

Guía para solicitar certificados de persona jurídica en Windows para la Jerarquía Nacional Sha2

Este documento permite al lector conocer los pasos necesarios para solicitar los certificados para personas jurídicas en sistemas operativos Windows para la jerarquía Sha2.



Guía para solicitar certificados de persona jurídica en Windows para la Jerarquía Nacional Sha2

La presente guía documenta los pasos a seguir para realizar una solicitud de certificados digitales para una persona jurídica, utilizando el sistema operativo Microsoft Windows.

Paso 1: Completar la información del archivo INF.

1. Descargue la plantilla según el tipo de certificado que desea generar. Para realizarlo es necesario ingresar al perfil de su entidad en la funcionalidad de firma digital de la plataforma Central Directo.
 - a. Debes seleccionar el menú firma digital, submenú Persona Jurídica, opción Sello o Agente no custodiado.
 - b. Ejecutar la acción solicitar
2. Del asistente de generación de certificado:
 - a. Para un certificado de tipo agente electrónico:

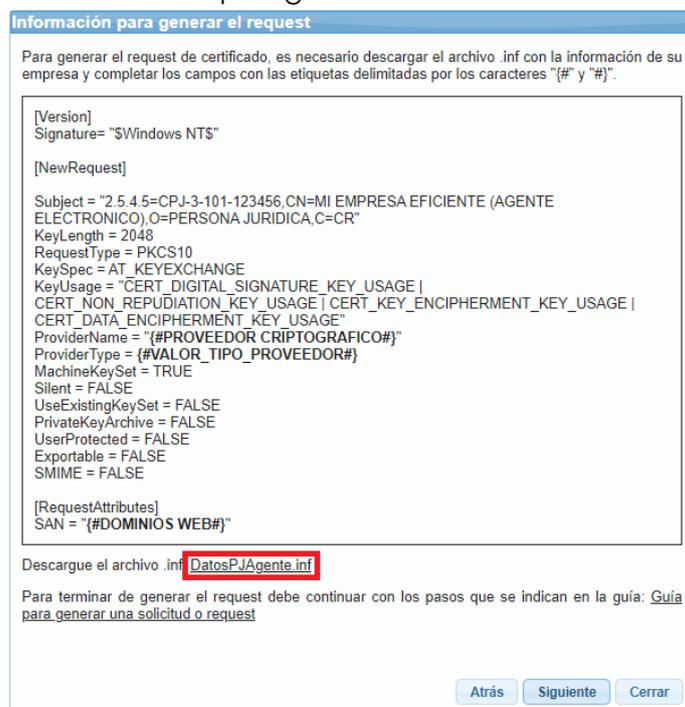


Imagen 1

- b. Para un certificado de tipo sello electrónico:



Imagen 2

3. Cree la carpeta C:\certificadoSINPE y copie en ella el archivo que descargó.
4. Abra el archivo con la aplicación "Bloc de notas".
5. Observe que en el archivo hay etiquetas delimitadas por los caracteres "{#" y "#}". **Estos son los únicos campos que usted debe modificar para realizar la solicitud de un certificado de Persona Jurídica.** Cámbielos según se indica a continuación:
 - a. **{#PROVEEDOR CRIPTOGRAFICO#}**: Escriba el proveedor criptográfico que está utilizando para comunicarse con el hardware o sistema criptográfico, donde se almacenará la llave privada del certificado, que será generado a partir del request. Para ver una lista de los proveedores criptográficos instalados en su máquina, abra la consola de comandos (CMD) y ejecute el comando: **"certutil -csp^{list}"** o **"netsh nap client show csp^s"**, el resultado será similar al mostrado en la imagen 3.

Si se decide no utilizar un hardware criptográfico (HSM) para almacenar la llave privada, entonces se recomienda utilizar el proveedor criptográfico "Microsoft Software Key Storage Provider", el cual es utilizado para almacenar llaves privadas en disco.

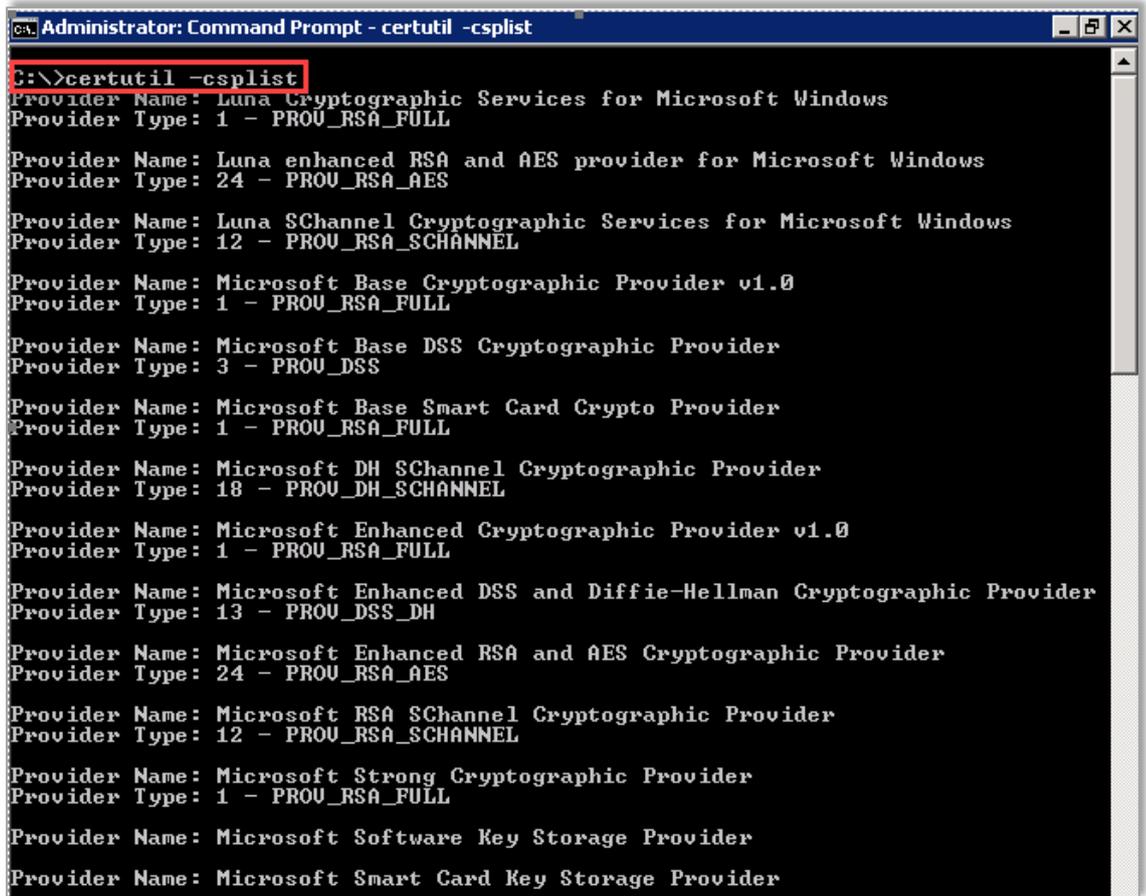


Imagen 1

- b. **{#VALOR_TIPO_PROVEEDOR#}**: Los proveedores criptográficos, pueden o no contar con un tipo de proveedor asociado, este dato se puede visualizar debajo del nombre del proveedor, como se muestra en la siguiente imagen.

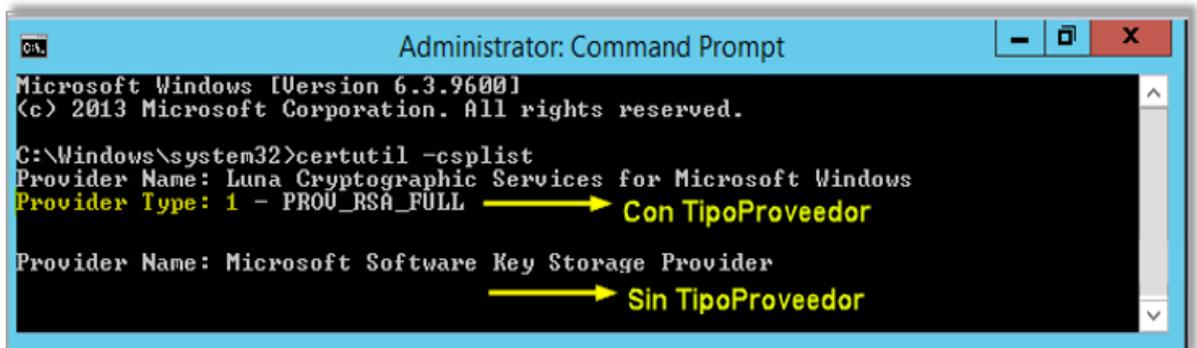


Imagen 2

Si el proveedor criptográfico seleccionado en el paso anterior (c) tiene asociado un tipo de proveedor (provider type), como el mostrado en la imagen 5, el valor que se debe indicar en este campo es el número que aparece después de los dos puntos. El ejemplo de cómo debe colocarse en el archivo “.inf” se muestra en la imagen 6.

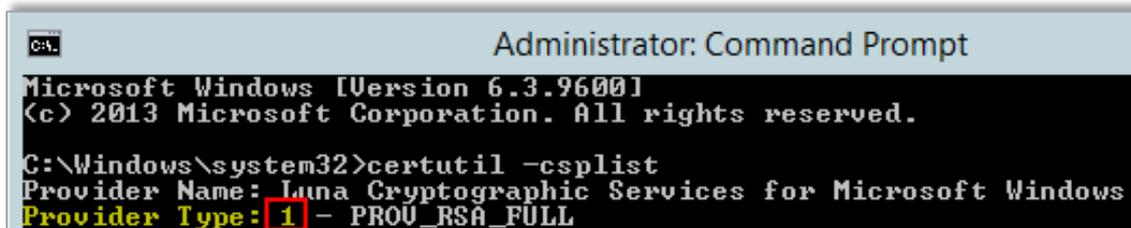


Imagen 3

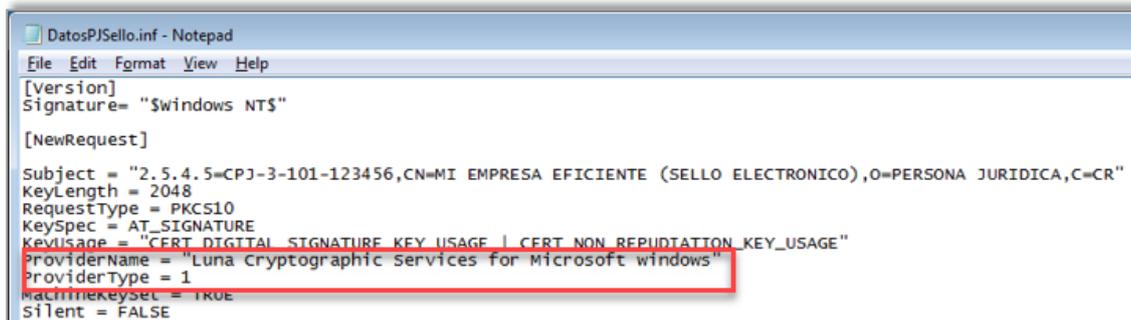


Imagen 4

Si el proveedor seleccionado **no** posee un tipo de proveedor asociado, como se visualiza en la imagen 7, se debe eliminar la línea completa de "ProviderType" del archivo .inf, como se muestra en la imagen 8.

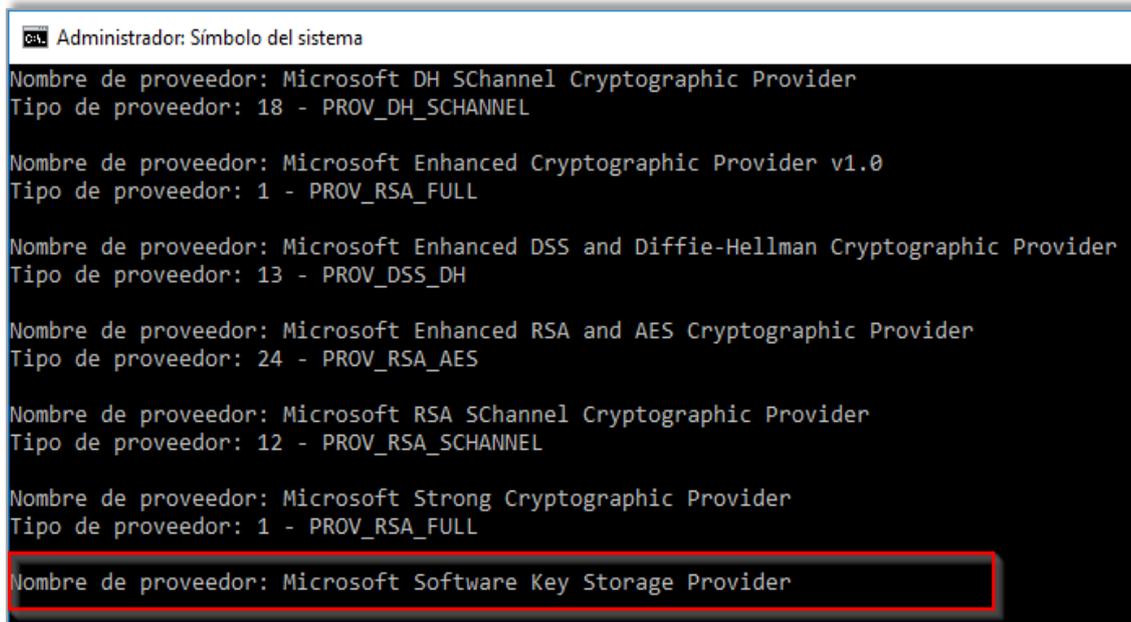


Imagen 5

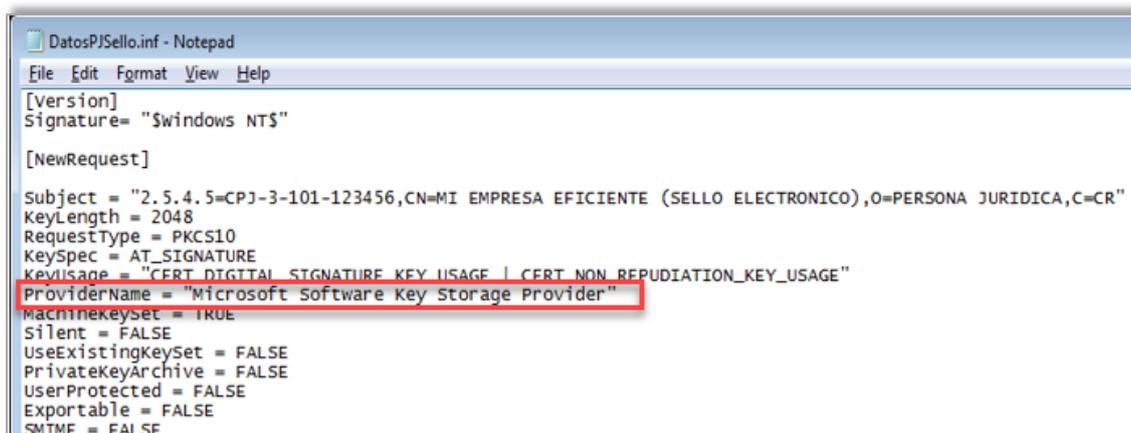


Imagen 6

- c. **{#DOMINIOS WEB#}**: Este campo es opcional y solo se usa con certificados de tipo **Agente Electrónico**. En este atributo se pueden incluir los nombres de los dominios con los que cuente la entidad, estos pueden ser de sitios o de servicios web que usted desee asegurar con el certificado de Agente Electrónico. Debe verificar que se cumplan con las siguientes reglas:
- Para efectos prácticos vamos a suponer que una entidad posee los dominios `www.miemp.co.cr`, `miservidor.miemp.co.cr` y `mail.miemp.co.cr`.
1. Se debe de escribir en minúscula.
 2. Los dominios no pueden contener caracteres especiales como la tilde.
 3. No debe contener http.
 4. Se puede escribir un dominio o múltiples dominios
 - SAN = "dns=[**dominio**]"
 - SAN = "dns=[**dominio**]&dns=[**dominio**]"
 - SAN = "dns=www.miemp.co.cr&dns=miservidor.miemp.co.cr&dns=mail.miemp.co.cr"
 5. El número máximo de registros en el SAN es de 10 dominios.
 6. Se puede escribir todo el dominio
 - miservidor.miemp.co.cr
 7. Se puede escribir sólo el final del dominio, pero debe de tener un asterisco antes del primer punto
 - *.miemp.co.cr
 8. Los dominios deben encontrarse registrados a nombre de la entidad
6. Se recomienda el uso de un hardware criptográfico (HSM) para almacenar la llave privada del certificado y que dicho HSM cuente con una certificación a nivel 3 o superior del estándar FIPS 140-2 o una certificación Common Criteria EAL 4+ en el perfil de protección SSCD Tipo 3 (Secure Signature-Creation Device), aunque existe la posibilidad de almacenar la llave privada del certificado en disco en un servidor.
7. Es importante tomar en consideración el campo "**EXPORTABLE**", que se encuentra en el archivo .inf, que permite determinar si la llave privada del certificado puede ser instalada en otro servidor. Si en el punto **d** se eligió un proveedor que utiliza un hardware criptográfico (HSM), no se debe modificar el valor de esta etiqueta. En caso contrario, si



la llave será almacenada en disco y se desea que el certificado emitido pueda ser exportado a otros servidores para ser reutilizado, se debe colocar el valor "TRUE". Este último escenario corresponde a los casos donde se tiene un clúster de servidores y se necesita que la llave privada este instalada en cada uno de los nodos que conforman dicho clúster.

- 8.** Guarde los cambios y cierre los archivos.



Ejemplo de archivos “. Inf” configurados

1. **Sello Electrónico:** El siguiente es un ejemplo de un archivo .inf completo con la información requerida para la solicitud de un certificado de tipo Sello Electrónico.

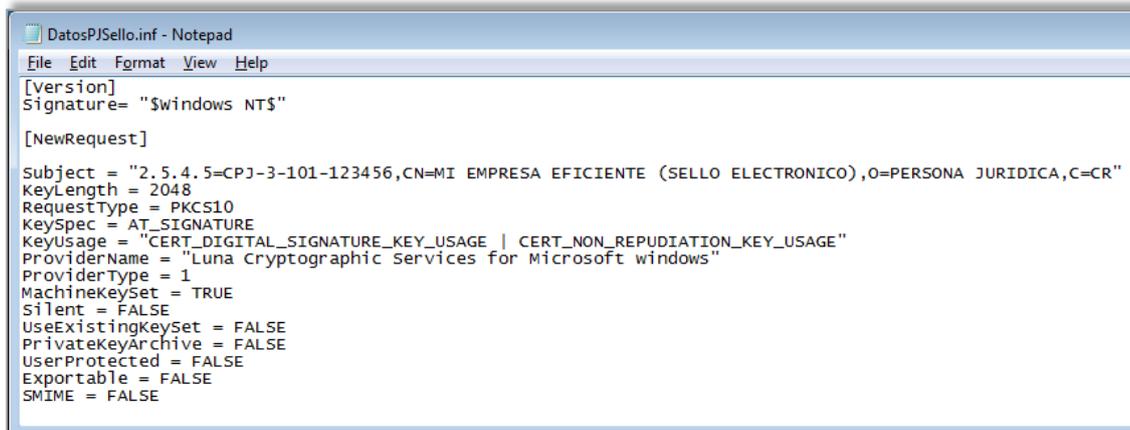


Imagen 7

2. **Agente Electrónico:** El siguiente es un ejemplo de un archivo .inf completo con la información requerida para la solicitud de un certificado de tipo Agente Electrónico



Imagen 8



Paso 2: Crear requests para los certificados digitales.

1. Haga clic en el botón  (Windows) y abra una consola de comandos (también conocida como "Símbolo del sistema") como Administrador escribiendo en la barra de búsqueda el comando **cmd.exe**, haciendo click derecho y finalmente click en "**Ejecutar como administrador**", como se muestra en la imagen 13.

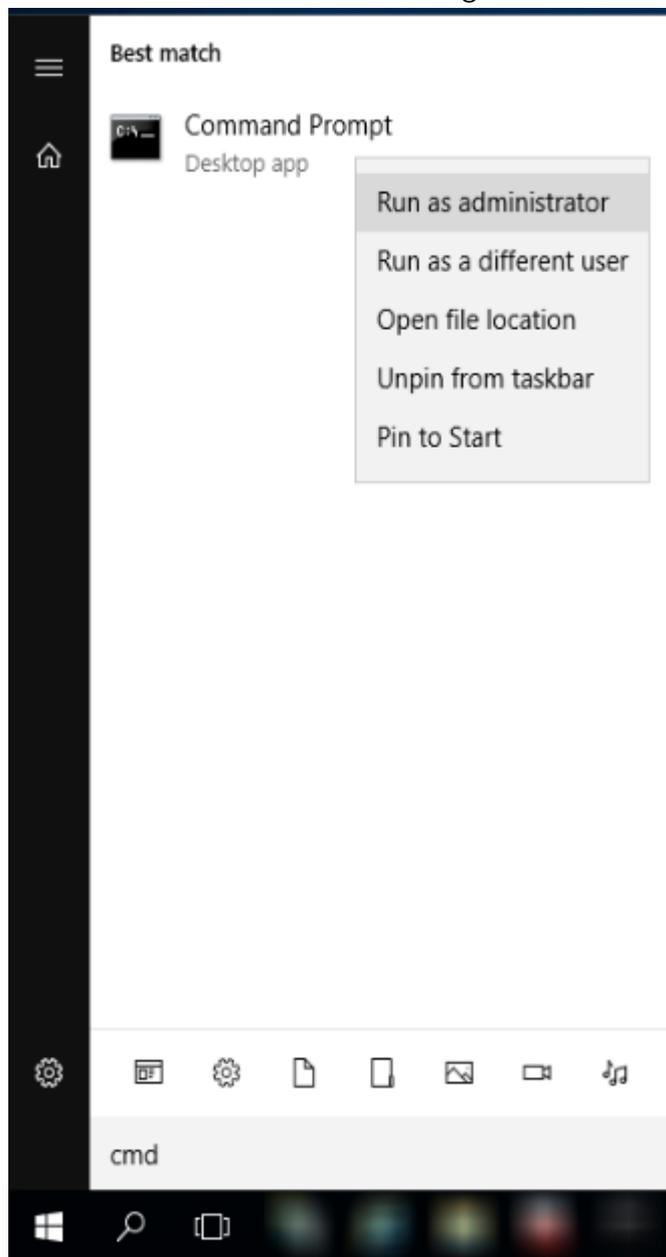


Imagen 9

2. En la línea de comandos, navegue hasta la carpeta C:\certificadoSINPE con el comando: **cd C:\certificadoSINPE**
3. Si se trata de una solicitud (request) de certificado de sello electrónico, ejecute el siguiente comando en la línea de comandos:



- a. **C:\WINDOWS\System32\certreq -new DatosPJSello.inf RequestSello.req**
 - b. En la carpeta C:\certificadoSINPE, habrá un archivo nuevo llamado RequestSello.req. que corresponde a la solicitud de certificado tipo Sello Electrónico
4. Si se trata de una solicitud (request) de certificado de agente electrónico, ejecute el siguiente comando en la línea de comandos:
- a. **C:\WINDOWS\System32\certreq -new DatosPJAgente.inf RequestAgente.req**
 - b. En la carpeta C:\certificadoSINPE, habrá un archivo nuevo, llamados RequestAgente.req que corresponde a la solicitud de certificado de tipo Agente Electrónico.

Otras consideraciones para entender el proceso

- **¿Qué tipo de servidor se requiere?** A nivel de servidor, no hay requerimiento. Básicamente sería un servidor que sea apto para los requerimientos del servicio.
- En caso de utilizar un dispositivo seguro de creación de firmas digitales (**HSM**), se recomienda utilizar un dispositivo que cuente con una certificación a nivel 3 o superior del estándar FIPS 140-2 o una certificación Common Criteria EAL 4+ en el perfil de protección SSCD Tipo 3 (Secure Signature-Creation Device).
- **¿El servidor puede ser virtual?** Sí, siempre y cuando el lugar donde se instale el certificado solicitado soporte trabajar con servidores virtuales.
- **Una vez que se haya emitido el certificado de persona jurídica (Sello Electrónico o Agente Electrónico). ¿Cuál sería el siguiente paso?** Una vez que se haya emitido el certificado, **la entidad debe modificar o crear su aplicación para que utilice este certificado.**
- **¿Se requiere de algún puerto en especial?** Esto depende de los requerimientos de la aplicación que vaya a utilizar el certificado y de cómo ésta se expone al público para ser consumida.
- **¿Qué tipo de sistema operativo se requiere?** Si fuera Windows Server, se recomienda de Windows Server 2008 R2 en adelante. Entre más nueva la versión del sistema operativo es mejor.



Anexos

Anexo A. La entidad solicitante del certificado posee una unidad organizacional

Si la entidad solicitante del certificado posee una unidad organizacional vinculada jurídicamente, puede incluir en el archivo “.inf” el **atributo opcional** “Unidad Organizacional (OU)”. Si se incluye, **éste debe ser diferente al nombre común de la persona jurídica solicitante (CN) y no debe sobrepasar los 64 caracteres**, en caso de que sobrepase los 64 caracteres deberá recortar el nombre a este número máximo de caracteres. Por ejemplo, para entidades con personería jurídica instrumental, se debe escribir en la unidad organizacional (OU) el **nombre de la persona jurídica instrumental en mayúscula**. A continuación, se muestran ejemplos de cómo se visualizaría un archivo “.inf” completo con la información requerida para la solicitud de un certificado de tipo Sello o Agente Electrónico con el atributo Unidad Organizacional.

a. Sello Electrónico con unidad organizacional

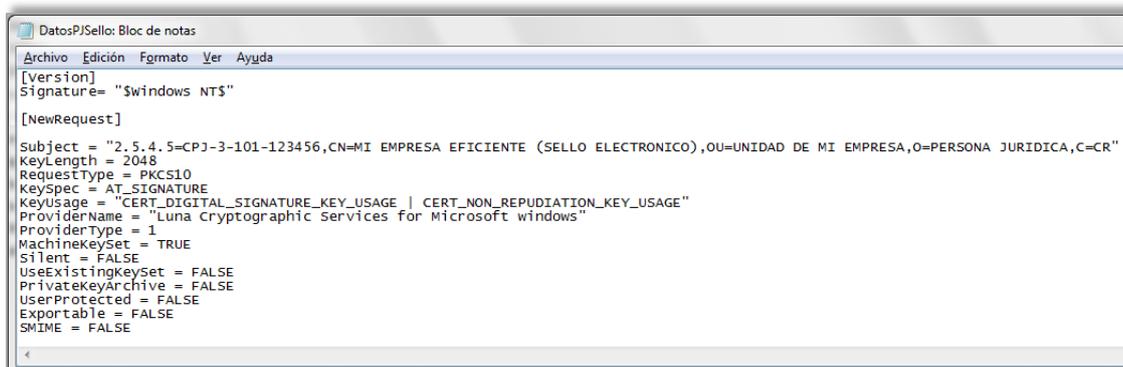


Imagen 10

b. Agente Electrónico con unidad organizacional

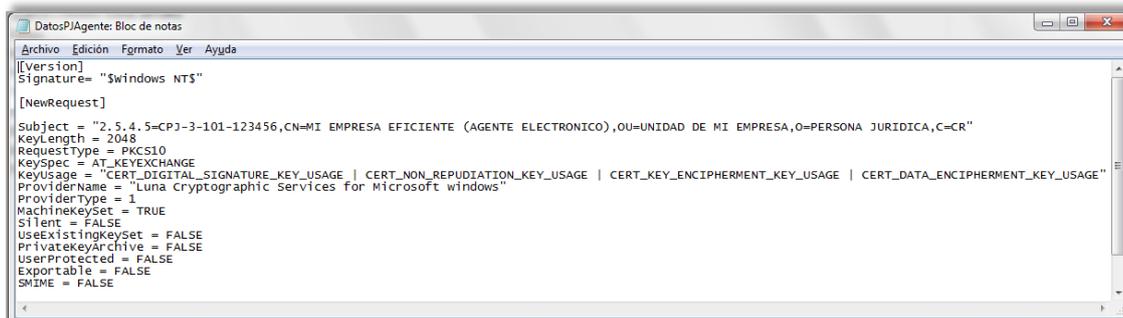


Imagen 11