كيف يمكنني تصدير وتحويل شهادة جذر Microsoft CA من خادم PFX CA ومفاتيح

سؤال:

تشير مقالة قاعدة المعارف هذه إلى البرامج التي لم يتم صيانتها أو دعمها من قبل Cisco. يتم توفير المعلومات كنوع من المجاملة لراحتك. للحصول على مزيد من المساعدة، يرجى الاتصال بمورد البرامج.

فيما يلي إرشادات لتصدير شهادة جذر ومفاتيح توقيع CA من خادم Microsoft CA 2003. هناك عدة خطوات في هذه العملية. ومن المهم جدا اتباع كل خطوة.

تصدير الشهادة والمفتاح الخاص من خادم MS CA
1. انتقل إلى 'start' ->'run' -> 'MMC'
2. انقر على 'file' ->'add / remove snap-in'
3. انقر فوق الزر **'إضافة...'**
4. حدد **'الشهادات'** ثم انقر فوق **'إضافة'**
5. حدد **'حساب الكمبيوتر'** -> **'التالي'** ->**'كمبيوتر محلي'** -> **'إنهاء'**
6. انقر فوق **'إغلاق'** ->**'موافق'**
تم تحميل MMC الآن باستخدام الأداة الإضافية "الشهادات".
7. قم بتوسيع **الشهادات** -> وانقر على **'شخصي'** -> **'الشهادات'**
8. انقر بزر الماوس الأيمن فوق شهادة CA المناسبة واختر **'كافة المهام** -> **'تصدير'**
سيتم تشغيل معالج تصدير الشهادات
9. انقر فوق **'التالي'** -> حدد **'نعم، تصدير المفتاح الخاص'** -> **'التالي'**
10. ***قم بإلغاء تحديد جميع*** الخيارات هنا. يجب أن يكون PKCS 12 هو الخيار الوحيد المتاح. طقطقة **'next'**
11. امنح المفتاح الخاص كلمة مرور من إختيارك
12. امنح اسم الملف للحفظ باسم وانقر فوق **'التالي'**، ثم **'إنهاء'**
الآن لديك شهادة توقيع CA وتم تصدير الجذر كملف PFX) PKCS 12).
إستخراج المفتاح العام (شهادة)
ستحتاج إلى الوصول إلى كمبيوتر يعمل ب OpenSSL. انسخ ملف PFX إلى هذا الكمبيوتر ثم قم بتشغيل

الأمر التالي:

openssl pkcs12 -في <filename.pfx> -clcerts -nokeys -out certificate.cer

يؤدي هذا إلى إنشاء ملف المفتاح العام المسمى "certificate.cer"

ملاحظة: تم التحقق من هذه التعليمات باستخدام OpenSSL على Linux. قد تختلف بعض الشاشات إذا تم إصدارها على Win32.

إستخراج المفتاح الخاص وفك تشفيره

يتطلب WSA أن يكون المفتاح الخاص غير مشفر. أستخدم أوامر OpenSSL التالية:

openssl pkcs12 -في <filename.pfx> -nocerts -out privatekey-encrypted.key

ستتم مطالبتك ب **إدخال كلمة مرور الاستيراد**". هذه هي كلمة المرور التي تم إنشاؤها في ***الخطوة 11*** أعلاه.
وستتم مطالبتك أيضا بإدخال **عبارة مرور PEM**". ال تشفير كلمة مرور (يستعمل أدناه).

سيؤدي هذا إلى إنشاء ملف المفتاح الخاص المشفر المسمى "privatekey-encrypted.key"

لإنشاء إصدار تم فك تشفير هذا المفتاح، أستخدم الأمر التالي:

openssl rsa -in privatekey-encrypted.key -out private.key

يمكن تثبيت المفاتيح العامة والمفاتيح الخاصة التي تم فك تشفيرها على WSA من **'إدارة الأمان -> HTTPS ليكو'**

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).