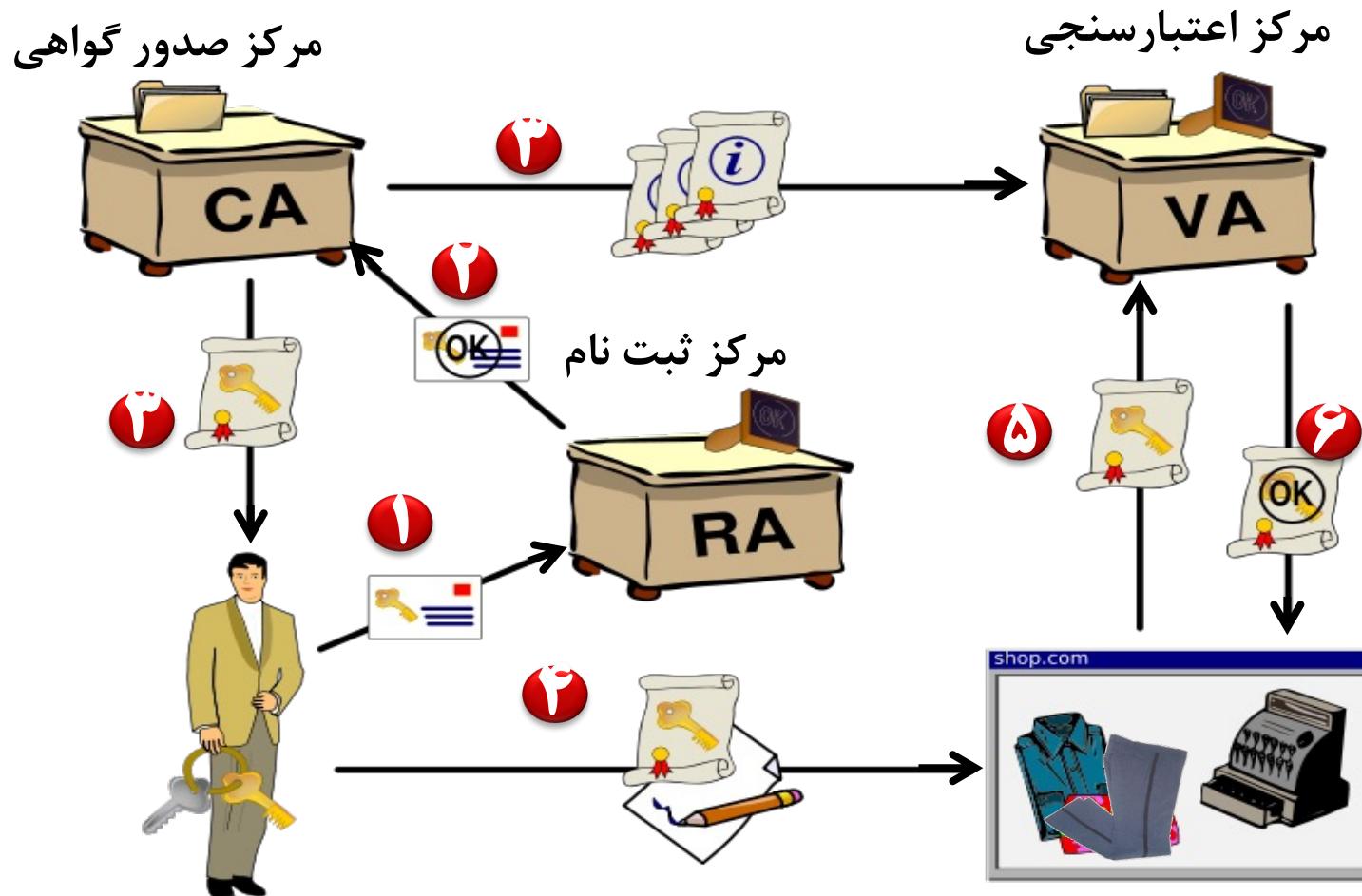


PKI مبانی

- نکته اصلی در رمزنگاری نامتقارن:
 - ”چه کسی کلید خصوصی متناظر با یک کلید عمومی را دارد؟“
 - در ارسال پیام رمز شده با کلید عمومی
 - در بررسی امضا فرد بر روی یک پیام
 - برای هر کلید عمومی باید یک گواهی از یک مرجع معترض 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.



در یک PKI





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 خط مشی‌ها



گواهی کلید عمومی

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

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

امضای مرکز صدور گواهی CA
بر روی گواهی

- برای وارسی صحت گواهی به کلید عمومی CA نیاز داریم.

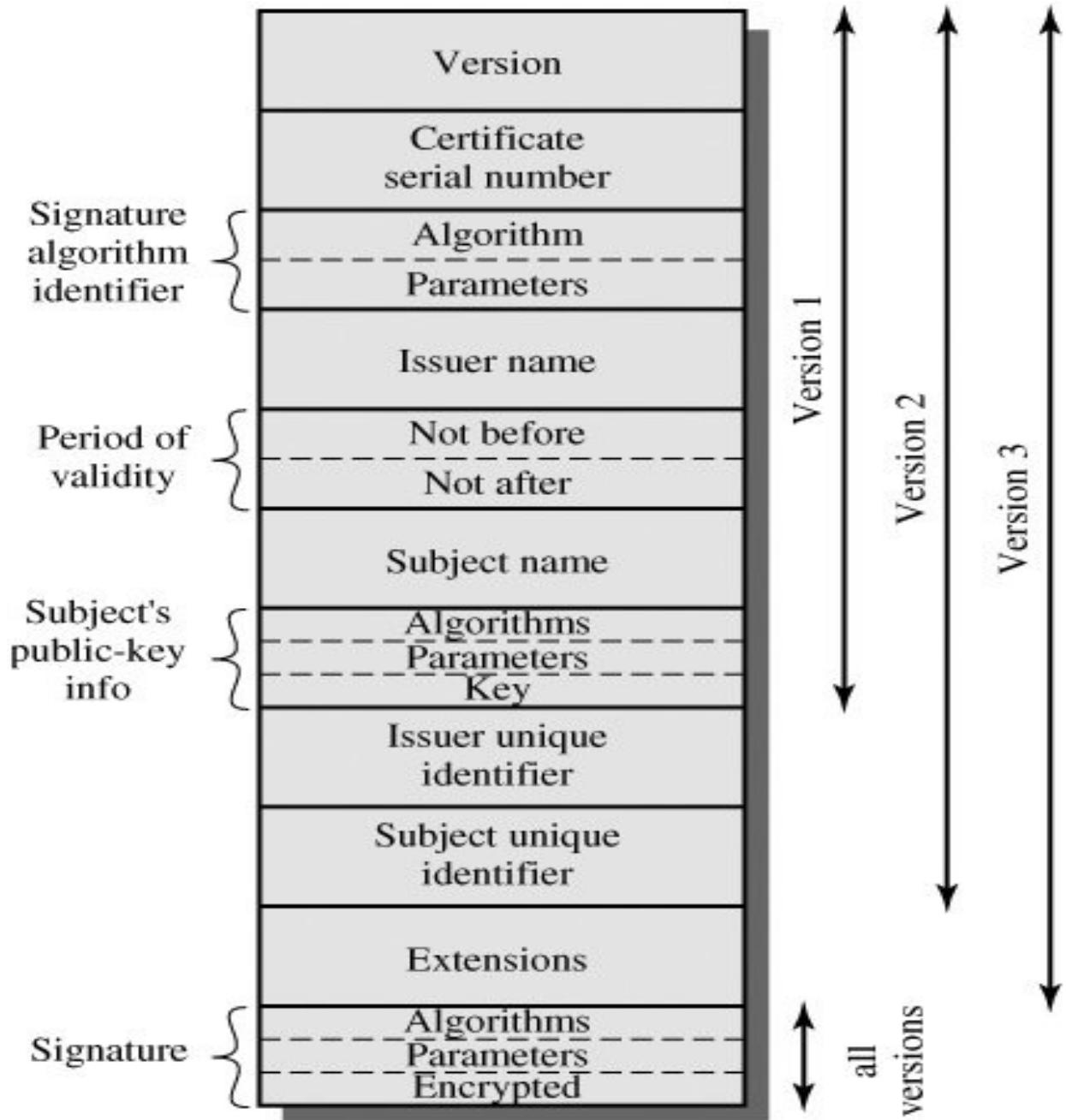


قالب گواهی X.509

- 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 باطل شده در این استاندارد تعریف شده است.



ساختار گواهی دیجیتال X.509





قالب نام در گواهی X.509

طبق استاندارد X.500 برای شناسایی منحصر به فرد موجودیت‌ها در گواهی‌ها از حاوی فیلد‌های زیر استفاده می‌شود.

عنوان فیلد	توصیف فیلد
CN	Common Name (URL in SSL certificates)
O	Organization name
OU	Organizational Unit name
C	Country
ST (or SP or S)	State or Province name
STREET	Street / First line of address
PC	Postal code / zip code
UNSTRUCTUREDNAME	Host name
UNSTRUCTUREDADDRESS	IP address



کواہی 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



ابطال 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.



ابطال گواهی

□ دو رویکرد:

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

استفاده از لیست **CRL**

- هر کس هرگاه گواهی خواست، از مرکز مورد اعتماد درخواست کند. یا به صورت برخط وضعیت گواهی را بررسی نماید.

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.

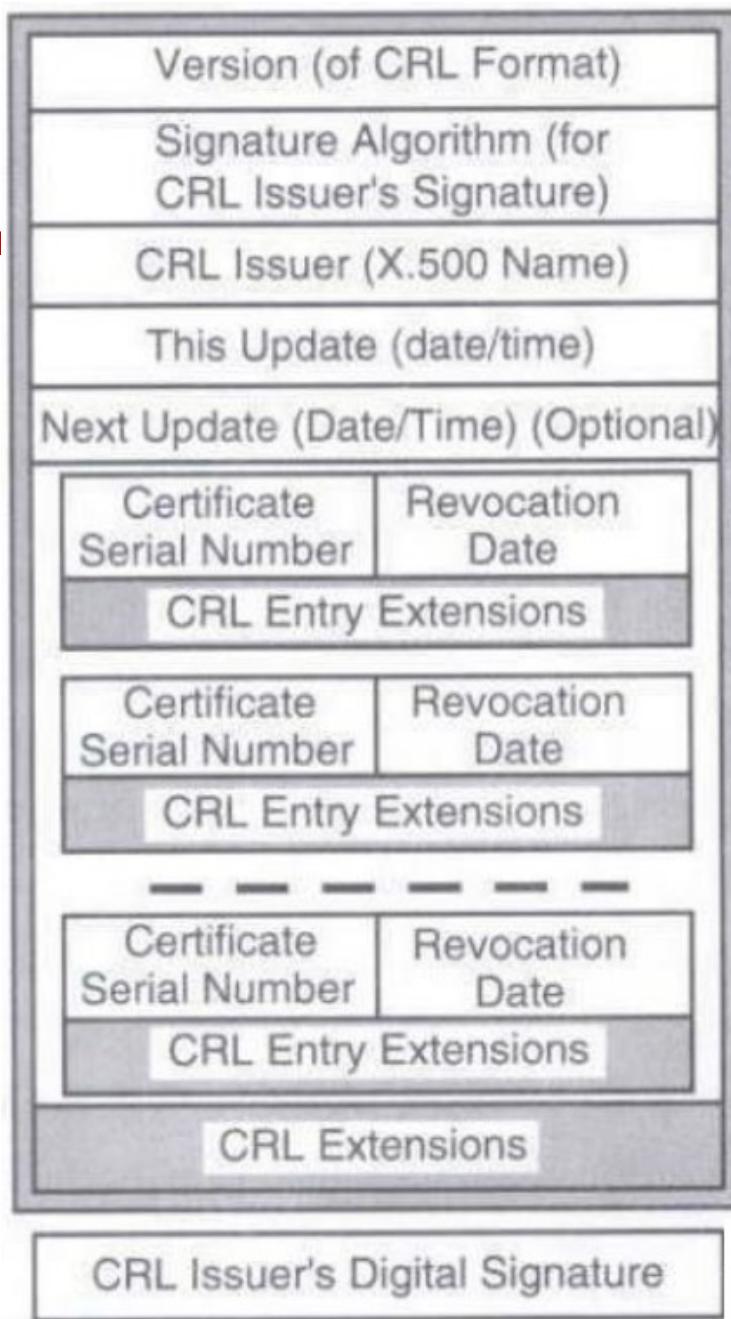
□ انواع CRL:

■ **Full CRL** در دوره‌های زمانی مشخص، مرکز CA لیست کامل گواهی‌های نامعتبر را منتشر می‌کند.

■ **Delta CRL** لیست گواهی‌های باطل شده اخیر (که تاریخ ابطال آنها بعد از تاریخ انتشار آخرین CRL است) را منتشر می‌کند.



X.509 CRL در ساختار





ابطال گواهی - CRL

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 ~e 1e 01 50 10 03 00 EF 7d 02 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



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 Responder، اصطلاحاً گفته می‌شود.
- مزیت نسبت به CRL: به دلیل برخط بودن اطمینان بیشتری را از وضعیت فعلی گواهی فراهم می‌نماید.
- عیب نسبت به CRL: نیاز به برخط بودن OCSP Responder



نسخه‌برداری و بازیابی کلید

□ کلید به دلایل مختلف ممکن است از دست برود! داده‌ها غیر قابل دسترس می‌شوند. باید امکانی برای بازیابی کلید وجود داشته باشد.

□ دلایل نسخه‌برداری کلید

- گم شدن،
- پاک شدن کلید،
- خرابی رسانه‌ای که کلیدها روی آن ذخیره شده است.



نسخه برداری و بازیابی کلید

- به لحاظ نظری بهتر است دو زوج کلید برای هر کاربر وجود داشته باشد:
- زوج کلید رمزنگاری: **نیازمند پشتیبان‌گیری** (چون در صورت از دست رفتن کلید نمی‌توانیم داده‌های قبلی را رمزگشایی کنیم.)
- زوج کلید امضاء: **عدم نیاز به پشتیبان** (چون در صورت از دست رفتن کلید می‌توانیم جفت کلید جدید تولید کنیم.)



بازتولید کلید و گواهی

□ نباید کلیدها ابدی باشند. پس باید:

- کلیدها را بروز آورد یا **بازتولید** (renew) کرد.
- سابقه زوج **کلیدهای رمزنگاری** قبلی (که برای محرمانگی داده به کار رفته) را نگه داشت تا دادههای رمز شده با زوج قبلی قابل رمزگشایی باشند.
- در نقطه مقابل برای بروزرسانی **کلیدهای امضاء** باید کاملاً کلید فعلی را نابود کرد!
- بروزآوری و بازتولید کلید و گواهی باید قبل از انقضاء صورت پذیرد.



نگهداشت کلید خصوصی و گواهی (ماژول‌های رمزنگاری)

ماژول رمزنگاری: مجموعه نرمافزار و سختافزاری که عملکرد رمزنگاری را به صورت امن و غیرقابل خدشهای پیاده‌سازی می‌کند و نگهداری و استفاده از کلیدهای سری و خصوصی در مرز مشخصی محصور است.

□ وظایف اصلی ماژول رمزنگاری

- تولید امن و تصادفی کلیدهای رمزنگاری (متقارن یا نامتقارن)
- نگهداری امن کلیدهای محترمانه و خصوصی
- رمزنگاری و رمزگشایی با کلید خصوصی (یا محترمانه) در محیطی امن
- نگهداری گواهی‌های کلید عمومی مرتبط با کلیدهای خصوصی



نگهداری کلید خصوصی و گواهی

□ انواع مازول‌های رمزگاری سخت‌افزاری:



- توکن
- کارت هوشمند
- مولفه امن موبایل (Secure Element)
- مازول سخت‌افزاری امن (HSM)

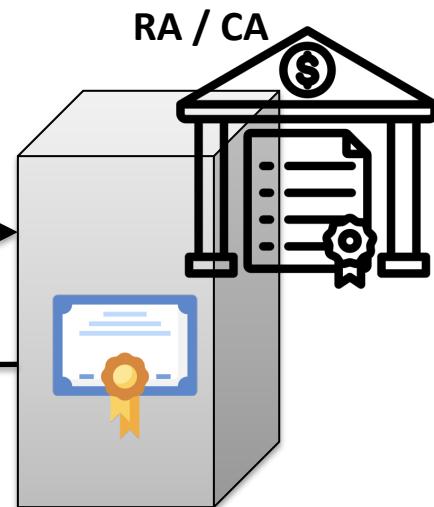
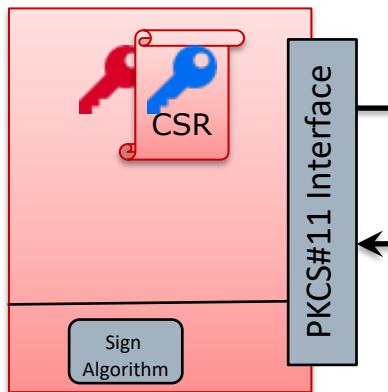




نحوه استفاده از ماثولهای رمزنگاری

تولید زوج کلید و دریافت گواهی

HSM/Token/Secure Element



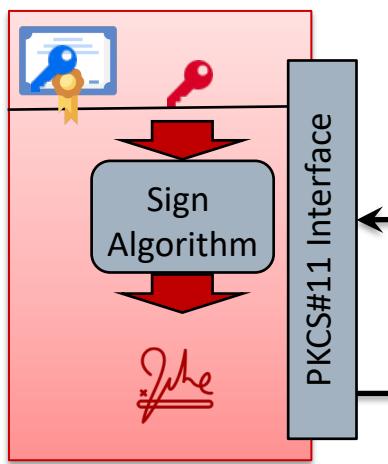
استاندارد قالب	فایل
PKCS#10	CSR
X.509	Public Key Certificate
PKCS#12	Private Key Storage



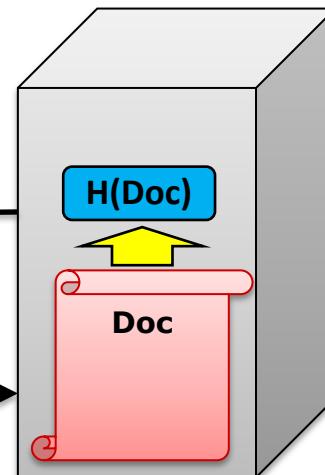
نحوه استفاده از ماثول های رمزگاری

امضای دیجیتال اسناد (داده ها)

HSM/Token/Secure Element



Application



استاندارد قالب	فایل
PKCS#7	Cryptographic Message Syntax (CMS)
PAdES	PDF Signature
XAdES	XML Signature



استاندارد امنیتی ماثولهای رمزنگاری

□ استاندارد FIPS 140-2

□ برای ارزیابی ماثولهای رمزنگاری ارایه شده است.

FIPS: Federal Information Processing Standards

□ دارای **چهار** سطح امنیتی (Level1 تا Level4) است.

□ در تهیه HSM باید حسب نیاز، سطح امنیتی مناسب آن را تعیین 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



مُؤْلَفَهَاتِ PKI

- کاربران یا دارندگان گواهی (End Users or Certificate Holders): کاربران انسانی، تجهیزات و هر آنچه که می‌تواند از گواهی استفاده نماید.
- مرکز ثبت نام (Registration Authority RA): مسئول دریافت درخواست گواهی، احراز هویت متقاضی و اطمینان از تعلق کلید به متقاضی.
- مرکز گواهی (Certificate Authority CA): مسئول تولید، مدیریت، توزیع گواهی و CRL.
- مخزن (Repository): ذخیره و انتشار گواهی‌ها و CRL‌ها (حداکثر کارآیی و دسترسی پذیری را لازم دارد).
- سرویس اعتبارسنجی (OCSP Responder): پاسخگویی به استعلام اعتبار و عدم ابطال گواهی‌ها.



مرکز ثبت نام RA

- قبل از ارائه درخواست به CA، **هویت متقاضی گواهی را احراز و اطلاعات لازم را جمعآوری و کنترل می‌کند.**
- اگر متقاضی قبلاً زوج کلید تولید کرده باشد، همان به CA ارسال می‌شود.
- در غیر این صورت RA و (یا CA) می‌تواند زوج کلید لازم را در حضور متقاضی تولید نماید.
- 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 زوج کلید و فایل CSR در سیستم‌عامل‌های مختلف به طور عملی بررسی شود.



احراز هویت متقاضی گواهی توسط RA

□ **فرد حقیقی:** مراجعه حضوری به دفاتر ثبت‌نام و احراز هویت بر اساس اسناد هویتی (مانند شناسنامه یا کارت ملی) یا احراز هویت غیرحضوری با روشهای بیومتریک (مانند تطابق چهره با عکس کارت ملی در ثبت احوال)

کاربردها:

- امضای دیجیتال اسناد و داده‌ها
- رمزنگاری و حفظ محربانگی
- امضای ایمیل
-

□ **فرد حقوقی (شرکت یا سازمان):** مراجعه حضوری نماینده قانونی شرکت/سازمان به دفاتر ثبت‌نام و وارسی اعتبار مدارک ثبتی ارایه شده توسط نماینده

کاربردها:

- امضا یا مهر سازمانی دیجیتال اسناد و داده‌ها
- رمزنگاری و حفظ محربانگی
- امضای گواهی‌های دیگر
-



احراز هویت متقاضی گواهی توسط RA

□ **وبسایت:** به یکی از روش‌های زیر:

کاربردها:

- برقراری ارتباطات امن با پروتکلهایی همچون SSL/TLS

■ **Domain Validation (DV):** بررسی مالکیت دامنه با ارسال ایمیل به admin@domain یا درخواست ثبت یک رکورد متنی با محتوای خاص در رکوردهای DNS دامنه

■ **Organization Validation (OV):** بررسی مالکیت دامنه (مشابه DV) و بررسی هویت شرکت/سازمان به صورت برخط (گاهی وارسی و استعلام از طریق شماره تلفن رسمی ثبت شده)

■ **Extended Validation (EV):** بررسی مالکیت دامنه و بررسی اعتبار مدارک ثبتی شرکت/سازمان ارایه شده توسط نماینده قانونی آن

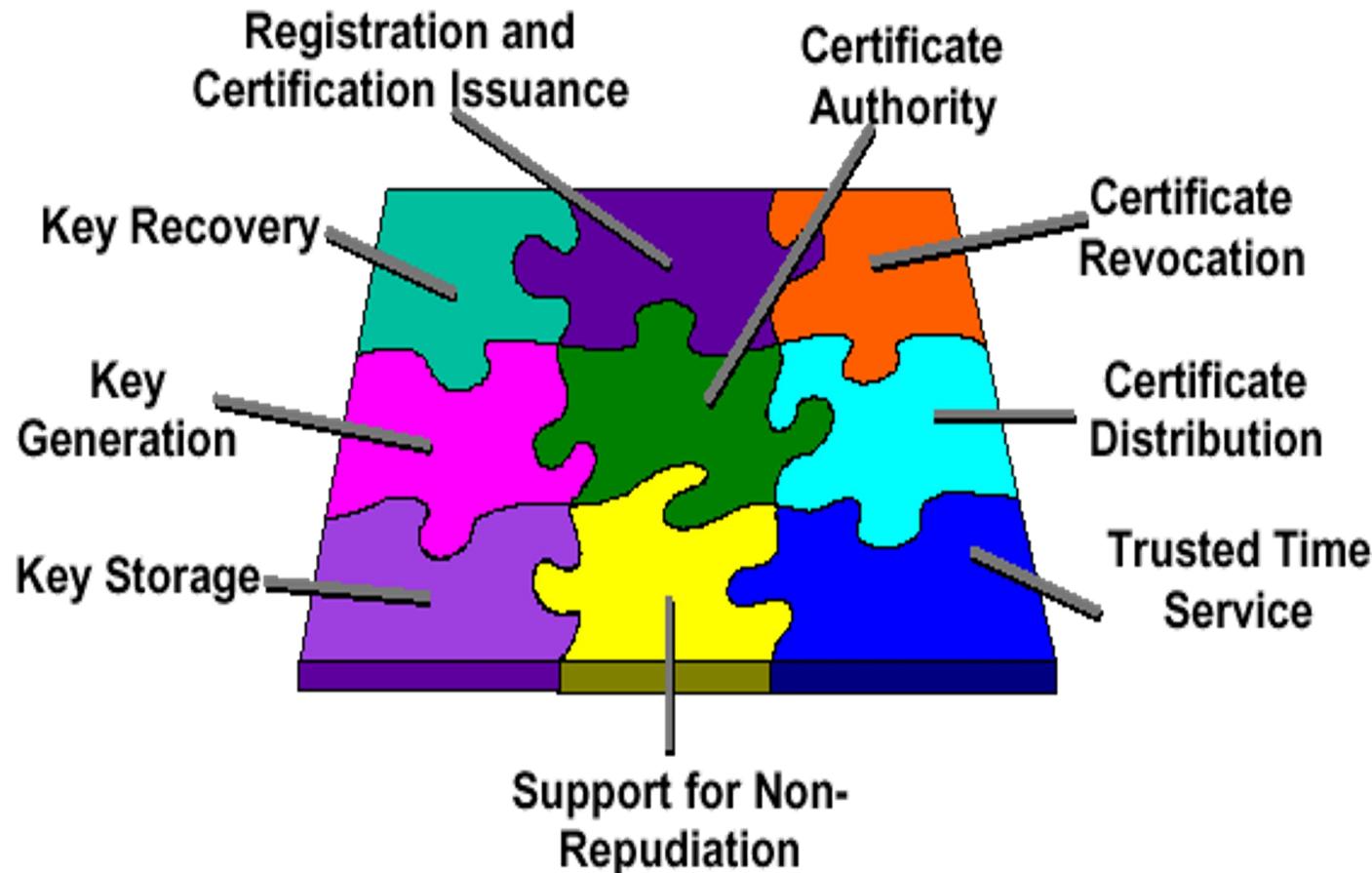


مرکز گواهی CA

- 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 گواهی و امضاء آن) برای کاربران و یا دیگر CAها.
- نگهداری وضعیت گواهی‌ها و تولید 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.



وظایف CA

- اولین وظیفه CA حفاظت از کلید خصوصی خودش است، حتی وقتی در حال پردازش است.
- زیرا اگر کلید خصوصی CA لو برود، همه گواهی‌های صادرهاش در معرض شک هستند و باید باطل شوند.



فهرست مطالب

- مبانی امضای دیجیتال
- استانداردهای امضای دیجیتال
- زیرساخت کلید عمومی (PKI)
- مبانی PKI
- گواهی دیجیتال و مدیریت آن
- مولفه‌های PKI
- معماřی PKI، رویه‌ها و خط مشی‌ها



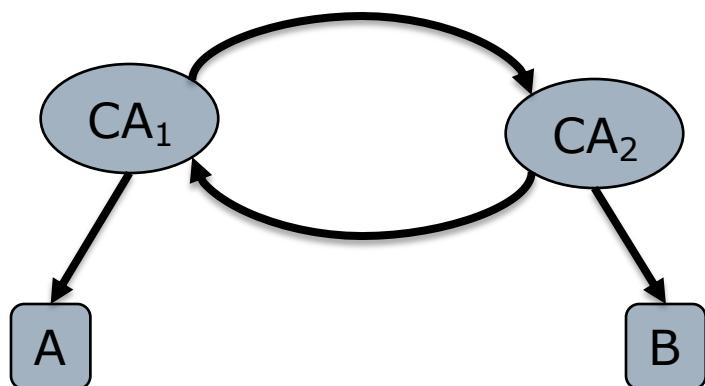
معماری PKI

- مادام که دارندگان گواهی از یک CA گرفته باشند مسأله ساده است.
- وقتی که دارندگان گواهی از CAهای مختلف گواهی گرفته باشند چگونه اعتماد کنند؟
- معماری ساده PKI (غیرعملی)
 - تنها یک CA در سازمان/کشور داشته باشیم (که عملی نیست).
 - وجود یک CA می‌تواند گلوگاه Single point of failure باشد و هرگونه اشکال منجر به لطمہ دیدن اعتماد و احتمالاً صدور مجدد گواهی‌ها شود.

گواهی ضربدری (Cross-Certificate)

□ گواهی ضربدری، گواهی‌ای است که یک CA برای CA دیگر صادر می‌کند تا گواهی‌های صادره توسط CA دوم توسط کاربران 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>> ■

به معنای گواهی
صادره CA برای کاربر A است.

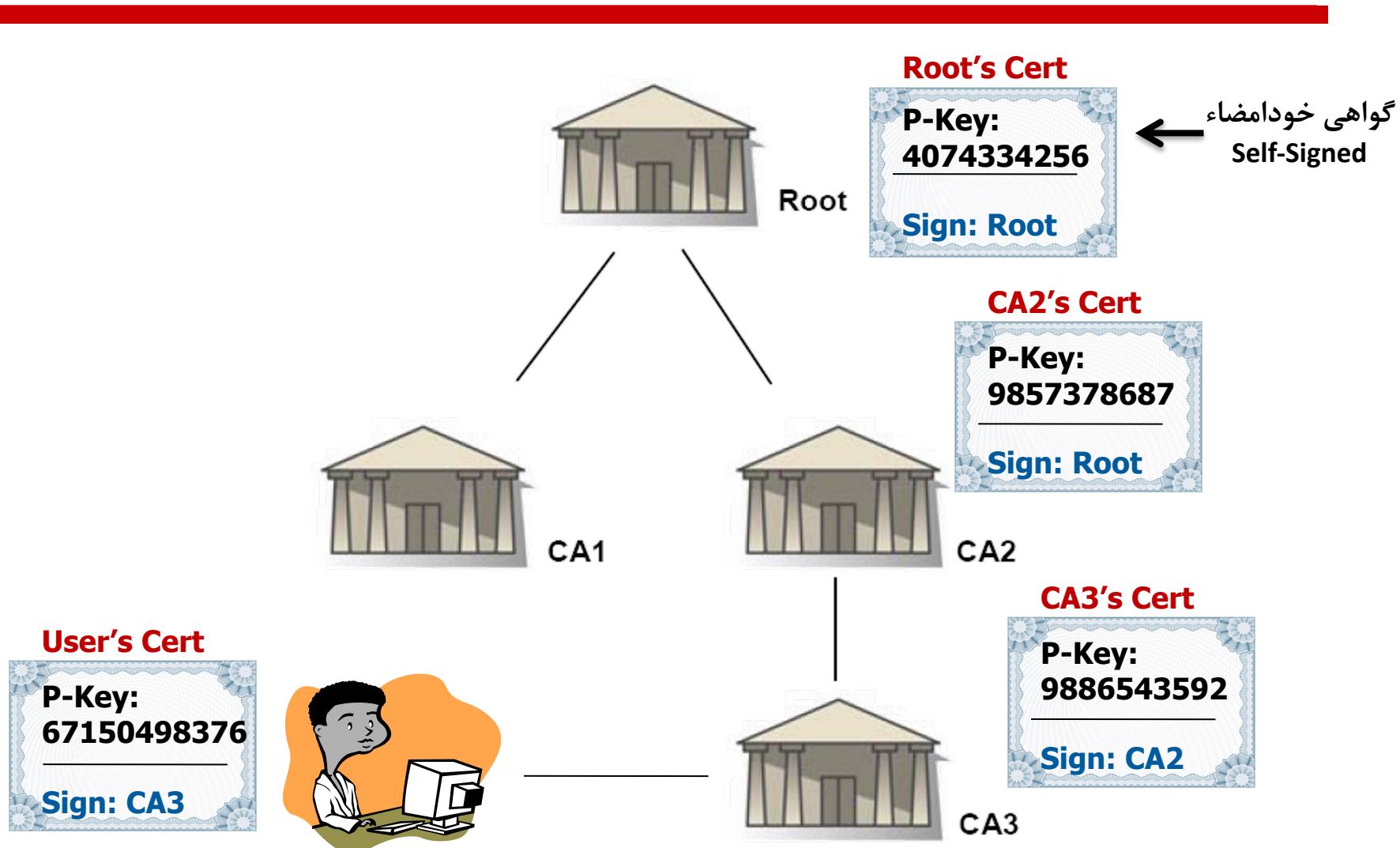


Enterprise PKI

- 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.

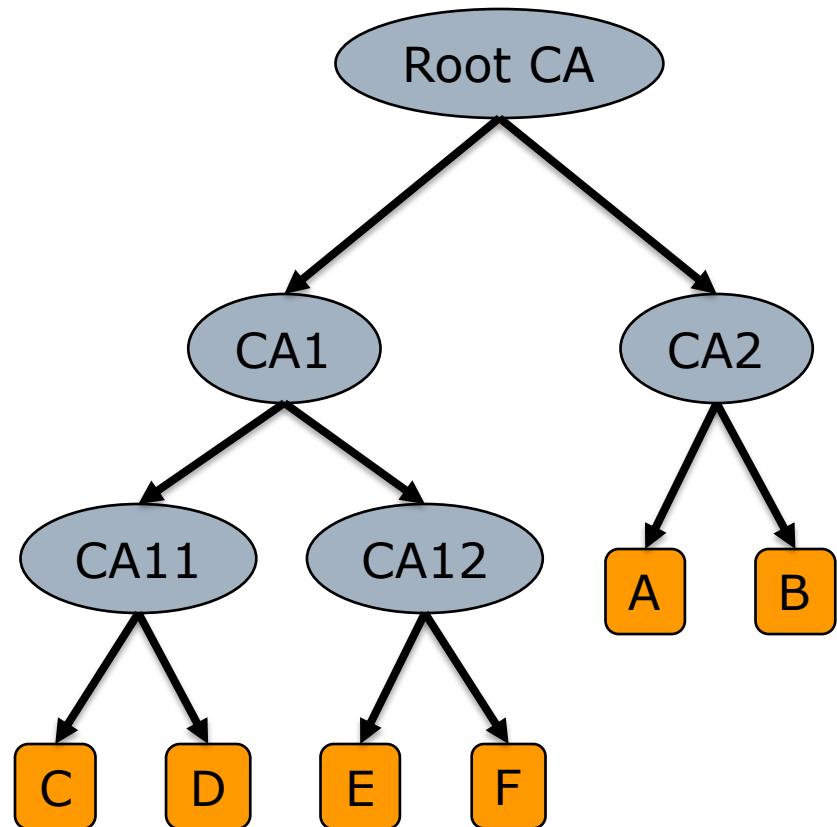


مدل سلسله مراتبی





مدل سلسله مراتبی



□ ساختار درختی از CA ها

□ ریشه و مجموعه‌ای CA میانی

□ مزایا:

■ توزیع کار و کاهش ریسک

■ کاهش هزینه برقراری امنیت فیزیکی

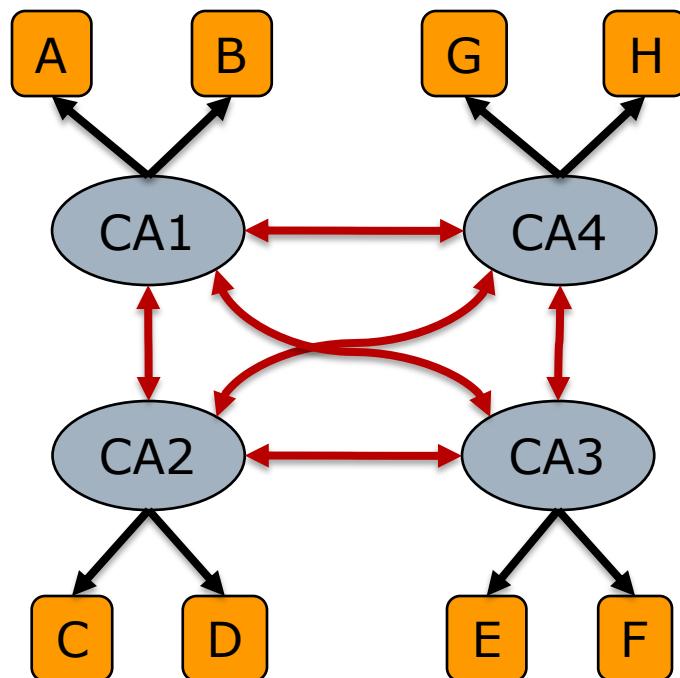
□ برای ریشه امنیت بالا نیاز است.

□ معایب:

■ همه CA ها را نمی‌توان در یک سلسله مراتب جای داد.

مدل توری

□ هر دو CA به یکدیگر گواهی ضربدری بدهند.



□ مزایا:

▪ استقلال CAها از یکدیگر

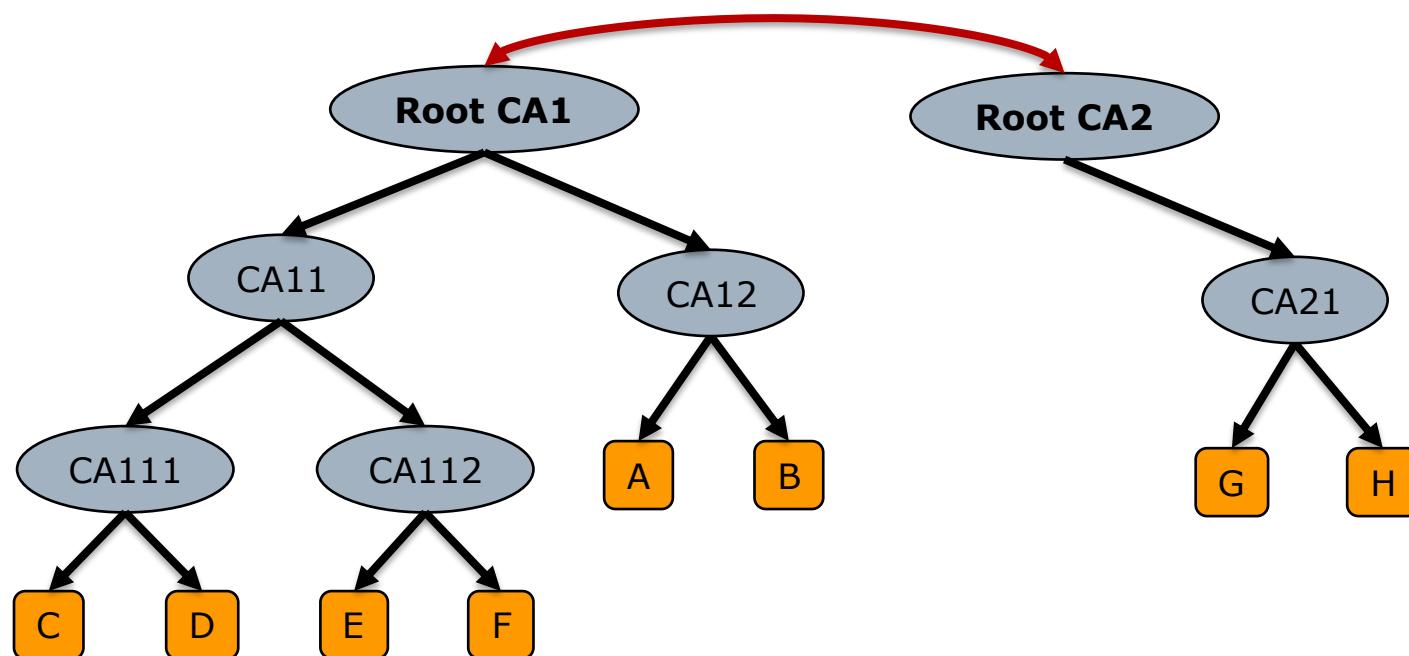
□ معایب:

▪ نیاز به صرف منابع و هزینه زیاد

▪ وضع سیاست‌های متفاوت توسط CAها

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 خط مشی‌ها

- 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 مخاطب متفاوت و هدف متفاوتی دارند.
- قالب استاندارد فعلی برای این دو مستند RFC 3647 است.



رویه‌ها و خط‌مشی‌ها

□ **CP** یک مستند سطح بالا متعلق به مرکز ریشه است که خط‌مشی و سیاست‌های صدور گواهی و نگهداری اطلاعات گواهی را شرح می‌دهد.

- شرح عملیات CA، انواع و سطوح مختلف گواهی‌ها، مسئولیت‌های کاربر برای درخواست، استفاده، و مدیریت کلیدها و گواهی‌ها را دارد.
- عمر این خط‌مشی و سیاست‌ها 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.



پایان

پست الکترونیکی

amini@sharif.edu

kharrazi@sharif.edu

یادداشتن و الامان



پیوست

معرفی ابزار OpenSSL



ابزار OpenSSL

□ OpenSSL دارای قابلیت‌ها مختلفی برای رمزنگاری و انجام امور مرتبط با زیرساخت کلید عمومی و امضای دیجیتال است.

□ مهم‌ترین قابلیت‌ها:

- تولید کلید به صورت تصادفی
- تولید درخواست گواهی CSR (مبتنی بر استاندارد PKCS#10)
- بررسی محتوای گواهی با فرمات‌های مختلف و تبدیل به فرمات‌های مختلف
- بررسی تطابق گواهی کلید عمومی با کلید خصوصی
- بررسی صحت کلید خصوصی، گواهی و ...
- رمزنگاری مبتنی بر الگوریتم‌های مختلف متقارن و یا نامتقارن
- تولید امضای دیجیتال مبتنی بر الگوریتم‌های مختلف نامتقارن



ابزار OpenSSL

□ برخی دستورات مفید و پرکاربرد

■ تولید زوج کلید RSA و تولید درخواست گواهی CSR

```
openssl req -out request.csr -new -newkey rsa:2048 -nodes -keyout  
private.key
```

■ مشاهده محتوای فایل درخواست گواهی CSR

```
openssl req -text -noout -verify -in request.csr
```

■ مشاهده محتوای یک گواهی

```
openssl x509 -in certificate.crt -text -noout
```

■ کنترل تطابق کلید خصوصی و گواهی RSA (خروجی هر دو باید یکسان باشد)

```
openssl rsa -modulus -noout -in private.key | openssl md5
```

```
openssl x509 -modulus -noout -in certificate.crt | openssl md5
```



ابزار OpenSSL

□ برخی دستورات مفید و پرکاربرد

■ تولید فایل با فرمت **pfx**. از فایل گواهی و کلید خصوصی

```
openssl pkcs12 -export -out certkey.pfx -inkey private.key -in  
certificate.crt -certfile chain.crt
```

■ مشاهده محتوای فایل **CRL**

```
openssl crl -in crlfile.crl -inform DER -text -noout
```

■ تبدیل فایل با فرمت **.cer/.p7b/.p7c**. به فرمت **.cer/.p7b/.p7c**.

```
openssl pkcs7 -print_certs -inform der -in infile.p7b -out outfile.cer
```