باسمه تعالی

درس: آزمایشگاه امنیت شبکه

نام و نام خانوادگی: هادی امینی

شماره دانشجویی: 9912762370

شماره آزمایش : 04

تاریخ تحویل: 1403/02/13

موضوع: **PKI**

بررسی زیرساخت کلید عمومی(PKI)

زیرساخت کلید عمومی (PKI) مجموعه‌ای از سخت‌افزار، نرم‌افزار، افراد، سیاست‌ها و رویه‌ها است که برای مدیریت، توزیع، استفاده، ذخیره و ابطال گواهی‌های دیجیتال به کار می‌رود. گواهی‌های دیجیتال، هویت دیجیتال افراد و سازمان‌ها را تأیید می‌کنند و امکان رمزنگاری امن داده‌ها و احراز هویت را فراهم می‌کنند.

اجزای کلیدی PKI عبارتند از:

- **مرکز صدور گواهی :(CA)** مسئول صدور، تمدید و ابطال گواهی‌های دیجیتال است.
- **دفتر ثبت نام :**هویت متقاضیان گواهی را تأیید می‌کند.
- **ذخیره گواهی :**مخزن امنی برای ذخیره گواهی‌های دیجیتال است.
- **سیاست‌های :PKI** قوانین و رویه‌هایی را که نحوه عملکرد PKI را مشخص می‌کنند، تعریف می‌کنند.

مزایای استفاده از PKI عبارتند از:

- **محرمانگی :**از داده‌ها در برابر دسترسی غیرمجاز با استفاده از رمزنگاری محافظت می‌کند.
- **احراز هویت :**هویت افراد و سازمان‌ها را تأیید می‌کند.
- **عدم انکار :**اطمینان حاصل می‌کند که فرستنده و گیرنده یک پیام نمی‌توانند ارسال یا دریافت پیام را انکار کنند.
- **integritet:**اطمینان حاصل می‌کند که داده‌ها در حین انتقال دستکاری نشده‌اند.

برخی از چالش‌های استفاده از PKI عبارتند از:

- **مدیریت کلید :**مدیریت ایمن کلیدهای خصوصی برای جلوگیری از دسترسی غیرمجاز ضروری است.

- **اعتماد :**کاربران باید به CA که گواهی‌ها را صادر می‌کند، اعتماد کنند.
- **هزینه :**پیاده‌سازی و نگهداری PKI می‌تواند پرهزینه باشد.

گواهی‌های دیجیتال موجود:

گواهی‌های دیجیتال انواع مختلفی دارند که هر کدام کاربرد و ویژگی‌های خاص خود را دارند. برخی از رایج‌ترین گواهی‌های دیجیتال عبارتند از:

- **گواهی‌های :X.509** این نوع گواهی که در سال 1988 توسط ITU-T استانداردسازی شد، رایج‌ترین نوع گواهی دیجیتال است. گواهی‌های X.509 برای تأیید هویت افراد و سازمان‌ها، رمزنگاری داده‌ها و امضای دیجیتال استفاده می‌شوند.
- **گواهی‌های :S/MIME** این نوع گواهی برای رمزگذاری ایمیل و امضای دیجیتال ایمیل استفاده می‌شود.
- **گواهی‌های :TLS/SSL** این نوع گواهی برای امن کردن اتصالات وب استفاده می‌شود.
- **گواهی‌های :OpenPGP** این نوع گواهی برای رمزگذاری ایمیل، امضای دیجیتال و رمزنگاری فایل‌ها استفاده می‌شود.

گواهی‌های:X.509

گواهی‌های X.509 مشتمل بر اطلاعات مختلفی از جمله موارد زیر هستند:

- **موضوع :**نام صاحب گواهی
- **صادر کننده :**نام CA که گواهی را صادر کرده است
- **محدوده زمانی اعتبار :**تاریخ شروع و پایان اعتبار گواهی
- **کلید عمومی :**کلید عمومی صاحب گواهی
- **اثر انگشت :**یک رشته منحصر به فرد که برای شناسایی گواهی استفاده می‌شود
- **استفاده‌های مجاز :**برنامه‌هایی که می‌توان از گواهی برای آنها استفاده کرد

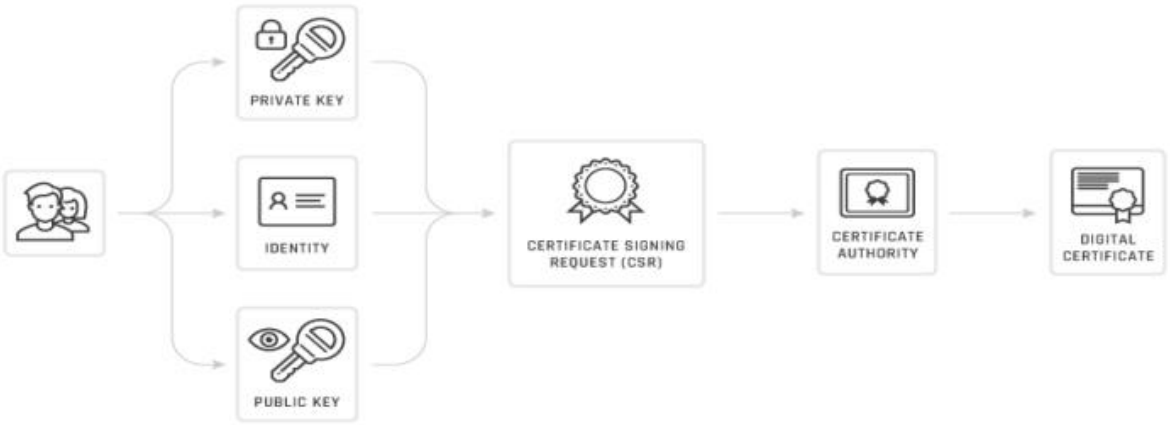
گواهی‌های:X.509x

گواهی‌های X.509x نسخه جدیدتر گواهی‌های X.509 هستند که شامل ویژگی‌های امنیتی جدیدی هستند. برخی از ویژگی‌های جدید گواهی‌های X.509x عبارتند از:

- **الگوریتم‌های رمزنگاری قوی‌تر :**گواهی‌های X.509x از الگوریتم‌های رمزنگاری قوی‌تر مانند RSA با 4096 بیت و ECCاستفاده می‌کنند.
- **مقاومت در برابر حملات :**گواهی‌های X.509x در برابر حملات هکری مانند حملات man-in-the-middle و حملات جعل هویت مقاوم‌تر هستند.

- **مدیریت کلید آسان‌تر :**گواهی‌های X.509x مدیریت کلید را آسان‌تر می‌کنند و نیاز به تمدید گواهی‌های مکرر را کاهش می‌دهند.

نحوه اعتبار سنجی گواهی SSL:

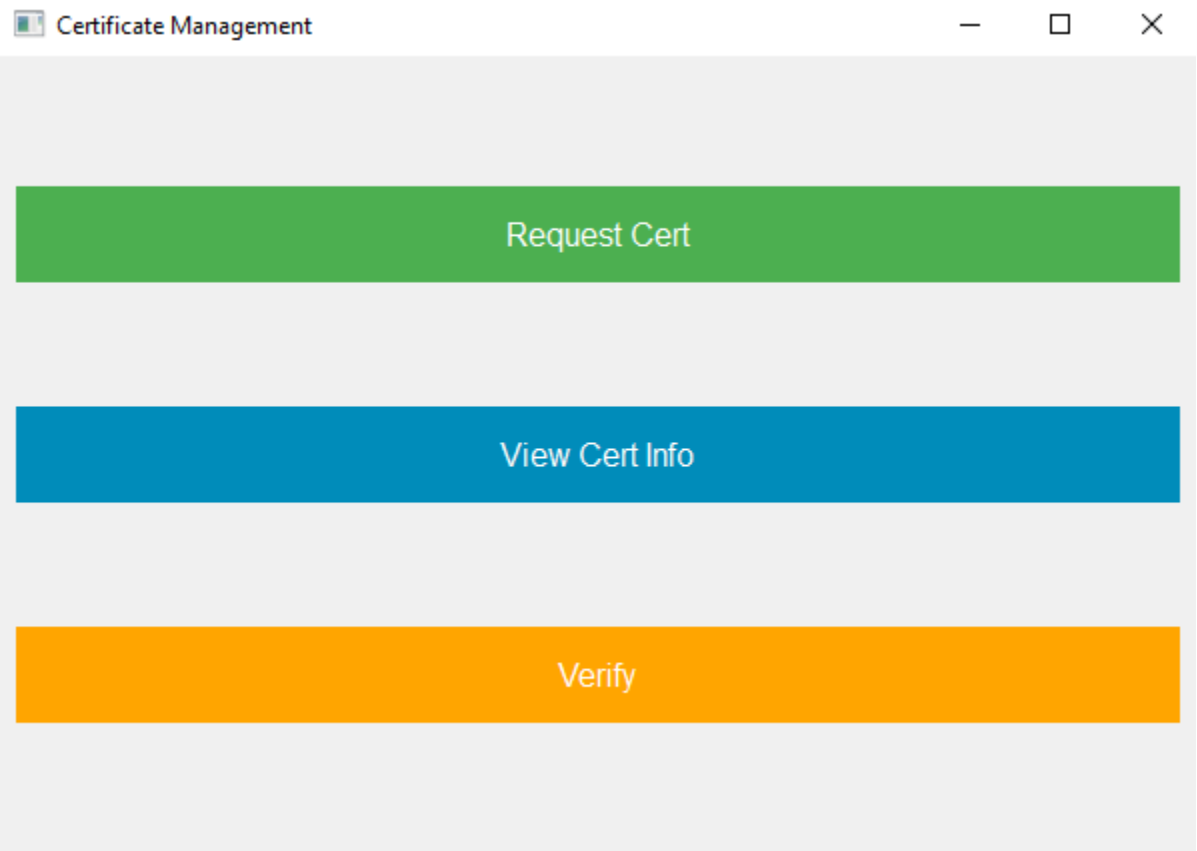


در این نمودار، گام‌های زیر به ترتیب نشان داده شده‌اند:

1. **درخواست گواهی :**
   - کاربر درخواست گواهی را به (RA) ارسال می‌کند.
   - درخواست شامل اطلاعاتی مانند نام کاربر، سازمان و آدرس ایمیل است.
2. **تأیید هویت :**
   - RAهویت کاربر را تأیید می‌کند.
   - این کار می‌تواند از طریق روش‌های مختلفی مانند تأیید هویت شخص ثالث، تأیید هویت ایمیل یا تأیید هویت از طریق اسناد انجام شود.
3. **صدور گواهی :**
   - اگر هویت کاربر تأیید شود، CAیک گواهی دیجیتال صادر می‌کند.
   - گواهی شامل کلید عمومی کاربر و اطلاعاتی در مورد CA است.
4. **استفاده از گواهی :**
   - کاربر می‌تواند از گواهی برای احراز هویت خود در هنگام دسترسی به منابع محافظت‌شده استفاده کند.

- به عنوان مثال، کاربر می‌تواند از گواهی برای ورود به وب‌سایت، امضای دیجیتال ایمیل یا رمزگذاری داده‌ها استفاده کند.

نتایج:



تصویر1- رابط گرافیکی

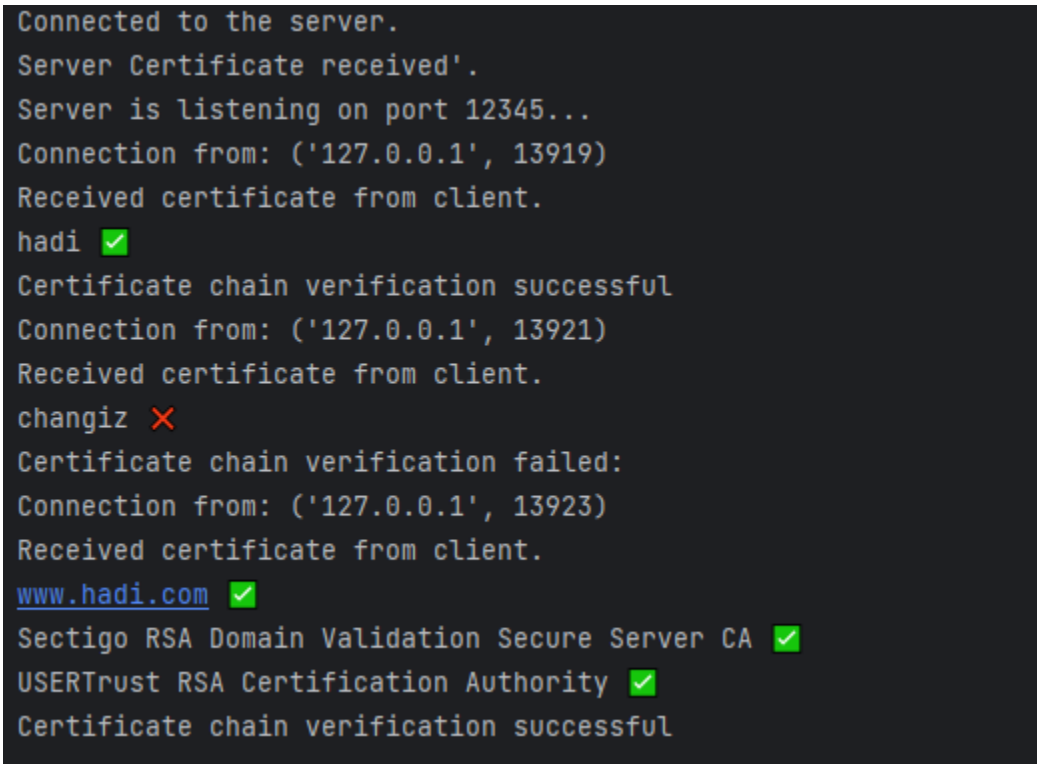
```
Connected to the RA
fdsklfsfklm not registered
Connected to the RA
Received certificate:
-----BEGIN CERTIFICATE-----
MIICqzCCAZOgAwIBAgIUD+4YF/I0rUAbLE+CuQqaJr9C50MwDQYJKoZIhvcNAQEL
BQAwEDEOMAwGA1UEAwwFTXkgQ0EwHhcNMjQwNTA4MDU1MTQyWhcNMjUwNTA4MDU1
MTQyWjAPMQ0wCwYDVQQDDARoYWRpMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAqFZ4sX+QUl0X0IQJwWqb1yE9njfbSvsbIWeHfv+6f4cZVU5yxnTG5zVv
oEQmMyoqbwjctMGuJP7AFTwM296mIOyfo/cv3zRGByXwRZzu2hVokiLjCzCaA+uL
SmZJb/8Ywg2wyJeldY8RL0YdHCxyClrPvjpkyY4jh9LYG1r3XEJMyviiEieXBqif
tfLvN6ZAw/75HXG6pkW3IsVtbl0Gu+f0S5+TSDo3fZSVEiA1rEZefm4HryCClZgm
FjhY9omU/uzz5bmjEBEw4QYs2iKNs3vhhs0n12FCZe6QMH4q2SALf5kJ8hoYZXrN
e3iWfZL7FeQgfWAyCLpEOTHVRipScQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAJ
tQmOTo+s6Gvj81qNnf9v+U5hTJw/qP4vx5lOyk9wvTuiVqdxjjzVjm601IXWDXPZ
rxBGoB+mOPGMq/an3uRbYsC42+4CCUyeZUUCuMQfHHo8gDXOND7fd9LPS+mUaD1s
KUcgitrHymBC6U5hXEgQbmRo5M97Hfv5G6peMJccYuh4YI8CRDlqVP9Zm1EY/NDi
a8J8Lw+moDHgbx6hLeCYDk228qBMB0FF86YOvNkJtgc2xVufMH9w5etuT6nJ6+pI
IB0CpdJA/8XFXuIT4HxasbGHfD+cmp+jc9PdMB/+owrOdY5A5hDHs4KLAjy1WxwW
lOUG2xjTX7Hb91PmUUer
-----END CERTIFICATE-----

Certificate received and saved to 'user_cert.crt'.
```

ارسال درخواست به RA و دریافت گواهی

```
ra listening on localhost:8888
Connected by ('127.0.0.1', 13967)
Received request from client: fdsklfsfklm
not registered
Connected by ('127.0.0.1', 13969)
Received request from client: hadi
certificate send
```

تصویر2- لاگ RA در PKI



تصویر3- لاگ VA