



وزارت ارتباطات و فناوری اطلاعات  
سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

# نحوه راه‌اندازی پروتکل SSL/TLS جهت برقراری ارتباط ایمن (HTTPS)

درخواست گواهی دیجیتال و پیکربندی آن بر روی سرویس‌دهنده‌ها



## فهرست مطالب

۱	مقدمه: اهمیت رمزنگاری و ارتباط ایمن	۱
۲	مراحل راه اندازی سرویس SSL/TLS بر روی سرویس دهنده وب	۱
2-1	انتخاب یک مرکز صدور گواهی بین المللی و رابط/نماینده آن در ایران	۱
۲-۲	انتخاب نوع گواهی مورد نظر	۲
2-3	تولید کلیدهای رمزنگاری و Certificate Signing Request (CSR)	۳
2-4	بررسی درخواست شما توسط مرکز صدور گواهی و صدور گواهی	۴
2-5	نصب گواهی و کلیدهای رمزنگاری بر روی سرویس دهنده	۴
۱-۵-۲	نصب گواهی امنیتی و کلیدهای رمزنگاری در APACHE	۵
۲-۵-۲	نصب گواهی امنیتی و کلیدهای رمزنگاری در IIS	۷
۶-۲	امن سازی پیکربندی SSL/TLS در سرویس دهنده	۹

## ۱ مقدمه: اهمیت رمزنگاری و ارتباط ایمن

با توجه به گسترده شدن استفاده از خدمات الکترونیک در سازمان‌ها و استفاده از شبکه اینترنت برای مبادله اطلاعات، نیاز است تا تمهیداتی برای امنیت داده‌های مبادله شده در اینترنت صورت پذیرد. برای تأمین محرمانگی و جامعیت داده‌های مبادله شده می‌توان از پروتکل‌های استاندارد که بدین منظور طراحی شده استفاده کرد. در حال حاضر مهم‌ترین پروتکل رمزنگاری که در سطح اینترنت برای رمزنگاری داده‌های لایه کاربرد و تأمین امنیت ارتباطات استفاده می‌شود، پروتکل SSL/TLS است که در وب با نام HTTPS نیز نامیده می‌شود. در این مستند فنی مراحل کلی و جزئیات راه‌اندازی سرویس HTTPS بیان می‌شود.

## ۲ مراحل راه‌اندازی سرویس SSL/TLS بر روی سرویس‌دهنده وب

### ۱-۲ انتخاب یک مرکز صدور گواهی بین‌المللی و رابط/نماینده آن در ایران

شما برای راه‌اندازی سرویس HTTPS نیاز به یک گواهی امنیتی (Security Certificate) دارید که می‌بایست توسط یکی از مراکز بین‌المللی صدور گواهی (CA یا Certificate Authority) صادر شده باشد. البته این گواهی را خود شما نیز می‌توانید ایجاد کنید ولی در این صورت یک گواهی خودامضا (Self-Signed) خواهید داشت که مرورگرها هنگام مواجهه با آن خطا می‌دهند. از آنجایی که گواهی‌های خودامضا توسط مهاجمین نیز قابل ایجاد و سواستفاده هستند، بهتر است برای امنیت بالاتر حتماً گواهی را از یک مرکز صدور گواهی معتبر دریافت کنید. بدین منظور ابتدا یکی از نمایندگان این شرکت‌ها در ایران را بیابید، و از جزئیات فنی و هزینه‌های آن آگاه شوید.

در صورتی که سایت شما دارای دامنه‌ای با پسوند .com/.net/.org. یا سایر دامنه‌هایی به جز .ir. می‌باشد، اغلب مراکز صدور گواهی، مشکلی با صدور گواهی برای دامنه شما ندارند. اما برای دامنه‌های .ir. تنها تعداد معدودی از مراکز بین‌المللی گواهی صادر می‌کنند. برای خرید گواهی دیجیتال از این مراکز بین‌المللی، باید از شرکت‌های واسط که بدین منظور در ایران فعالیت می‌کنند اقدام به خرید گواهی کرد. برخی از مراکز بین‌المللی صدور گواهی دیجیتال که دامنه .ir. را پشتیبانی می‌کنند در جدول زیر آمده است:

کشور	نام و آدرس مرکز صدور گواهی	نمونه سایت استفاده کننده
چین	WoSign <a href="https://www.wosign.com/english">https://www.wosign.com/english</a>	sslcheck.certcc.ir
ترکیه	TurkTrust <a href="http://www.turktrust.com.tr/en/">http://www.turktrust.com.tr/en/</a>	sadad.shaparak.ir ib.bsi.ir

chmail.ir ict.gov.ir sabteahval.ir ebanksepah.ir	<i>KEYNECTIS OpenTrust</i> <a href="https://www.opentrust.com/">https://www.opentrust.com/</a>	فرانسه
modern.izbank.ir pg.tejaratbank.ir	<i>Certum (Unizeto Technologies S.A.)</i> <a href="https://www.certum.eu">https://www.certum.eu</a>	لهستان
webmail.nri.ac.ir	<i>NetLock Kft</i> <a href="https://www.netlock.hu/">https://www.netlock.hu/</a>	مجارستان
---	<i>Let's Encrypt (ISRG)</i> <a href="https://letsencrypt.org">https://letsencrypt.org</a>	آمریکا*

\* مرکز گواهی Let's Encrypt، به صورت رایگان گواهی صادر می‌کند. اما با توجه به معماری مورد استفاده در آن، برای استفاده در مراکز دولتی به هیچ وجه توصیه نمی‌شود.

## ۲-۲ انتخاب نوع گواهی مورد نظر

در این مرحله باید با توجه به شرایط سازمان و نیازمندی‌ها، نوع گواهی امنیتی مد نظر خود را انتخاب نمایید. انواع مختلفی از گواهی‌نامه‌های SSL بر اساس تعداد دامنه و زیر دامنه‌های قابل پوشش به شرح زیر است:

- **Single** - تنها یک دامنه یا زیردامنه را در بر می‌گیرد.
- **Wildcard** - یک دامنه و تعداد نامحدود از زیردامنه‌های آن را پوشش می‌دهد.
- **Multi-Domain** - چندین دامنه را پوشش می‌دهد.

### نکات

- در صورتی که می‌خواهید تنها یک زیردامنه خاص را مجهز به سرویس SSL نمایید، از گواهی‌های Single استفاده نمایید که هزینه کمتری دارد.
- در صورتی که سازمان شما چندین زیردامنه دارد که می‌خواهید سرویس SSL را برای همه آنها فعال کنید، می‌توانید از یک گواهی Wildcard استفاده کنید. در این حالت کلیدهای رمزنگاری یکسانی در تمامی سرویس‌دهنده‌های شما مورد استفاده قرار خواهد گرفت.
- برای شرایطی که امنیت بالاتری مد نظر است و قصد به اشتراک گذاری کلید خصوصی بین سرویس‌دهنده‌های مختلف را ندارد، می‌توانید در کنار گواهی‌نامه Wildcard، برای برخی از زیردامنه‌ها گواهی مجزا از نوع single تهیه نمایید.

سطح اعتبار گواهی‌ها نیز متفاوت بوده و شامل موارد زیر است:

- **Domain Validation (DV)** - این سطح حداقل هزینه را دارد و اعتبارسنجی‌های پایه را پوشش می‌دهد. در این حالت صدور گواهی بر این مبنا صورت می‌گیرد که مرکز صدور گواهی اطمینان حاصل می‌کند که کلید عمومی موجود در گواهی، توسط مالک دامنه ساخته شده است (ولذا کلید خصوصی آن تنها در اختیار مالک دامنه است و نه فرد دیگری). گرفتن این گواهی ممکن است چند دقیقه تا چند ساعت طول بکشد.
- **Organization Validation (OV)** - علاوه بر اعتبارسنجی مربوط به مالکیت دامنه، جزئیات خاصی از مالک (مثل نام و آدرس) هم تصدیق اصالت می‌شود. گرفتن این گواهی ممکن است چند ساعت الی چند روز طول بکشد.
- **Extended Validation (EV)** - این مورد بالاترین درجه از امنیت را فراهم می‌آورد زیرا قبل از صدور این گواهی، بررسی‌های کاملی روی آن انجام شده است و مورد تایید است. گرفتن این گواهی معمولاً بین چند روز الی چند هفته طول می‌کشد.

## ۳-۲ تولید کلیدهای رمزنگاری و Certificate Signing Request (CSR)

ابتدا می‌بایست، بر اساس مستندات مرکز صدور گواهی که در مرحله ۱ انتخاب کرده اید کلید عمومی و خصوصی مربوط به سرویس دهنده خود را ایجاد نمایید. کلید خصوصی می‌بایست نزد شما به صورت محرمانه باقی بماند و حتی نمی‌بایست برای مرکز صدور گواهی نیز ارسال شود. کلید عمومی در قالب CSR برای مرکز صدور گواهی ارسال می‌شود تا مرکز صدور گواهی پس از انجام بررسی‌های لازم آن را امضا کند. در حقیقت در CSR شما تنها کلید عمومی و دامنه/دامنه‌های مد نظر و مشخصات سازمان خود را برای مرکز صدور گواهی ارسال می‌کنید. با توجه به نوع گواهی مد نظر، مرکز صدور گواهی ممکن است مدارک دیگری را نیز از شما درخواست نماید.

### نکات

- تولید کلیدهای رمزنگاری و CSR در هر سیستمی قابل انجام است و لازم نیست حتماً بر روی سرویس دهنده ای انجام شود که می‌خواهید بر روی آن SSL را فعال کنید. به عنوان مثال در صورتی که یک سرویس دهنده Windows/IIS دارید، می‌توانید CSR آن را با استفاده از یک سیستم لینوکس تولید کنید.
- امنیت سرویس SSL شما کاملاً وابسته به کلید خصوصی ایجاد شده در این مرحله است. این کلید خصوصی را در جایی محافظت شده قرار دهید.

- در تولید CSR برای دامنه‌های wildcard مانند \*.domain.ir دقت کنید که بهتر است حتماً فیلد SAN یا SubjectAlternateName را هم پر کرده و دامنه بدون پیشوند خود را (یعنی domain.ir) در آن قرار دهید. این کار سبب می‌شود که گواهی صادر شده برای نام دامنه بدون هیچ پیشوندی هم معتبر باشد (برای خود domain.ir). در این حالت پس از نصب و فعالسازی SSL، با وارد کردن آدرس زیر در مرورگر فایرفاکس خطای گواهی نخواهید داشت:  
<https://domain.ir>

### تولید CSR نمونه با استفاده از ابزار OpenSSL

یک نمونه روش تولید CSR برای دامنه های \*.domain.ir با استفاده از ابزار openssl را ذیلاً مشاهده می‌کنید. در این CSR خود دامنه domain.ir (بدون پیشوند) هم در بخش SubjectAltName قرار داده‌ایم.

```
openssl req -nodes -newkey rsa:2048 -keyout public_private.key -out domain.ir.csr -subj  
'/C=IR/ST=Tehran/L=Tehran/O=Organization/OU=IT/CN=*.domain.ir/subjectAltName=D  
NS.1=*.domain.ir,DNS.2=domain.ir'
```

با اجرای دستور فوق دو فایل ایجاد می‌شود که یکی حاوی کلیدهای رمزنگاری است و دیگری حاوی CSR. تنها فایل CSR می‌بایست برای مرکز صدور گواهی ارسال شود و فایل کلیدها بصورت محرمانه نزد شما باقی بماند تا بعداً بر روی سرویس دهنده خود نصب کنید.

## ۴-۲ بررسی درخواست شما توسط مرکز صدور گواهی و صدور گواهی

CA، CSR ارسالی توسط شما را بررسی کرده و یک گواهی امنیتی که به صورت یک یا چند فایل است در اختیار شما قرار می‌دهد. غالباً این گواهی شامل یک فایل با پسوند cer برای دامنه شما است. البته برخی از مراکز صدور گواهی یک یا تعداد دیگری فایل cer حاوی گواهی مراکز CA میانی و نهایتاً یکی از CA های اصلی نیز برای شما ارسال می‌کنند.

## ۵-۲ نصب گواهی و کلیدهای رمزنگاری بر روی سرویس دهنده

با توجه به اینکه از چه نوع سرویس‌دهنده ای استفاده می‌کنید، می‌توانید به راحتی گواهی و کلیدهای رمزنگاری را بر روی سرویس دهنده نصب کنید. مستندات فنی این کار هم توسط مراکز

صدور گواهی و هم از طریق منابع اینترنتی قابل دسترسی است. در این گزارش مراحل دو نمونه پیکربندی برای سرویس دهنده های پر کاربرد IIS و Apache است، بیان می شود.

## ۲-۵-۱ نصب گواهی امنیتی و کلیدهای رمزنگاری در APACHE

مراحل زیر را دنبال کنید:

### ۱. کپی فایل های گواهی نامه به سرور

گواهی های میانی (CA.crt) و اصلی (Your\_domain\_name.cert) را دانلود کنید و سپس آنها را در سرور خود و در مسیری مورد نظر کپی کنید. این شاخه فقط توسط مدیر سیستم (root) باید قابل دسترس باشد.

### ۲. فایل پیکربندی آپاچی را برای ویرایش پیدا کنید

مکان و نام فایل های پیکربندی در سرورهای مختلف ممکن است متفاوت باشد، مخصوصاً اگر شما از واسط خاصی برای مدیریت پیکربندی سرور استفاده می کنید.

نام فایل پیکربندی سرور آپاچی httpd.conf یا apache2.conf است. مکان ذخیره سازی این فایل ممکن است /etc/httpd/ یا /etc/apache2/ باشد. برای مشاهده یک لیست جامع از پیش فرض های نصب آپاچی روی سیستم عامل ها و توزیع های مختلف لینوکس به لینک زیر مراجعه کنید:

<http://wiki.apache.org/httpd/DefaultLayout>

غالباً پیکربندی گواهی نامه SSL در بلوک <VirtualHost> و در فایل پیکربندی متفاوتی قرار دارد. فایل های پیکربندی ممکن است در مسیرهای زیر یا در یک فایل به اسم ssl.conf باشند:

/etc/httpd/vhosts.d/

/etc/httpd/sites/

یکی از راه ها برای یافتن فایل پیکربندی مناسب در توزیع های لینوکس این است که با استفاده از grep مانند مثال زیر جستجو کنیم.

```
grep -i -r "SSLCertificateFile" /etc/httpd/
```

که "/etc/httpd/" مسیر پایه برای نصب آپاچی شما است.

### ۳. شناسایی بلاک <VirtualHost> برای پیکربندی

اگر شما نیاز دارید که سایت شما توسط هر دو پروتکل ارتباطی امن (https) و ناامن (http) قابل دسترسی باشد، شما برای هر نوع ارتباط نیاز به یک میزبان مجازی دارید. ابتدا یک کپی از میزبان مجازی ناامن که موجود است تهیه کنید و سپس آن را برای SSL به صورتی که در قدم چهارم توصیف شده، پیکربندی کنید.

#### ۴. پیکربندی بلاک <VirtualHost> برای فعال کردن SSL

در زیر یک مثال ساده از پیکربندی یک میزبان مجازی برای SSL بیان شده است. قسمت‌های پررنگ شامل قسمت‌هایی هستند که باید برای پیکربندی SSL اضافه شوند.

```
<VirtualHost 192.168.0.1:443>  
    DocumentRoot /var/www/html2  
    ServerName www.yourdomain.com  
    SSLEngine on  
    SSLCertificateFile /path/to/your_domain_name.crt  
    SSLCertificateKeyFile /path/to/your_private.key  
    SSLCertificateChainFile /path/to/YourCA.crt  
</VirtualHost>
```

سازگار کردن نام فایل‌ها برای هماهنگی با فایل‌ها گواهی شما:

- SSLCertificateFile باید فایل گواهی‌نامه دریافتی از مرکز صدور گواهی باشد.
- SSLCertificateKeyFile باید فایل کلید تولید شده در زمان ساخت CSR باشد.
- SSLCertificateChainFile باید فایل گواهی‌نامه میانی مرکز صدور گواهی باشد.

اگر فایل SSLCertificateChainFile کار نمی‌کند، به جای آن با استفاده از فایل SSLCACertificateFile امتحان کنید.

#### ۵. پیکربندی آپاچی را قبل از راه‌اندازی مجدد تست کنید

همیشه بهتر است فایل‌های پیکربندی آپاچی را برای هر خطا قبل از راه‌اندازی مجدد بررسی کنید، زیرا اگر فایل پیکربندی آپاچی خطا داشته باشد، آپاچی نمی‌تواند دوباره اجرا شود. دستور زیر را اجرا کنید: (روی بعضی سیستم‌ها، apache2ctl است)

```
apachectl configtest
```

#### ۶. راه‌اندازی مجدد آپاچی

شما می‌توانید از دستور apachectl برای شروع و متوقف کردن آپاچی با پشتیبانی SSL استفاده کنید.

```
apachectl stop
```

```
apachectl start
```



## ۲-۵-۲ نصب گواهی امنیتی و کلیدهای رمزنگاری در IIS

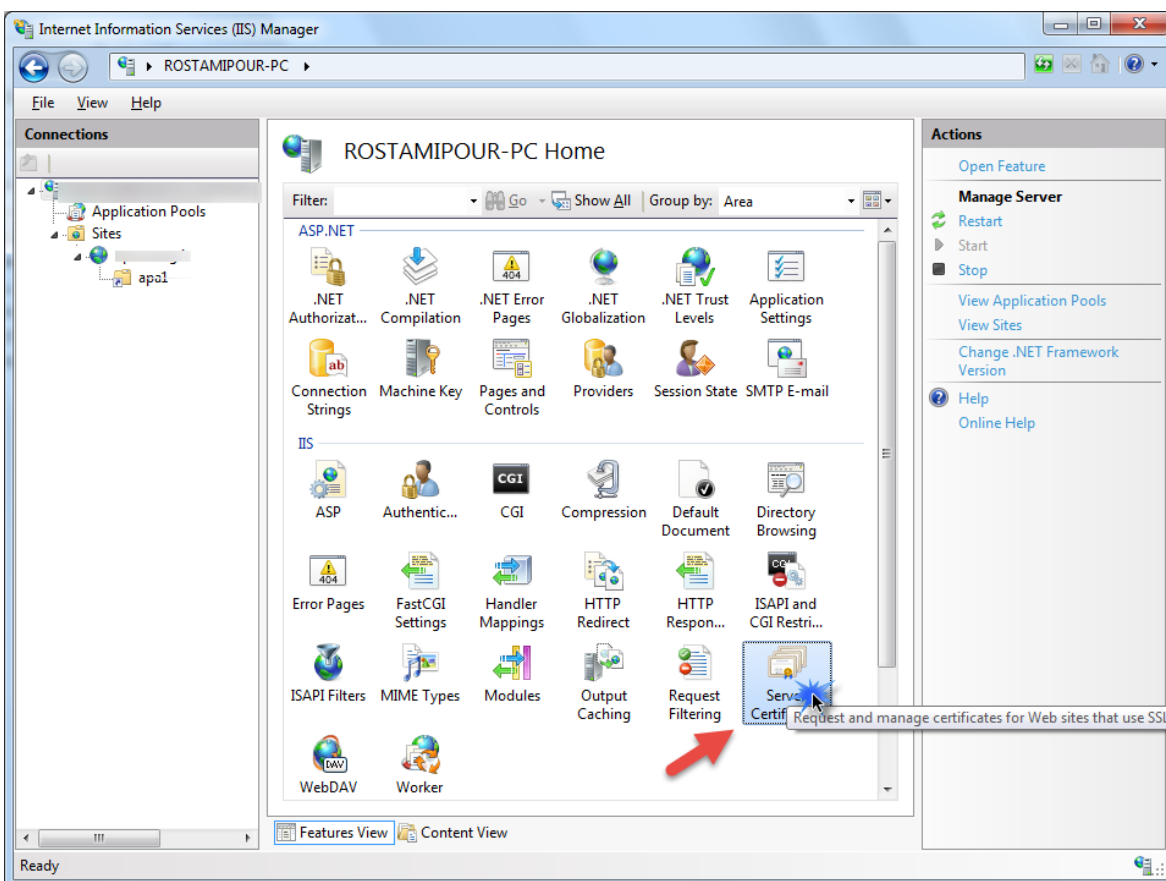
پس از دریافت گواهی امنیتی از یک CA معتبر، کلید عمومی و خصوصی ایجاد شده باید با استفاده از دستور openssl زیر به یک کلید به فرمت pfx تبدیل گردد. (private.key نام فایل حاوی کلید خصوصی، Certificate.crt نام گواهی ارسالی توسط CA و Intermediate\_CA.crt فایل حاوی کلید عمومی CA)

```
openssl pkcs12 -export -out certificate.pfx -inkey private.key -in Certificate.crt -certfile Intermediate_CA.crt
```

پس از وارد کردن این دستور یک کلمه عبور از کاربر دریافت می شود.

سپس فایل خروجی (certificate.pfx) باید در وب سرور IIS اضافه شود. مراحل زیر باید جهت انجام این امر صورت پذیرد:

۱. باید پس از باز کردن IIS Manager بر روی Server Certificate از پنجره Home کلیک کرد.

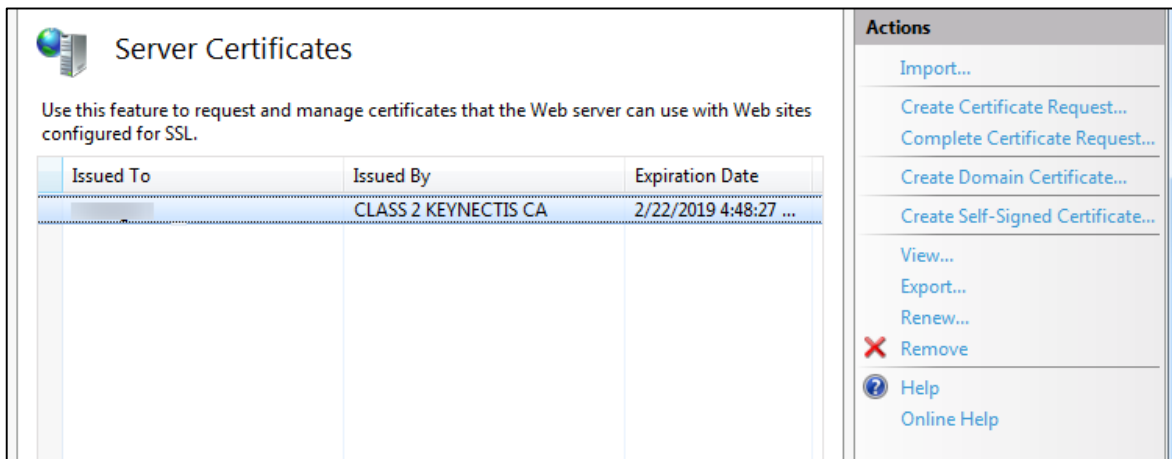


شکل ۱: نمایشی از IIS Manager و انتخاب Server Certificate

۲. سپس از منوی Action باید گزینه import انتخاب شود.

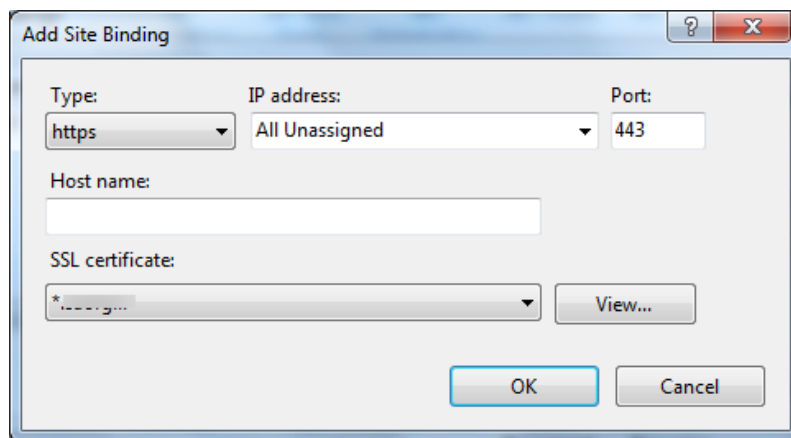
۳. سپس باید مسیر فایل کلید تولید شده در مرحله ی قبل را در بخش Certificate file وارد کرده و

کلمه عبور وارد شده نیز در بخش password وارد شود.



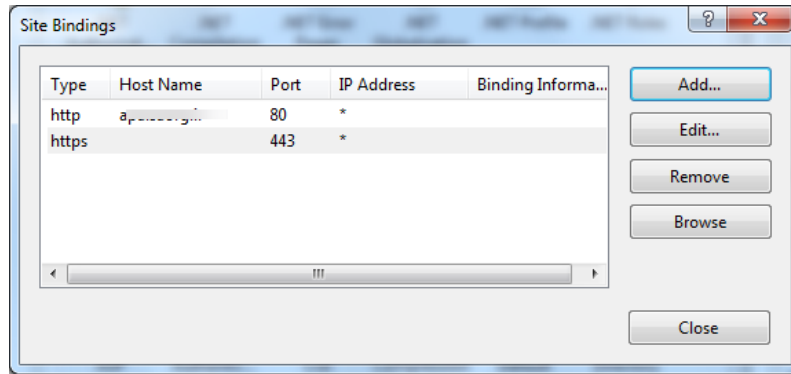
شکل ۲: نمایی از کلید اضافه شده به سرور

۴. در مرحله بعد باید از بخش sites بر روی نام سایت مورد نظر کلیک کرده و سپس گزینه‌ی Binding از منوی Action را انتخاب کرد.
۵. سپس بر روی گزینه‌ی add از پنجره‌ی باز شده کلیک شود.
۶. در پنجره‌ی باز شده باید type به https تغییر یابد. سپس از منوی SSL Certificate نام certificate اضافه شده در مراحل قبل را انتخاب کرد.



شکل ۳: نمایی از اضافه کردن کلید به سرور

۷. در نهایت با کلیک بر روی OK زوج کلیدها بر روی سرور فعال می‌گردد.



شکل ۴: نمایی از نتیجه‌ی نهایی تنظیمات کلید

## ۶-۲ امن سازی پیکربندی SSL/TLS در سرویس دهنده

پس از فعالسازی سرویس SSL بر روی سایت خود، می‌بایست امنیت آن را ارتقا دهید. پیاده‌سازی و استفاده ایمن از SSL/TLS دارای جزئیات فنی متعددی است که می‌بایست به‌درستی رعایت شود. در صورت عدم رعایت ملاحظات و نکات امنیتی در پیاده‌سازی این پروتکل، محرمانگی و یکپارچگی داده‌های مبادله شده به خطر می‌افتد.

ابتدا می‌بایست سرویس دهنده خود را ارزیابی نمایید تا مشکلات احتمالی «مشخص شود». بدین منظور می‌توانید از ابزارهای آنلاین که بدین منظور وجود دارد استفاده نمایید:

سایت SLCheck مرکز ماهر:

<https://sslcheck.certcc.ir/>

سایت SSL Labs:

<https://www.ssllabs.com/ssltest/>

سپس در صورت وجود مشکل، برای ایمن‌سازی SSL/TLS در سرویس‌دهنده Apache یا SSL از مستندات که بدین منظور توسط مرکز ماهر و آپای دانشگاه صنعتی امیرکبیر تهیه شده، می‌توانید استفاده نمایید:

<https://sslcheck.certcc.ir/HelpDoc-pe.php>