



Guía para solicitar certificados de persona jurídica en Windows Sha2 2026



Contenido

Introducción	3
Paso 1: Completar la información del archivo INF.....	3
Paso 2: Crear requests para los certificados digitales.	9
Otras consideraciones para entender el proceso	10
Anexos.....	11

Introducción

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. Debe 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:

PRERREQUISITOS	TIPO	PLANTILLA	ARCHIVO	GENERACIÓN	RESULTADO	INFORMACIÓN	FIRMAR	DESCARGAR
----------------	------	-----------	---------	------------	-----------	-------------	--------	-----------

Para generar el request de certificado, es necesario descargar el archivo .inf con la información de su empresa y completar los campos con las etiquetas delimitadas por los caracteres "{#" y "#}".

```
[Version]
Signature= "Windows NT5"

[NewRequest]

Subject = "2.5.4.5=CPJ-3-101-123456, CN=NOMBRE EMPRESA (AGENTE ELECTRONICO),O=PERSONA JURIDICA,C=CR"
KeyLength = 3072
RequestType = PKCS10
KeySpec = AT_KEYEXCHANGE
KeyUsage = "CERT_DIGITAL_SIGNATURE_KEY_USAGE | CERT_NON_REPUDIATION_KEY_USAGE | CERT_KEY_ENCIIPHERMENT_KEY_USAGE | CERT_DATA_ENCIIPHERMENT_KEY_USAGE"
ProviderName = "{#PROVEEDOR CRIPTOGRAFICO#}"
ProviderType = "{#VALOR_TIPO_PROVEEDOR#}"
MachineKeySet = TRUE
Silent = FALSE
UseExistingKeySet = FALSE
PrivateKeyArchive = FALSE
UserProtected = FALSE
Exportable = FALSE
SMIME = FALSE

[RequestAttributes]
SAN = "{#DOMINIOS WEB#}"
```

Descargue el archivo .inf. [SatosP.Agente.inf](#)

Para terminar de generar el request debe continuar con los pasos que se indican en la guía: [Guía para generar una solicitud o request](#)
1. En Internet Explorer

- b. Para un certificado de tipo sello electrónico:

PRERREQUISITOS	TIPO	PLANTILLA	ARCHIVO	GENERACIÓN	RESULTADO	INFORMACIÓN	FIRMAR	DESCARGAR
----------------	------	-----------	---------	------------	-----------	-------------	--------	-----------

Para generar el request de certificado, es necesario descargar el archivo .inf con la información de su empresa y completar los campos con las etiquetas delimitadas por los caracteres "{#" y "#}".

```

[Version]
Signature = "$Windows NTS"

[NewRequest]

Subject = "2.5.4.5=CPJ-3-101-123456, CN=NOMBRE EMPRESA (SELLO ELECTRONICO), O=PERSONA JURIDICA, C=CR"
KeyLength = 3072
RequestType = PKCS10
KeySpec = AT_SIGNATURE
KeyUsage = "CERT_DIGITAL_SIGNATURE_KEY_USAGE | CERT_NON_REPUDIATION_KEY_USAGE"
ProviderName = "{#PROVEEDOR CRIPTOGRAFICO#}"
ProviderType = ({#VALOR_TIPO_PROVEEDOR#})
MachineKeySet = TRUE
Silent = FALSE
UseExistingKeySet = FALSE
PrivateKeyArchive = FALSE
UserProtected = FALSE
Exportable = FALSE
SMIME = FALSE
  
```

Descargue el archivo .inf [DatosPJ.Sello.inf](#)

Para terminar de generar el request debe continuar con los pasos que se indican en la [guía: Guía para generar una solicitud o request](#)

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**" o "**netsh nap client show csps**", el resultado será similar al mostrado en la siguiente imagen.

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.

```
Administrator: Command Prompt
C:\Windows\System32>certutil -csplist
Provider Name: Microsoft Base Cryptographic Provider v1.0
Provider Type: 1 - PROV_RSA_FULL

Provider Name: Microsoft Base DSS and Diffie-Hellman Cryptographic Provider
Provider Type: 13 - PROV_DSS_DH

Provider Name: Microsoft Base DSS Cryptographic Provider
Provider Type: 3 - PROV_DSS

Provider Name: Microsoft Base Smart Card Crypto Provider
Provider Type: 1 - PROV_RSA_FULL

Provider Name: Microsoft DH SChannel Cryptographic Provider
Provider Type: 18 - PROV_DH_SCHANNEL

Provider Name: Microsoft Enhanced Cryptographic Provider v1.0
Provider Type: 1 - PROV_RSA_FULL

Provider Name: Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider
Provider Type: 13 - PROV_DSS_DH

Provider Name: Microsoft Enhanced RSA and AES Cryptographic Provider
Provider Type: 24 - PROV_RSA_AES

Provider Name: Microsoft RSA SChannel Cryptographic Provider
Provider Type: 12 - PROV_RSA_SCHANNEL

Provider Name: Microsoft Strong Cryptographic Provider
Provider Type: 1 - PROV_RSA_FULL

Provider Name: Smart Card Middleware CSP
Provider Type: 1 - PROV_RSA_FULL

Provider Name: Microsoft Software Key Storage Provider

Provider Name: Athena Key Storage Provider

Provider Name: Microsoft Passport Key Storage Provider

Provider Name: Microsoft Platform Crypto Provider

Provider Name: Microsoft Smart Card Key Storage Provider
CertUtil: -csplist command completed successfully.

C:\Windows\System32>
```

- 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.

```

Provider Name: Microsoft Strong Cryptographic Provider
Provider Type: 1 - PROV_RSA_FULL → Con Tipo Proveedor

Provider Name: Smart Card Middleware CSP
Provider Type: 1 - PROV_RSA_FULL

Provider Name: Microsoft Software Key Storage Provider
Provider Name: Athena Key Storage Provider → Sin Tipo Proveedor

```

Si el proveedor criptográfico seleccionado en el paso anterior tiene asociado un tipo de proveedor (provider type), como el mostrado en la imagen anterior, el valor que se debe indicar en este campo es el número que aparece después de los dos puntos (1). El ejemplo de cómo debe colocarse en el archivo ".inf" se muestra en la siguiente imagen.

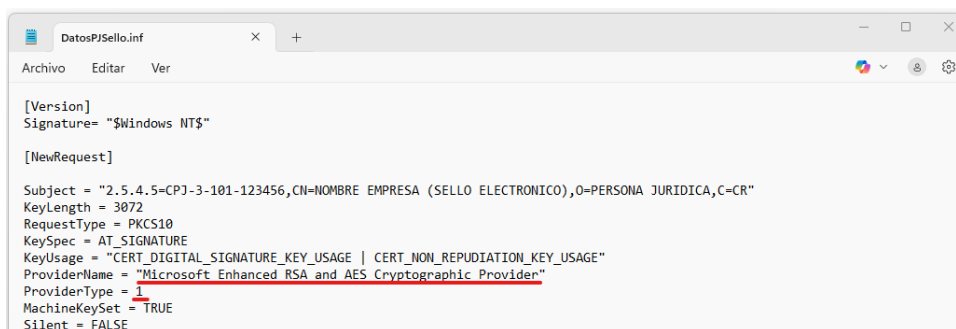
```

Provider Name: Microsoft Strong Cryptographic Provider
Provider Type: 1 - PROV_RSA_FULL

Provider Name: Smart Card Middleware CSP
Provider Type: 1 - PROV_RSA_FULL

Provider Name: Microsoft Software Key Storage Provider
Provider Name: Athena Key Storage Provider

```



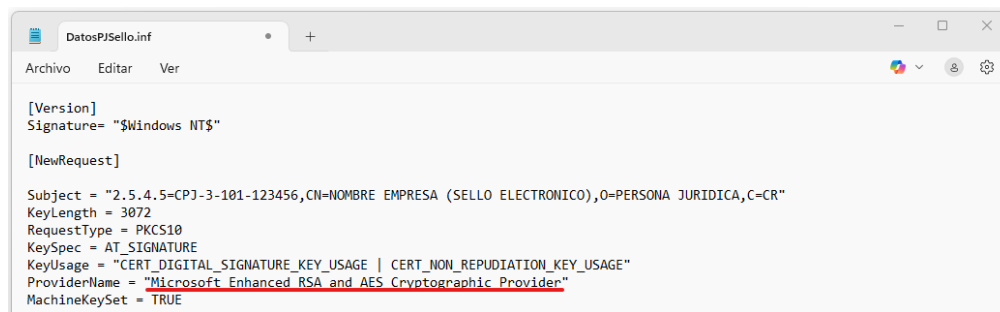
```

[Version]
Signature= "$Windows NT$"

[NewRequest]
Subject = "2.5.4.5=CPJ-3-101-123456,CN=NOMBRE EMPRESA (SELLO ELECTRONICO),O=PERSONA JURIDICA,C=CR"
KeyLength = 3072
RequestType = PKCS10
KeySpec = AT_SIGNATURE
KeyUsage = "CERT_DIGITAL_SIGNATURE_KEY_USAGE | CERT_NON_REPUDIATION_KEY_USAGE"
ProviderName = "Microsoft Enhanced RSA and AES Cryptographic Provider"
ProviderType = 1
MachineKeySet = TRUE
Silent = FALSE

```

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



- 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

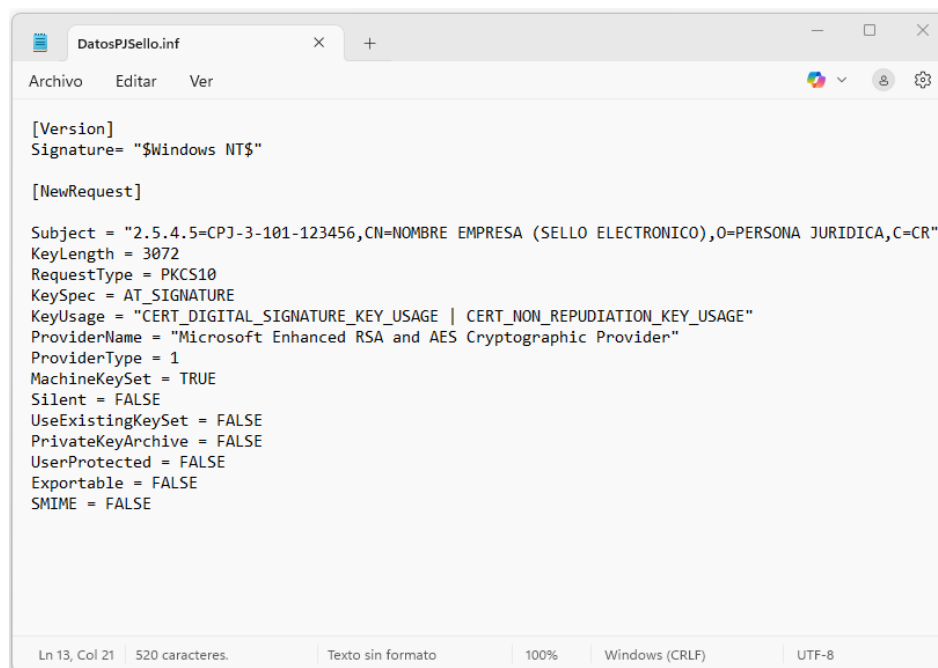
- Se debe de escribir en minúscula.
 - Los dominios no pueden contener caracteres especiales como la tilde.
 - No debe contener http.
 - Se puede escribir un dominio o múltiples dominios
 - SAN = "dns=[dominio]"
 - SAN = "dns=[dominio]&dns=[dominio]"
 - SAN = "dns=www.miemp.co.cr&dns=miservidor.miemp.co.cr&dns=mail.miemp.co.cr"
 - El número máximo de registros en el SAN es de 10 dominios.
 - Se puede escribir todo el dominio
 - miservidor.miemp.co.cr
 - Se puede escribir sólo el final del dominio, pero debe de tener un asterisco antes del primer punto
 - *.miemp.co.cr
 - 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.



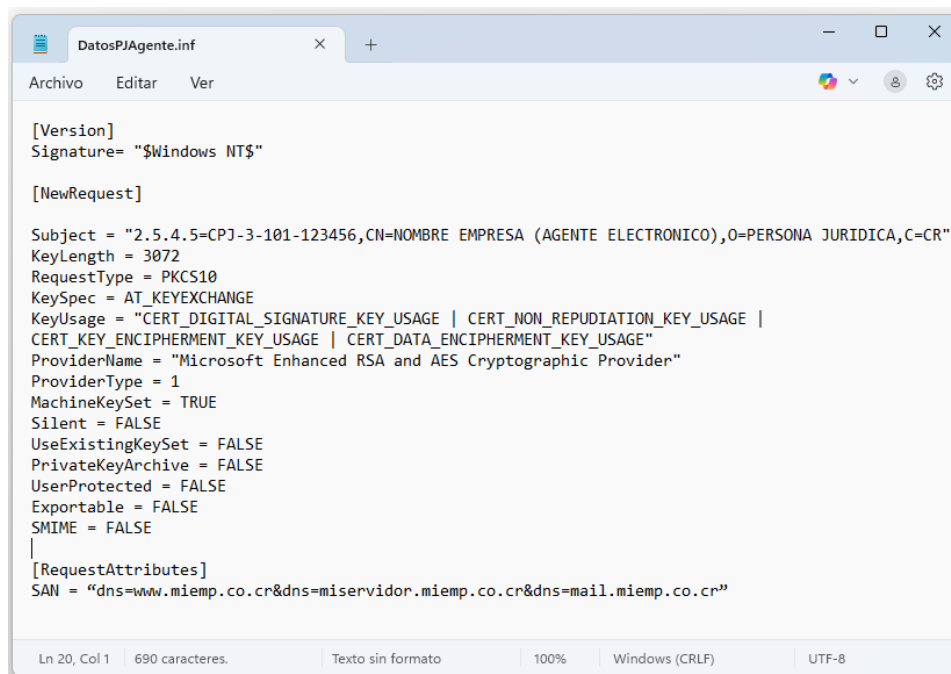
```
[Version]
Signature= "$Windows NT$"

[NewRequest]

Subject = "2.5.4.5=CPJ-3-101-123456,CN=NOMBRE EMPRESA (SELLO ELECTRONICO),O=PERSONA JURIDICA,C=CR"
KeyLength = 3072
RequestType = PKCS10
KeySpec = AT_SIGNATURE
KeyUsage = "CERT_DIGITAL_SIGNATURE_KEY_USAGE | CERT_NON_REPUDIATION_KEY_USAGE"
ProviderName = "Microsoft Enhanced RSA and AES Cryptographic Provider"
ProviderType = 1
MachineKeySet = TRUE
Silent = FALSE
UseExistingKeySet = FALSE
PrivateKeyArchive = FALSE
UserProtected = FALSE
Exportable = FALSE
SMIME = FALSE
```

Ln 13, Col 21 | 520 caracteres. | Texto sin formato | 100% | Windows (CRLF) | UTF-8

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



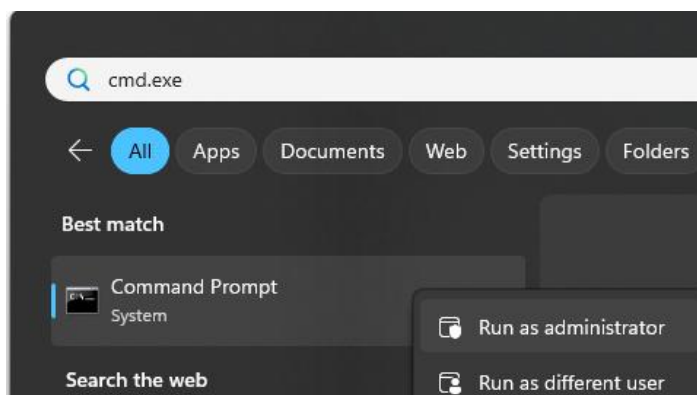
```
[Version]
Signature= "$Windows NT$"

[NewRequest]

Subject = "2.5.4.5=CPJ-3-101-123456,CN=NOMBRE EMPRESA (AGENTE ELECTRONICO),O=PERSONA JURIDICA,C=CR"
KeyLength = 3072
RequestType = PKCS10
KeySpec = AT_KEYEXCHANGE
KeyUsage = "CERT_DIGITAL_SIGNATURE_KEY_USAGE | CERT_NON_REPUDIATION_KEY_USAGE | CERT_KEY_ENCIPHERMENT_KEY_USAGE | CERT_DATA_ENCIPHERMENT_KEY_USAGE"
ProviderName = "Microsoft Enhanced RSA and AES Cryptographic Provider"
ProviderType = 1
MachineKeySet = TRUE
Silent = FALSE
UseExistingKeySet = FALSE
PrivateKeyArchive = FALSE
UserProtected = FALSE
Exportable = FALSE
SMIME = FALSE
[RequestAttributes]
SAN = "dns=www.miemp.co.cr&dns=miservidor.miemp.co.cr&dns=mail.miemp.co.cr"
```

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 "cmd.exe", haciendo clic derecho y finalmente clic en "Ejecutar como administrador"



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 DatosPJSello.inf RequestSello.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.

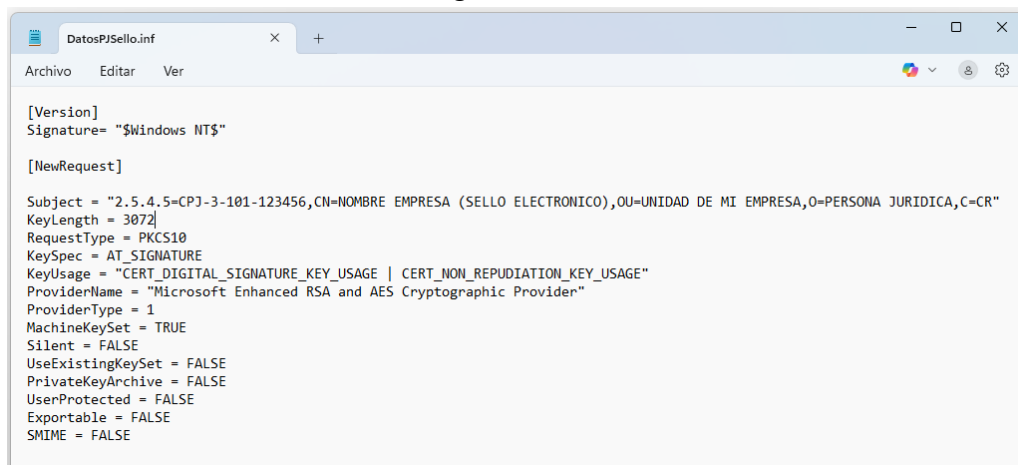
- **¿Se requiere de algún puerto en especial?** Esto depende de los requerimientos de la aplicación que vaya a utilizar el certificado y de cómo ésta se expone al público para ser consumida.
- **¿Qué tipo de sistema operativo se requiere?** Se requiere utilizar un sistema operativo Windows Server que se encuentre dentro de las versiones soportadas por Microsoft.

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



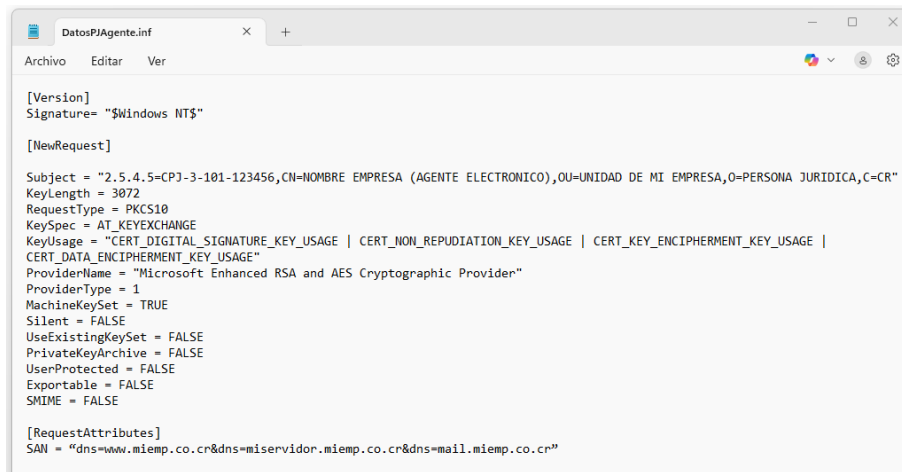
```

[Version]
Signature= "$Windows NT$"

[NewRequest]

Subject = "2.5.4.5=CPJ-3-101-123456,CN=NOMBRE EMPRESA (SELLO ELECTRONICO),OU=UNIDAD DE MI EMPRESA,O=PERSONA JURIDICA,C=CR"
KeyLength = 3072
RequestType = PKCS10
KeySpec = AT_SIGNATURE
KeyUsage = "CERT_DIGITAL_SIGNATURE_KEY_USAGE | CERT_NON_REPUDIATION_KEY_USAGE"
ProviderName = "Microsoft Enhanced RSA and AES Cryptographic Provider"
ProviderType = 1
MachineKeySet = TRUE
Silent = FALSE
UseExistingKeySet = FALSE
PrivateKeyArchive = FALSE
UserProtected = FALSE
Exportable = FALSE
SMIME = FALSE
  
```

b) Agente Electrónico con unidad organizacional



A screenshot of a text editor window titled 'DatosPIAgente.inf'. The window has a menu bar with 'Archivo', 'Editar', and 'Ver'. The content is an INI-style configuration file for a digital agent. It includes sections for version, signature, new request parameters, and request attributes. The 'NewRequest' section contains detailed settings for a certificate request, including subject, key length, request type, key spec, key usage, provider name, and various flags like 'MachineKeySet' and 'Exportable'.

```
[Version]
Signature= "$Windows NT$"

[NewRequest]
Subject = "2.5.4.5=CPJ-3-101-123456,CN=NOMBRE EMPRESA (AGENTE ELECTRONICO),OU=UNIDAD DE MI EMPRESA,O=PERSONA JURIDICA,C=CR"
KeyLength = 3072
RequestType = PKCS10
KeySpec = AT_KEYEXCHANGE
KeyUsage = "CERT_DIGITAL_SIGNATURE_KEY_USAGE | CERT_NON_REPUDIATION_KEY_USAGE | CERT_KEY_ENCIPHERMENT_KEY_USAGE | CERT_DATA_ENCIPHERMENT_KEY_USAGE"
ProviderName = "Microsoft Enhanced RSA and AES Cryptographic Provider"
ProviderType = 1
MachineKeySet = TRUE
Silent = FALSE
UseExistingKeySet = FALSE
PrivateKeyArchive = FALSE
UserProtected = FALSE
Exportable = FALSE
SMIME = FALSE

[RequestAttributes]
SAN = "dns=www.miemp.co.cr&dns=miservidor.miemp.co.cr&dns=mail.miemp.co.cr"
```