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.

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

وعنوان النطاق: damascusuniversity.edu.sy

والشهادة المطلوبة هي شهادة البيئة التجريبية (test)

يتم ملء الحقول كما يلي:

epaytest.damascusuniversity.edu.sy:commonName

organizationName: جامعة دمشق

organizationalUnitName: IT

شهادات ال Code Signing:

حقل ال commonName: يتم ملؤه حسب الشهادة المطلوبة كما يلي:

شهادة البيئة الفعلية (Production): اكتب Organization 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.

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

والشهادة المطلوبة هي شهادة البيئة التجريبية (test)

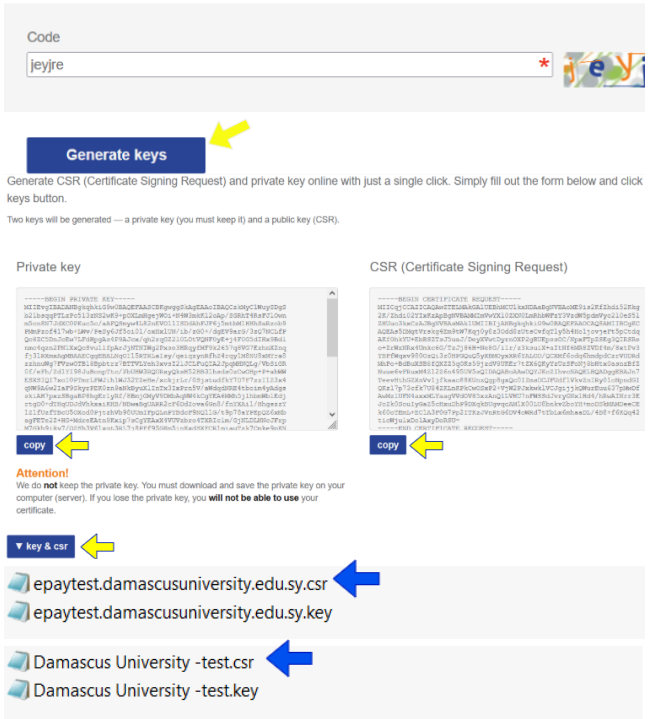
يتم ملء الحقول كما يلي:

commonName: Damascus University –test

organizationName: جامعة دمشق

organizationalUnitName: IT

- بعد ملء كامل الحقول نضغط على Generate Keys فيتم توليد ملفي
  ال Private Key (ملف المفتاح الخاص)
  وال CSR (ملف طلب توقيع الشهادة) كما مُوضح 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 فيتم تحميل ملف مضغوط يحوي كل من ال Private Key و ال CSR كما هو مُوضح جانباً بالصور.

للتنويه: 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

التعليمة التالية ستقوم بتوليد ملفين أحدهما هو الملف الخاص Private key والآخر هو طلب الشهادة (ذو اللاحقة csr)
يمكن تنفيذ التعليمة 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
title=الصفة الوظيفية          Change Me #
O=جهتي                         Change Me #
OU=المديرية                    Change Me #
CN=اسمي                        Change Me #
                    emailAddress=my@email.sy    # Change Me
                serialNumber=NID-01010101010    # Change the Number
                                               EOF
                                                )
```

باستخدام خوارزمية ECDSA

التعليمة التالية ستقوم بتوليد ملفين أحدهما هو الملف الخاص Private key والآخر هو طلب الشهادة (ذو اللاحقة csr) يمكن تنفيذ التعليمة 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
title=الصفة الوظيفية # Change Me
O=جهتي # Change Me
OU=المديرية # Change Me
CN=اسمي # Change Me
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 (لحماية 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 Private key وملف طلب شهادة CSR للنطاق example.sy
مع ملاحظة ضرورة تعديل قيم الحقول التالية بالطلب حسب الحاجة، o و CN و DNS.1 و DNS.2 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
(
```