

# إدارة المفاتيح والشهادة

## عبر نظام Windows

توليد مفتاح خاص (Private Key) وطلب توقيع شهادة (CSR) عبر موقع: <https://tools.ecc.sy>

- بعد فتح الموقع، من تبويبة CSR Generate املأ الحقول كما يلي:



### شهادات ال SSL:

حقل ال commonName: يتم ملؤه حسب الشهادة

المطلوبة كما يلي:

شهادة البيئة الفعلية (Production): اكتب

epay.domainName

شهادة البيئة التجريبية (Test): اكتب

epaytest.domainName

حيث أن المقصود بال domainName هو اسم النطاق للجهة

حقل ال organizationName: اسم الجهة باللغة العربية.

حقل ال organizationUnitName: اسم القسم / المديرية.

حقل ال Key type: يتم اختياره recommended (RSA 2048).

حقل ال Code: أدخل رمز التحقق الظاهر بجانب الحقل.

**مثال للتوضيح كما في الصور جانباً:**

بفرض أن:

اسم الجهة باللغة العربية: جامعة دمشق

واسمها باللغة الأجنبية: Damascus University

وعنوان النطاق: damascusuniversity.edu.sy

والشهادة المطلوبة هي شهادة البيئة التجريبية (test)

يتم ملء الحقول كما يلي:

epaytest.damascusuniversity.edu.sy:commonName

جامعة دمشق: organizationName

IT: organizationalUnitName



### شهادات ال Code Signing:

حقل ال commonName: يتم ملؤه حسب الشهادة

المطلوبة كما يلي:

شهادة البيئة الفعلية (Production): اكتب

Name

## شهادة البيئة التجريبية (Test): اكتب – Organization Name

test

حيث المقصود بال Organization Name هو اسم الجهة باللغة الأجنبية مع مراعاة كتابة حرف كبير ببداية كل كلمة.

حقل ال organizationName: اسم الجهة باللغة العربية.

حقل ال organizationUnitName: اسم القسم / المديرية.

حقل ال Key type: يتم اختياره: RSA 2048 (recommended).

حقل ال Code: أدخل رمز التحقق الظاهر بجانب الحقل.

### مثال للتوضيح كما في الصور جانباً:

بفرض أن:

اسم الجهة باللغة العربية: جامعة دمشق

واسمها باللغة الأجنبية: Damascus University

والشهادة المطلوبة هي شهادة البيئة التجريبية (test)

يتم ملء الحقول كما يلي:

Damascus University –test :commonName

جامعة دمشق: organizationName

IT :organizationalUnitName



Code  
jeyre

Generate keys

Generate CSR (Certificate Signing Request) and private key online with just a single click. Simply fill out the form below and click keys button.

Two keys will be generated — a private key (you must keep it) and a public key (CSR).

Private key

-----BEGIN PRIVATE KEY-----  
MIIEvQIBAAQCEA9...  
-----END PRIVATE KEY-----  
  
-----BEGIN CERTIFICATE REQUEST-----  
MIIEvQIBAAQCEA9...  
-----END CERTIFICATE REQUEST-----  
  
Attention!  
We do not keep the private key. You must download and save the private key on your computer (server). If you lose the private key, you will not be able to use your certificate.

copy

copy

copy

copy

### • بعد ملء كامل الحقول نضغط على Generate Keys فيتم توليد ملف

ال Private Key (ملف المفتاح الخاص) وال CSR (ملف طلب توقيع الشهادة) كما موضح في الصور جانباً.

### • هناك طريقتان للاحتفاظ بالملفات:

1) إما يتم نسخ كل ملف على حدى بالضغط على copy وحفظ كل ملف على حدى.

2) أو نضغط على زر key & csr ف يتم تحميل ملف مضغوط يحوي كل من ال Private Key و ال CSR كما هو موضح جانباً بالصور.

**للتنوية:** ملف ال CSR هو ما يُرسل إلى الجهة المختصة لإصدار الشهادة أما ال Private Key يتم الاحتفاظ به من قبل الجهة المالكة.

## عبر نظام Linux

### توليد مفتاح خاص وطلب شهادة لعامل

#### باستخدام خوارزمية RSA 2048

التعليمية التالية ستقوم بتوليد ملفين أحدهما هو الملف الخاص Private key والآخر هو طلب الشهادة (ذو اللامقة csr) يمكن تنفيذ التعليمية بأي نظام تشغيل يحوي الحزمة Openssl يجب التأكيد وضع القيم الصحيحة لمكان العمل والصفة الوظيفية والرقم الوطني قبل تنفيذ الأمر

```
openssl req -new -utf8 -nameopt multiline,utf8 -nodes -out my_name.csr -  
newkey rsa:2048 -keyout my_name.key -config <(  
    cat <<-EOF  
        [req]  
            prompt = no  
            default_md = sha256  
            distinguished_name = dn  
  
            [ dn ]  
                C=SY  
                Change Me #             title=الصفة الوظيفية  
                Change Me #             =جهتي0  
                Change Me #             OU=المديريه  
                Change Me #             CN=اسمي  
                emailAddress=my@email.sy    # Change Me  
                serialNumber=NID-0101010101 # Change the Number  
            EOF  
(
```

#### باستخدام خوارزمية ECDSA

التعليمية التالية ستقوم بتوليد ملفين أحدهما هو الملف الخاص Private key والآخر هو طلب الشهادة (ذو اللامقة csr) يمكن تنفيذ التعليمية بأي نظام تشغيل يحوي الحزمة Openssl يجب التأكيد وضع القيم الصحيحة لمكان العمل والصفة الوظيفية والرقم الوطني قبل تنفيذ الأمر

```
openssl ecparam -name prime256v1 -genkey -out my_name.key  
openssl req -new -utf8 -nameopt multiline,utf8 -key my_name.key -out  
    my_name.csr -config <(  
        cat <<-EOF  
            [req]
```

```
prompt = no
default_md = sha256
distinguished_name = dn

[ dn ]
C=SY

Change Me #       الصفة الوظيفية
Change Me #       جهة
Change Me #       المديرية
Change Me #       اسمى
emailAddress=my@email.sy   # Change Me
serialNumber=NID-01010101010 # Change the Number
EOF
()
```

## تشكيل ملف pfx/pkcs12

يمكن دمج ملف الشهادة الرقمية مع ملف المفتاح الخاص لتشكيل ملف pfx (الحماية الملف الخاص بكلمة مرور وكذلك للتمكن من تنصيب الشهادة على نظام التشغيل أو وتحميلها على حامل إلكتروني) باستخدام الأمر التالي الذي يمكن تنفيذه من أي نظام تشغيل يحوي الحزمة Openssl كما يلي:

```
openssl pkcs12 -export -out my_name.pfx -inkey my_name.key -in my_name.pem
```

سيتم طلب رمز لقفل الملف به، ندخل الرمز مرتين

ملاحظة: الأمر السابق يحتاج لأن تكون الشهادة بتنسيق pem (base64) فإذا كانت الشهادة بتنسيق der/cer(binary) فيمكن تحويلها باستخدام الأمر التالي:



```
openssl x509 -inform der -in my_name.cer -out my_name.pem
```

## توليد مفتاح خاص وطلب شهادة Code Signing

الأمر التالي سيقوم بتوليد مفتاح خاص Private key وملف طلب شهادة CSR للنطاق example.sy مع ملاحظة ضرورة تعديل قيم الحقول التالية بالطلب حسب الحاجة، o و CN وكذلك يمكن إضافة حقول أخرى عند الحاجة

```
openssl req -new -nodes -out example.sy.csr -newkey rsa:2048 -keyout
example.sy.key -config <(
cat <<-EOF
```

```

[req]
prompt = no
default_md = sha256
distinguished_name = dn

[ dn ]
C=SY
O=Organization Name
CN=Organization Name
EOF
(

```

## توليد مفتاح خاص وطلب شهادة ssl

الأمر التالي سيقوم بتوليد مفتاح خاص CSR وملف طلب شهادة Private key للنطاق example.sy مع ملاحظة ضرورة تعديل قيم الحقول التالية بالطلب حسب الحاجة، o و 1.1 و 1.2 DNS و CN و CN=Organization Name و CN=example.sy وكذلك يمكن إضافة حقول أخرى عند الحاجة

```

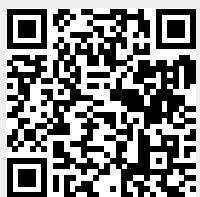
openssl req -new -nodes -out example.sy.csr -newkey rsa:2048 -keyout
example.sy.key -config <(
cat <<-EOF
[req]
prompt = no
default_md = sha256
distinguished_name = dn
req_extensions = ssl_reqext

[ dn ]
C=SY
O=Organization Name
CN=example.sy

[ ssl_reqext ]
subjectAltName=@alt_names

[ alt_names ]
DNS.1 = example.sy
DNS.2 = *.example.sy
EOF
(

```



From:  
- مركز معلومات مركز التصديق /https://info.ecc.sy

Permanent link:

<https://info.ecc.sy/doku.php?id=howto:keymgmt&rev=1746435525>

Last update: **2025/05/05 08:58**