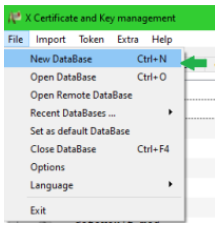
دليل استخدام الحامل الالكتروني ePass2003 في توليد المفاتيح

يتم توليد المفتاح الخاص بالشهادة Private Key ضمن الحامل الالكتروني ePass2003 باستخدام تطبيق الـ XCA كما يلي:

XCA

- النسخة xca-portable-2.6.0
- النسخة xca-portable-2.7.0
- النسخة xca-portable-2.8.0



التأكد من تعريف الحامل الإلكتروني

يجب التأكد من تنصيب برنامج التعريف الخاص بالحامل الإلكتروني قبل البدء بأي إجراء، برنامج التعريف إما يكون مضمن ضمن الحامل الإلكتروني أو عبر ملف تنصيب خارجي حسب نوع الحامل، يمكن الإطلاع على صفحة التعاريف

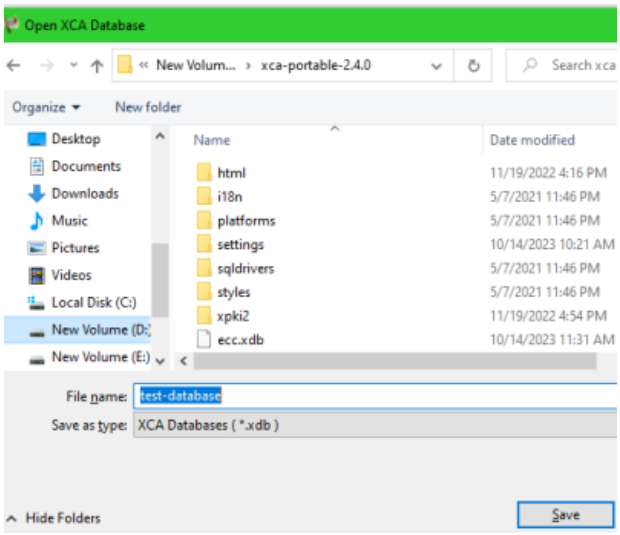
تهيئة برنامج XCA

قبل استعمال التطبيق، يجب أن نقوم بتهيئته للعمل عبر إنشاء قاعدة بيانات وتعريف

الواجهة pkcs11
لنتمكن من التعامل
مع الحوامل
الإلكترونية

إنشاء قاعدة بيانات لحفظ كافة الاعدادات وبيانات المفاتيح والشهادات:

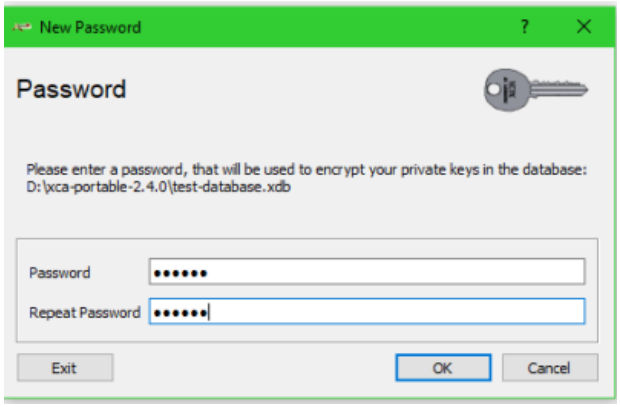
- نختار من File الخيار New DataBase

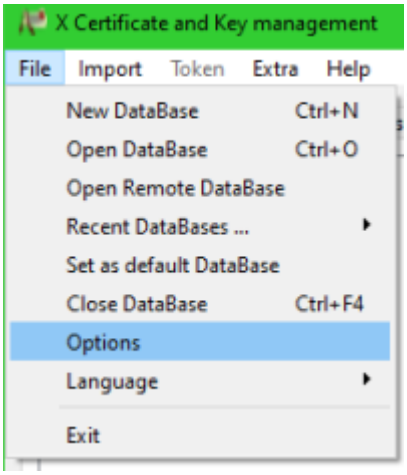


- نختار المسار المراد حفظ قاعدة البيانات فيه:

- ثم يطلب كلمة مرور لحماية قاعدة البيانات
- يفضل أن نختار قاعدة البيانات هذه كخيار افتراضي عند فتح التطبيق، عبر الضغط على القائمة File ومنها نختار Set as

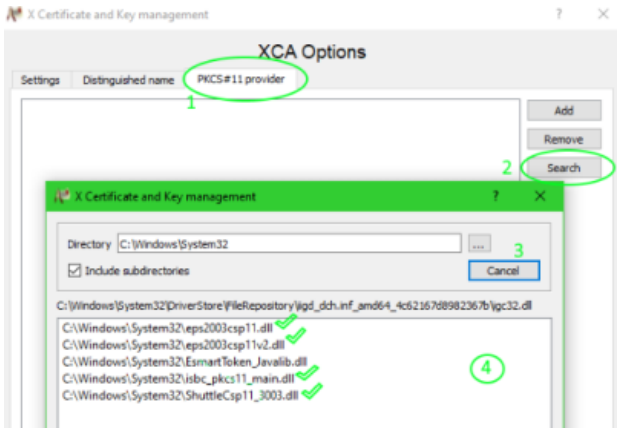
default DataBase





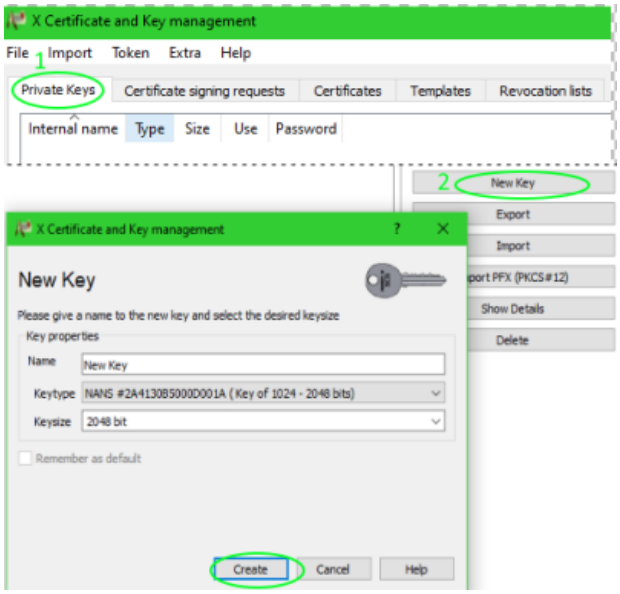
إعداد البرامج بواجهة PKCS11 مناسب للحامل الإلكتروني

- لإعداد البرنامج ليتعرف على الحامل الإلكتروني عبر الواجهة PKCS11، نختار من File الخيار Options

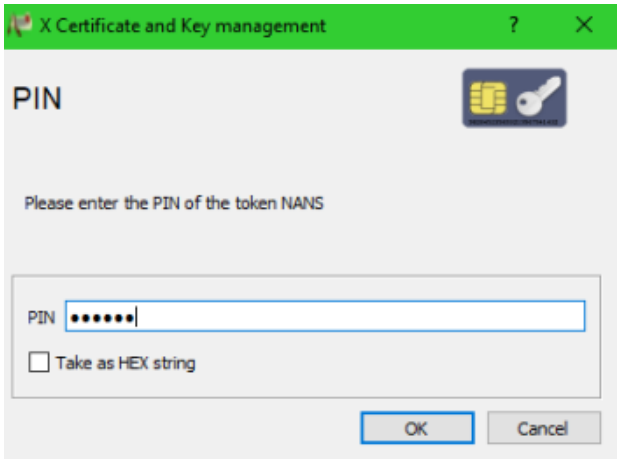


- نختار التبويب PKCS#11 provider.
- نختار search.
- تظهر النافذة البحث، نختار منها الخيار include subdirectories.
- نضغط على زر بحث search.
- نختار الملفات المراد تضمينها كما هو محدد بالصورة (ملفات dll وهي مكاتب الحامل الإلكتروني التي تدعم الواجهة pkcs11) ثم نختار ok،

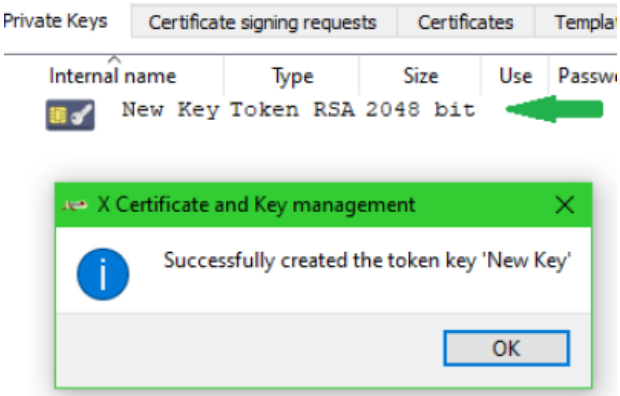
توليد المفتاح الخاص ضمن الحامل الإلكتروني



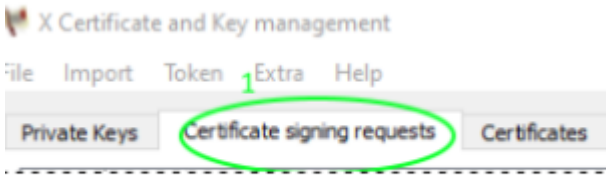
- نحدد التبويب Private Keys
- نختار New Key
- فتظهر النافذة المحددة بالشكل
- نختار اسم مميز للمفتاح Name
- نختار نوع المفتاح Keytype، وهنا يجب ان يظهر اسم الحامل الإلكتروني مع الخوارزميات وأطوال المفاتيح المدعومة
- نختارح طول المفتاح Keysize، مثلاً 1024 أو 2048 في حالة الخوارزمية rsa
- ثم نختار Create



- ثم تظهر نافذة تطلب إدخال رقم pin الخاص بالحامل الإلكتروني من أجل توليد وحفظ المفتاح الخاص ضمن الحامل.



- تظهر نافذة تشير أنه تم توليد وحفظ المفتاح بنجاح.

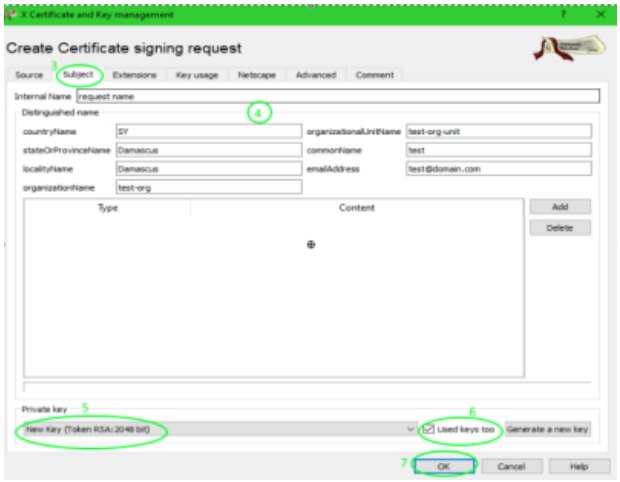


إنشاء طلب توقيع شهادة CSR

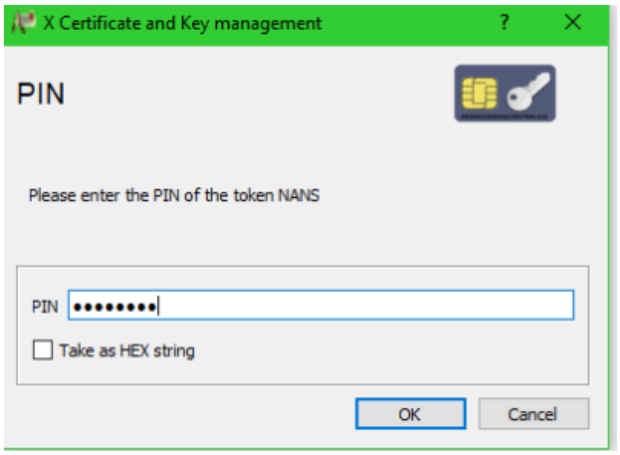


لتوليد ملف طلب توقيع الشهادة CSR انطلاقاً من المفتاح الخاص الذي تم إنشاءه في الخطوة السابقة، نختار التبويب certificate signing requests.

- ثم نضغط الزر New request.

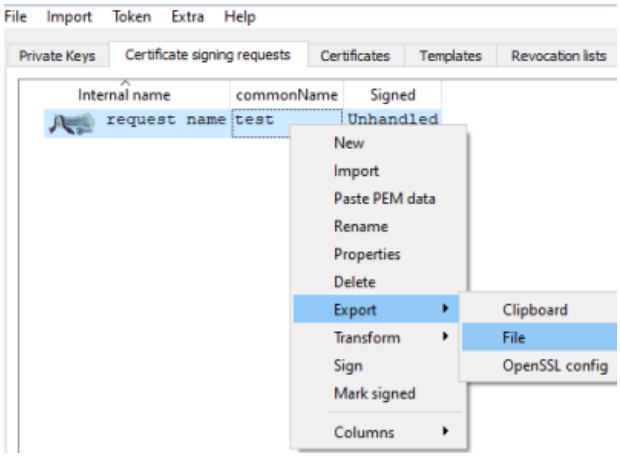


- بعد ذلك تظهر النافذة التالية:
- من تبويبة subject نقوم بادخال المعلومات الخاصة بصاحب الشهادة.
- ثم نختار المفتاح الخاص بالشهادة الذي تم توليده مسبقاً.
- عند الحاجة لاستخدام مفتاح خاص تم استخدامه سابقاً في إنشاء طلبات توقيع شهادة، نحدد على الخيار Used key too

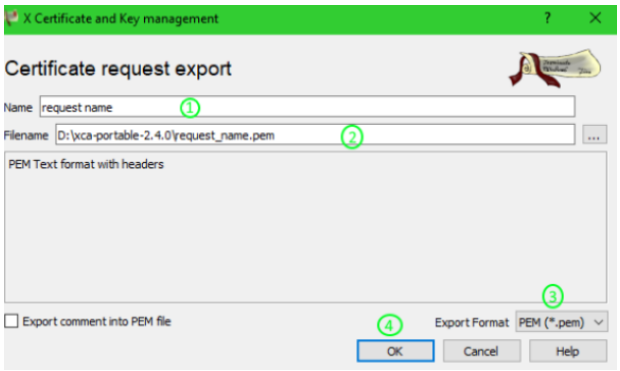


- ثم يطلب رقم الـ pin الخاص بالحامل الإلكتروني (للوصول للمفتاح الخاص)
- بعد ذلك تظهر نافذة تشير بأنه تم انشاء طلب الشهادة بنجاح.

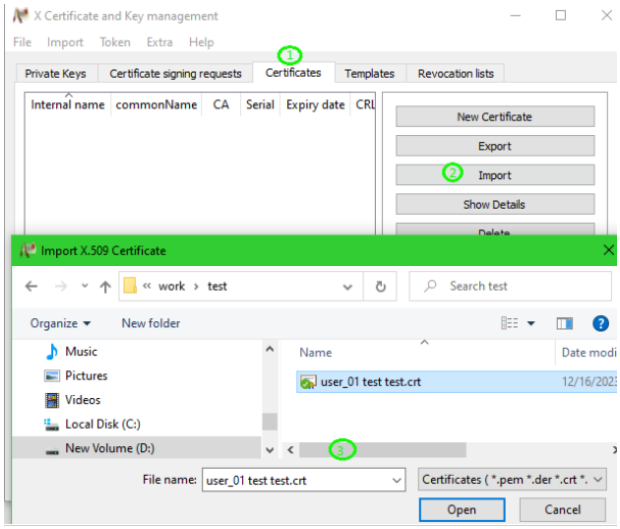
- نقوم بتصدير طلب توقيع الشهادة CSR.



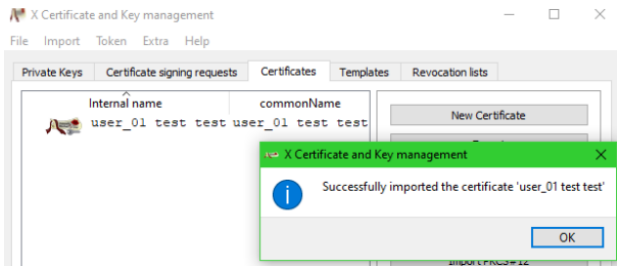
- يتم حفظ الطلب في مكان محدد بالتنسيق pem وإرساله إلى الجهة المصدرة للشهادات من أجل توقيعه.



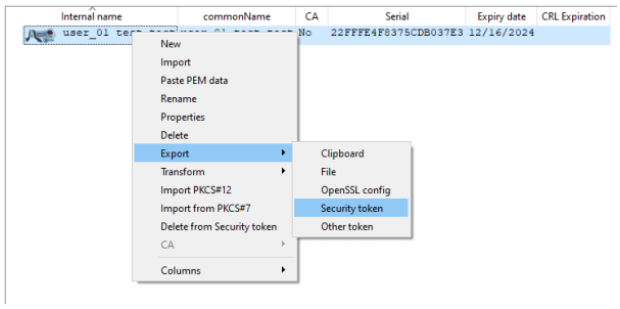
- بعد توقيع الطلب وإصدار الشهادة ،نذهب الى XCA من أجل حفظ الشهادة بالحامل، حيث نقوم باستيراد الشهادة الى تبويبة الـ certificates كما هو موضح بالصورة التالية:



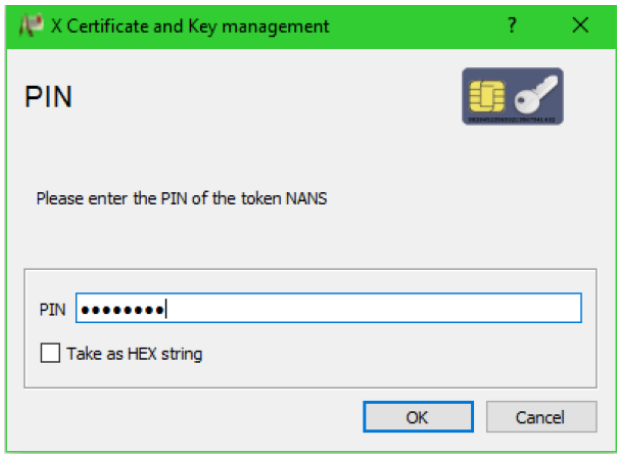
- ثم تظهر الرسالة التالية أنه تم استيراد الشهادة الى تطبيق الـ XCA بنجاح.



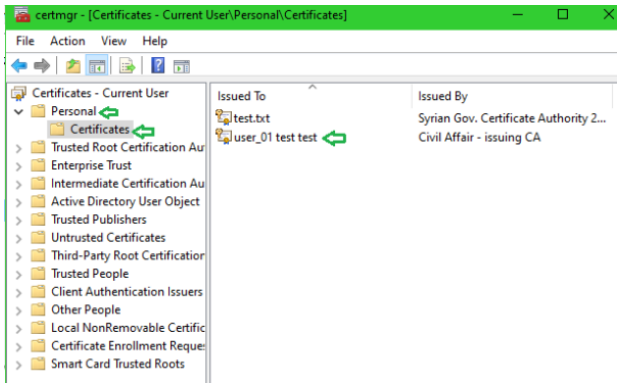
- بعد ذلك نقوم بتصدير الشهادة من XCA إلى الحامل الإلكتروني Security token كما هو موضح بالشكل:



- يقوم البرنامج بطلب إدخال الـ PIN الخاص بالـ token:



- نستطيع التأكد بأنه تم تصدير الشهادة الى التوكن من خلال التأكد من وجودها في مخزن شهادات نظام التشغيل windows كما هو موضح بالصورة:



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

Permanent link:
https://info.ecc.sy/doku.php?id=howto:useepass

Last update: **2024/11/12 07:30**