Come esportare e convertire una chiave e un certificato radice CA pfx da un server CA Microsoft

Domanda:

Questo articolo della Knowledge Base fa riferimento a software non gestito o supportato da Cisco. Le informazioni sono fornite a titolo di cortesia. Per ulteriore assistenza, contattare il fornitore del software.

Di seguito sono riportate le istruzioni per esportare un certificato radice di firma e una chiave CA da un server Microsoft CA 2003. In questo processo sono previste diverse fasi. È fondamentale che ogni passo sia seguito.

Esportazione del certificato e della chiave privata dal server CA MS
1. Selezionare **'Start'** -> **'Esegui'** -> **MMC** 2. Fare clic su **'File'** -> **'Aggiungi/Rimuovi snap-in'** 3. Fare clic su **'Aggiungi...'** pulsante 4. Selezionare **'Certificati'**, quindi fare clic su **'Aggiungi'** 5. Selezionare **'Account computer'** -> **'Avanti'** -> **'Computer locale'** -> **'Fine'** 6. fare clic su **'Chiudi'** -> **'OK'** *MMC verrà caricato con lo snap-in Certificati.* 7. Espandere **Certificati** -> e fare clic su **'Personali'** -> **'Certificati'** 8. Fare clic con il pulsante destro del mouse sul certificato CA appropriato e scegliere **'Tutte le attività'** -> **'Esporta'** *Verrà avviata l'Esportazione guidata certificati* 9. Fare clic su **'Avanti'** -> Selezionare **'Sì, Esporta la chiave privata'** -> **'Avanti'** 10. ***Deselezionare tutte*** le opzioni. PKCS 12 dovrebbe essere l'unica opzione disponibile. Fare clic su **'Avanti'** 11. Assegnare alla chiave privata una password a scelta 12. Assegnare un nome al file con cui salvare e fare clic su **'Avanti'**, quindi su **'Fine'**

Il certificato di firma CA e la radice sono stati esportati come file PKCS 12 (PFX).

Estrazione della chiave pubblica (certificato)

Ènecessario accedere a un computer che esegue OpenSSL. Copiare il file PFX su questo computer ed eseguire il comando seguente:

openssl pkcs12 -in <nomefile.pfx> -clcerts -nokeys -out certificate.cer

Verrà creato il file di chiave pubblica denominato "certificate.cer"

Nota: Queste istruzioni sono state verificate utilizzando OpenSSL su Linux. Alcune sintassi possono variare nella versione Win32.

Estrazione e decrittografia della chiave privata

WSA richiede che la chiave privata non sia crittografata. Utilizzare i seguenti comandi OpenSSL:

openssl pkcs12 -in <nomefile.pfx> -nocerts -out privatekey-encrypted.key

Verrà richiesto di **immettere** la **password di importazione**. Questa è la password creata al *passaggio 11* sopra.
Verrà inoltre richiesto di **immettere la passphrase PEM**. è la password di crittografia (utilizzata di seguito).

Verrà creato il file di chiave privata crittografato denominato "privatekey-encrypted.key"

Per creare una versione decrittografata della chiave, utilizzare il comando seguente:

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

Le chiavi pubbliche e private decrittografate possono essere installate sul server di sicurezza di Windows da **'Security Services'** -> **'HTTPS Proxy'**