AGESIC
Área de tecnología

Tutorial para la Solicitud e Instalación de Certificados para la PGE

Plataforma Java

Nombre actual del archivo: Tutorial_Certificados_Java_v2.0.odt

Liniers 1324 piso 4, Torre Ejecutiva Sur
Montevideo – Uruguay
Tel./Fax: (+598) 2901.2929*
Email: soporte@agesic.gub.uy
www.agesic.gub.uy

Índice de contenido

1 - Introducción 4
1.1 - Objetivo 4
1.2 - Prerrequisitos 4
1.3 - Establecimiento de una comunicación segura con la PGE 4
1.4 - Autenticación ante la PGE 6
1.5 - Sobre las herramientas utilizadas 6
2 - Obtención y configuración de certificados para SSL 8
2.1 - Objetivo 8
2.2 - Creación de almacén de claves (keystore) 9
2.2.1 - Paso 1: Generación de clave privada (PK) 9
2.2.2 - Paso 2: Solicitud de Firma de Certificado 15
2.2.3 - Paso 3: Obtener e importar en el repositorio de certificados de confianza el certificado de la PGE 18
2.2.4 - Paso 4: Importar CSR firmado por la CA en el almacén de claves 20
2.3 - Creación del almacén de confianza (truststore de SSL) 22
3 - Obtención y configuración de certificados de persona jurídica 27
3.1 - Objetivo 27
3.2 - Importar PFX firmado por la CA en el almacén de claves 28

Introducción

1.1 - Objetivo

Este documento se propone ser una guía para la generación e instalación de los certificados digitales que necesitan los clientes para consumir servicios web publicados en la Plataforma de Gobierno Electrónico (PGE).

1.2 - Prerrequisitos

Este documento asume que el lector conoce los conceptos y las tecnologías involucradas:

- RedUy y la Plataforma de Gobierno Electrónico (PGE).
- Criptografía de clave pública, certificados digitales, SSL.

1.3 - Establecimiento de una comunicación segura con la PGE

Una comunicación segura, lograda mediante la tecnología SSL o TLS (SSL, o Secure Socket Layer, fue remplazada por TSL, o Transport Secure Layer) proporciona autenticación entre cliente y servidor, y confidencialidad e integridad de la información entre los extremos en una red mediante el uso de criptografía, encriptando la información en el emisor y desencriptándola en el receptor. Entre los pasos que realiza el protocolo SSL para establecer una conexión segura se encuentra el intercambio de claves públicas entre las partes (cliente y PGE) y la autenticación basada en certificados digitales. Habitualmente, sobre la PGE el cliente y el servidor son autenticados (es decir, cada uno garantiza la identidad del otro) mediante el uso de certificados digitales: tanto el cliente como el servidor cuentan cada uno con un certificado propio que deben presentar a la contraparte, la cual debe reconocer dicho certificado (o en su defecto, la firma del mismo) para admitir el establecimiento de la conexión; en el caso de que una de las partes no reconozca el certificado de la otra, la conexión segura no podrá ser establecida. En el caso de la PGE, el certificado que debe presentar el cliente es emitido por AGESIC, y es propio de cada cliente (es decir, de cada organismo que pretende consumir servicios a través de la PGE), e intransferible. El certificado presentado

al cliente por la PGE es también emitido por AGESIC, y es el mismo para todos los organismos.

El procedimiento que debe seguir un organismo para configurar los certificados digitales con el fin de establecer una comunicación segura con la PGE se resume en los siguientes pasos:

1. Crear un certificado digital conteniendo un par de claves (pública y privada); la clave privada será propiedad del organismo, y no debe hacerse pública bajo ningún motivo.
2. Crear, para el certificado creado en el paso anterior, la solicitud de firma de certificado (CSR, Certificate Signing Request) y enviarlo a la autoridad certificadora (CA, Certificate Authority), la cual en este caso será AGESIC, para que lo firme digitalmente y lo devuelva firmado.
3. Obtener e importar en el repositorio de certificados de confianza el certificado de la PGE en el cual se confiará e incluirlo dentro de los certificados de confianza del organismo.
4. Una vez recibida la respuesta de la autoridad certificadora, conteniendo el certificado firmado, importarlo en el repositorio de certificados propios.

En la sección **Obtención y configuración de certificados para SSL** se describe con mayor detalle cada uno de estos pasos.

1.4 - Autenticación ante la PGE

Además del establecimiento de una comunicación segura entre el cliente y la PGE, es necesario que el cliente se autentique a los efectos de que la PGE pueda autorizarlo, o no, a invocar servicios en la plataforma. Para ello se utiliza un certificado emitido por una entidad certificadora reconocida por el Estado que lo identifique como una Persona Jurídica existente y válida. Esto se distingue de lo descrito anteriormente en que el establecimiento de la comunicación segura usando SSL permite el intercambio de información de forma confiable entre

servidores, mientras que en este caso el objetivo es que la PGE reconozca al cliente a nivel de cuál organismo realiza cuál transacción. En este caso, solo el cliente debe presentar el certificado de persona jurídica a la PGE.

El procedimiento que debe seguir un organismo para configurar el certificado digital con el fin de autenticarse ante la PGE se resume en los siguientes pasos:

1. Solicitar un certificado de Persona Jurídica a una entidad certificadora reconocida por el estado (por el momento solo El Correo está habilitada para ello).
2. Una vez recibida la respuesta de la autoridad certificadora, conteniendo el certificado firmado, importarlo en el repositorio de certificados propios.

En la sección **Obtención y configuración de certificados de persona jurídica** se describe con mayor detalle cada uno de estos pasos.

1.5 - Sobre las herramientas utilizadas

Existen diferentes herramientas para realizar la generación de claves y la importación de certificados digitales. En este documento se utilizará la herramienta Keystore Explorer, la cual se puede descargar del sitio http://keystore-explorer.sourceforge.net/. Los certificados se almacenan en almacenes de claves. Un almacén de claves es similar a un archivo comprimido que contiene una o más claves (públicas o privadas) y certificados digitales, y donde cada entrada está identificada por un nombre, deniminado “alias” (dado un alias particular, o bien corresponde a un único certificado o clave, o a ninguno).

Para establecer la comunicación segura utilizando SSL se requerirán dos almacenes de claves:

1. Un almacén de claves, llamado **keystore de SSL**, en el cual se almacenarán las claves privadas propias del organismo y que solo el propio organismo conoce [1]
2. Un almacén de claves de confianza, llamado **truststore de SSL**, donde se almacenarán las claves públicas de las entidades en las cuales se confía (en particular, el certificado conteniendo la clave pública de la PGE).

Por otra parte, para la autenticación del cliente ante la PGE, solo es necesario un almacén de claves, llamado **keystore del organismo**, que contenga la clave privada del organismo (certificado de persona jurídica que demuestra que es un organismo reconocido por el Estado).

Importante: Se recomienda fuertemente que el keystore de SSL y el keystore del organismo sean archivos diferentes.

En resumen, se gestionarán tres almacenes de certificados: un truststore y dos keystores. Los detalles de la generación de los mismos se describirán en el resto del documento.

Obtención y configuración de certificados para SSL

1.6 - Objetivo

En esta sección se describirá el proceso de configuración de los certificados digitales para que el cliente pueda establecer una comunicación segura con la PGE, utilizando la tecnología SSL.

Como se explicó anteriormente, se requerirán dos certificados digitales. Uno de estos certificados contendrá la clave pública de la PGE y deberá instalarse en el

[1] En la práctica no solo se tendrán las claves privadas, sino que se necesitará el certificado de la CA como una entrada más de este almacén para la correcta ejecución de los pasos. Se detallará más adelante.

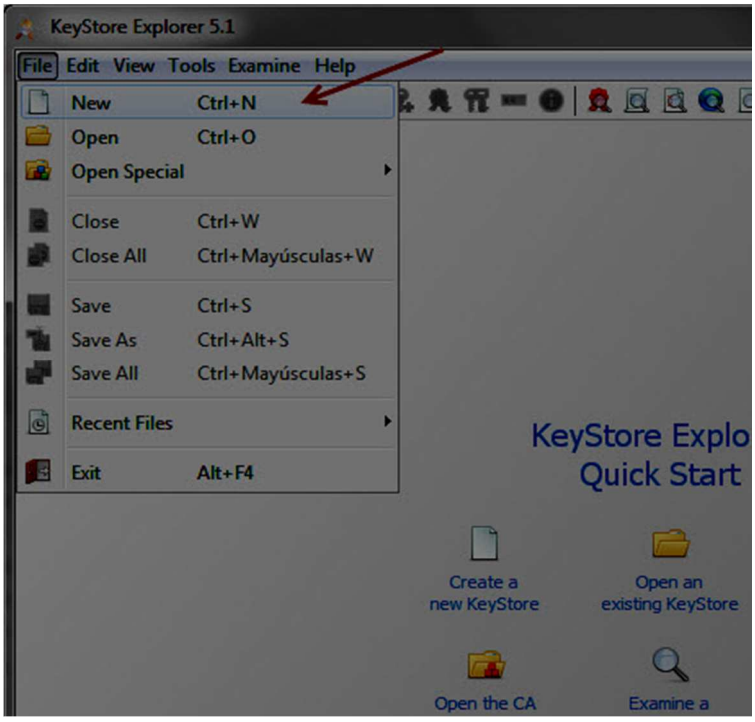
NOTA: todos los procedimientos que se describen en esta sección aplican tanto al ambiente de testing como de producción. Sin embargo, para el ambiente de testing, no es necesaria la utilización de un certificado de persona jurídica. El Keystore de Organismo puede ser el mismo que el Keystore SSL.

truststore de SSL, de forma tal que cuando el cliente intente establecer una comunicación con la PGE, conozca la clave pública de la misma y así pueda encriptar información que solo la PGE podrá desencriptar utilizando su clave privada. El otro de los certificados, que se debe instalar en el keystore de SSL, contiene tanto la clave pública como la privada del propio cliente, de forma tal de que cuando intente establecer una comunicación con la PGE pueda proporcionarle su clave pública, para que la PGE pueda encriptar información usando dicha clave, que solo el cliente podrá desencriptar usando su propia clave privada. La PGE confiará en el certificado proporcionado por el cliente debido a que estará firmado por una entidad certificadora reconocida por la PGE (la propia AGESIC).

1.7 - Creación de almacén de claves (keystore)

1.7.1 - Paso 1: Generación de clave privada (PK)

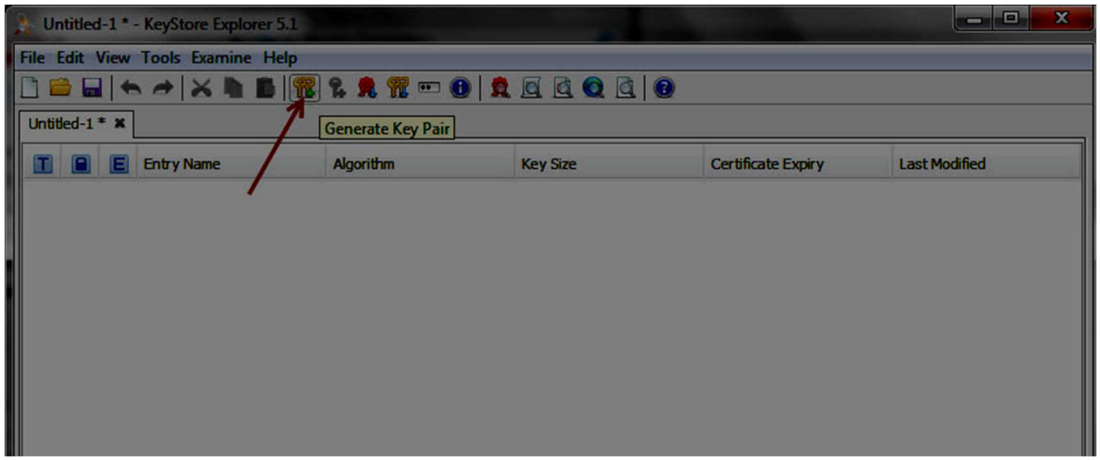
El primer paso para solicitar un certificado digital para SSL es crear el par de claves (una pública y otra privada), las cuales se almacenarán en un almacén de claves (keystore de SSL). La herramienta para la gestión de keystores a utilizar en este tutorial se denomina *Keystore Explorer y se puede descargar del sitio http://keystore-explorer.sourceforge.net/.*



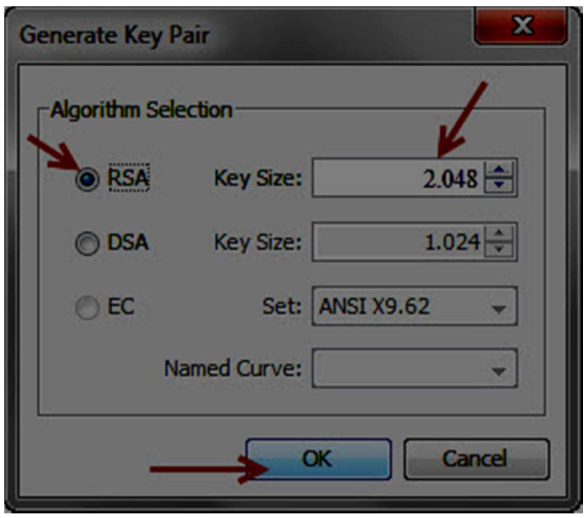
A continuación se presentan los pasos a ejecutar para crear la clave privada del certificado SSL:

1. Crear almacén de claves de tipo JKS:

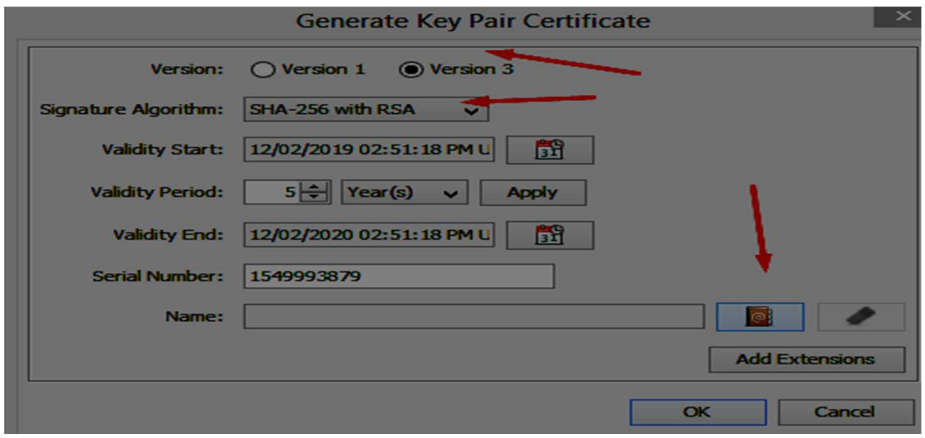
2. Seleccionar la opción para crear un nuevo par de claves:

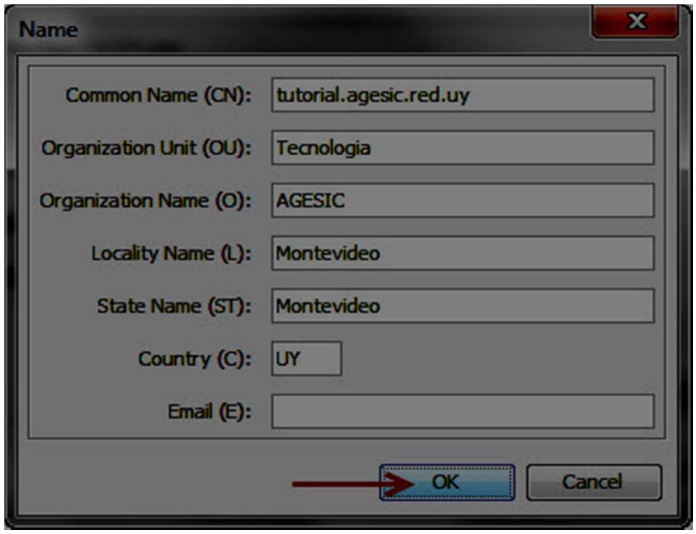


3. Seleccionar algoritmo RSA de largo 2048



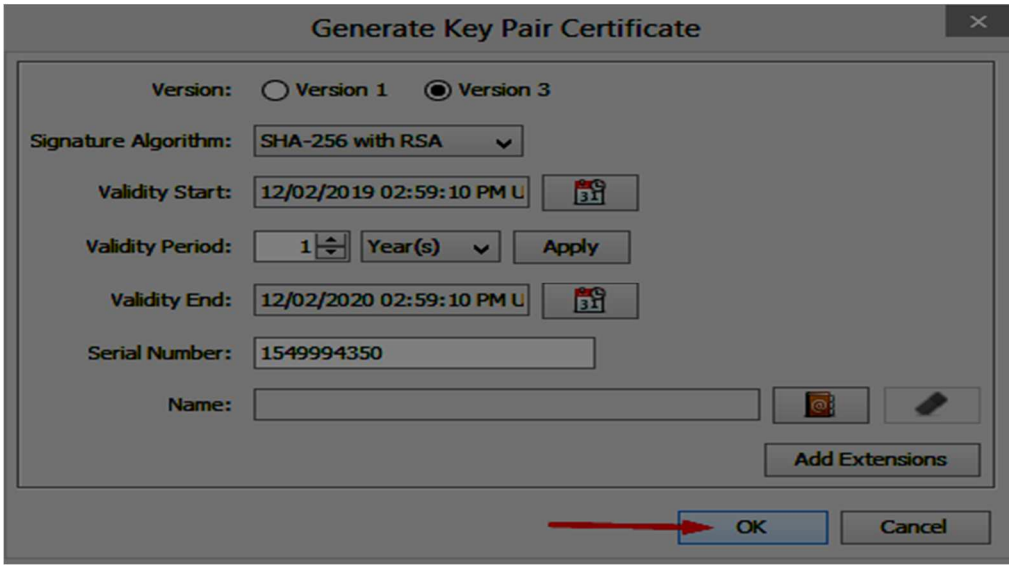
4. Seleccionar versión 3 de SSL y algoritmo de firma SHA-256 with RSA. Luego hacer clic en la opción de configuración del nombre del certificado:



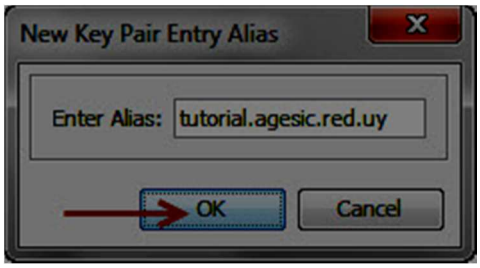


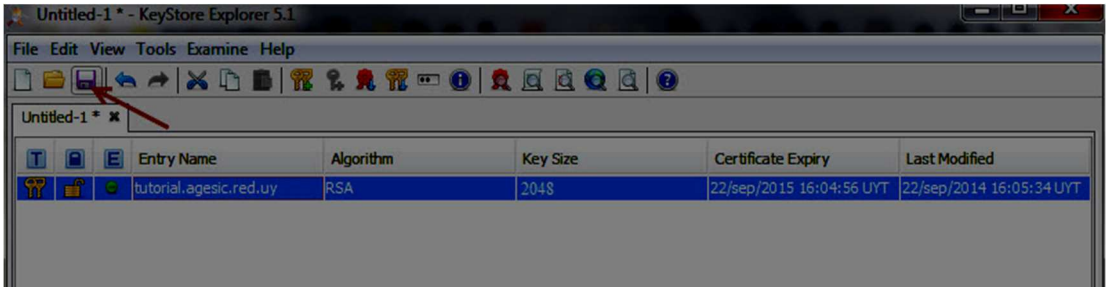
5. Configurar el nombre teniendo en cuenta los siguientes puntos:
   a. *Common Name (CN)*: debe corresponder preferentemente con el nombre del host del cliente en REDuy. Es el nombre del servidor registrado en el DNS de la PGE. El formato a seguir debe ser *nombreServidor.nombreOrganismo.red.uy* (ej: tutorial.agesic.red.uy).
   b. *Organization Unit (OU)*: debe ser el nombre de la unidad dentro de la Unidad Ejecutora; evitar las tildes, eñes y otros caracteres especiales (ej: Secretaria General).
   c. *Organization (O)*: debe ser el nombre completo de la Unidad Ejecutora u Organismo. Evitar las tildes, eñes y otros caracteres especiales (ej: Direccion Nacional de Policia Tecnica).
   d. *Locality Name (L)*: debe ser el nombre de la ciudad donde se encuentra la Unidad Ejecutora (ej: Montevideo).
   e. *State Name (ST)*: debe ser el nombre del departamento en el cual se encuentra la Unidad Ejecutora (ej: Montevideo).
   f. *Country (C)*: debe ser el código ISO del país en el formato de 2 letras (ej: UY).

6. Confirmar la configuración del certificado:



7. Setear alias y password del certificado. El alias identificará al par de claves dentro del almacén (ej: tutorial.agesic.red.uy). Si se especifica un alias que ya identifica a otra entrada en el keystore, el procedimiento fallará con un mensaje de error





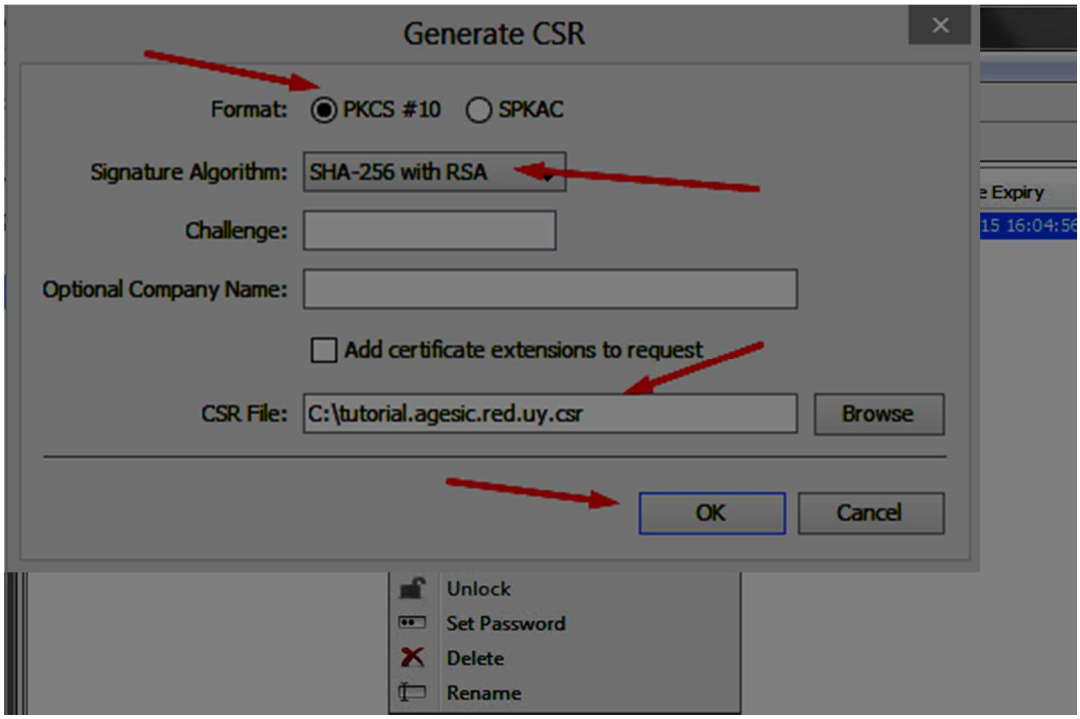
8. Guardar el keystore creado y configurar la password. **La password debe ser exactamente la misma que la configurada en el paso anterior**.

Una vez cumplidos estos pasos, se tendrá un almacén de claves, llamado keystore de SSL, conteniendo un par de claves (pública y privada) protegidas por la misma contraseña que el keystore. El siguiente paso consiste en enviar parte

de esta información para que AGESIC la valide y firme.

1.7.2 - Paso 2: Solicitud de Firma de Certificado

El segundo paso consiste en obtener la firma de la autoridad certificadora (CA o Certification Authority) del certificado creado en el paso 1, que en este caso será AGESIC, que garantice que la información contenida en el certificado es válida (de esta forma, la PGE confiará en el certificado cuando el cliente intente establecer una comunicación SSL). Para ello primero se generará, a partir del certificado recientemente creado, un archivo CSR (Certificate Signed Request, solicitud de firma de certificado), el cual es un archivo con extensión .csr que sigue



el estándar PKCS10 para la solicitud de firma de certificado, y luego se enviará dicho archivo vía correo electrónico a AGESIC.

Para la generación del CSR también se utiliza la herramienta *keystore explorer*.

Los pasos para generar el CSR son los siguientes:

1. Hacer clic derecho sobre el certificado recién creado y seleccionar la opción “Generate CSR”:

2. Seleccionar el formato “PKCS #10” y el algoritmo de firma “SHA-256 with RSA”. Luego especificar la ruta donde se desa guardar el archivo csr a generar:

Luego de generado el archivo CSR (en formato PKCS10) se debe enviarlo por correo electrónico a soporte@agesic.gub.uy con asunto “**Solicitud de PKCS12 –**

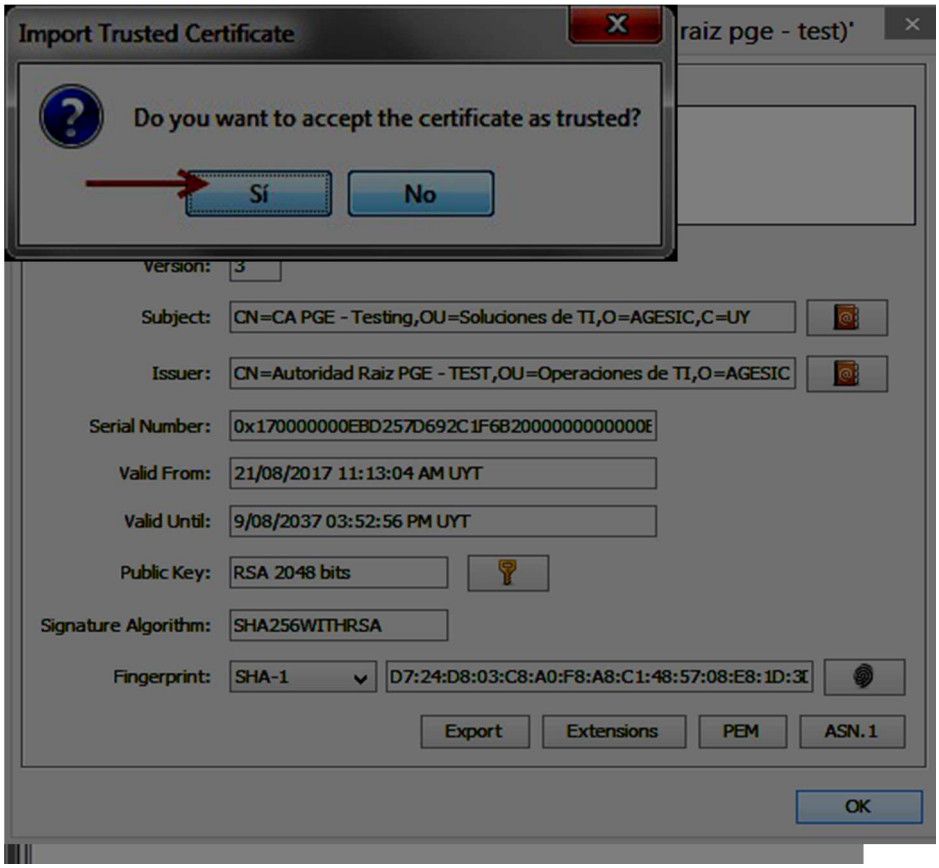
Ambiente X", donde X debe ser uno de "Testing" o "Producción". Luego, se debe esperar la respuesta de AGESIC conteniendo la firma de los datos; cuando se reciba la respuesta, deberá importarse en el mismo almacén de claves que se ha utilizado hasta el momento para añadir a los datos contenidos la firma hecha por AGESIC (ver sección 2.2.3 y 2.2.4).

1.

1.7.3 - Paso 3: Obtener e importar en el repositorio de certificados de confianza el certificado de la PGE

Para poder importar correctamente el certificado firmado que fue devuelto por AGESIC al almacén de claves es necesario tener previamente en el mismo almacén de claves el certificado público de la CA (que debe ser proporcionado por AGESIC). Para hacerlo, nuevamente se utiliza la herramienta Keystore Explorer. Los pasos para hacer esto se presentan a continuación:

1. En el Keystore creado anteriormente, ejecutar la opción "Import Trusted Certificate", y seleccionar el archivo correspondiente a la CA del ambiente en cuestión (HGTivoliCA.cer para testing, CA.pge.red.uy.cer para producción):



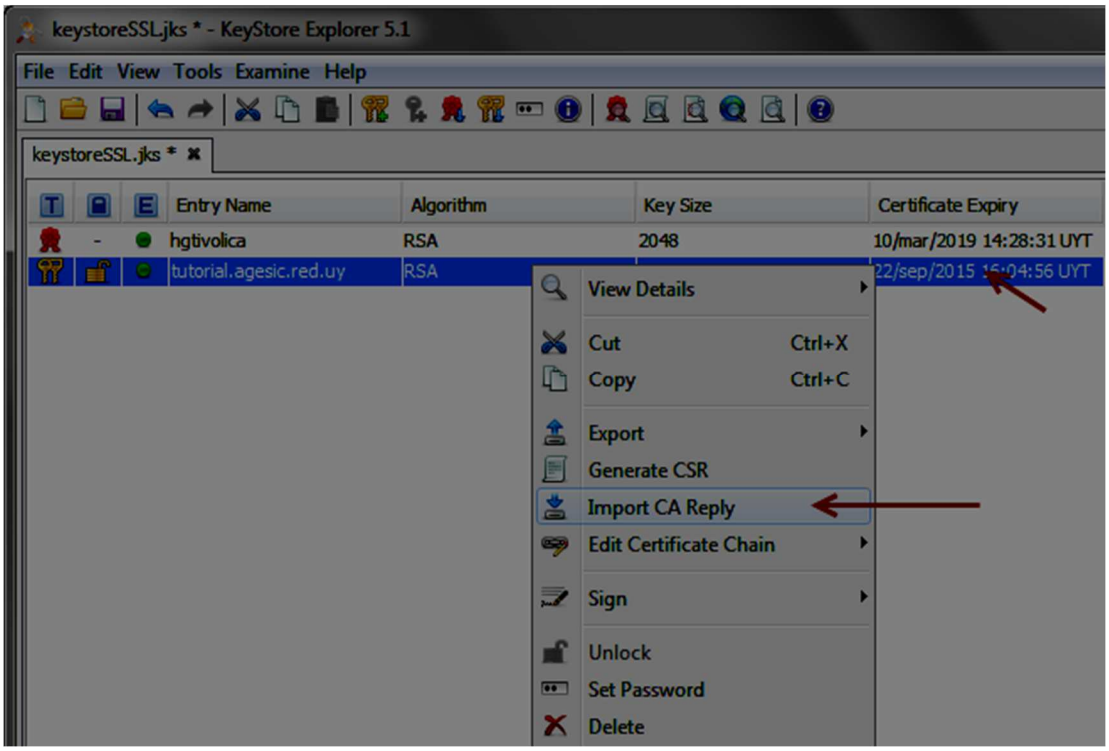
1.7.4 - Paso 4: Importar CSR firmado por la CA en el almacén de claves

El paso final es importar el archivo recibido como respuesta, que contiene los datos firmados por la CA (en este caso, AGESIC) en el almacén de claves. Para hacerlo, nuevamente se utiliza la herramienta *Keystore Explorer.* A continuación

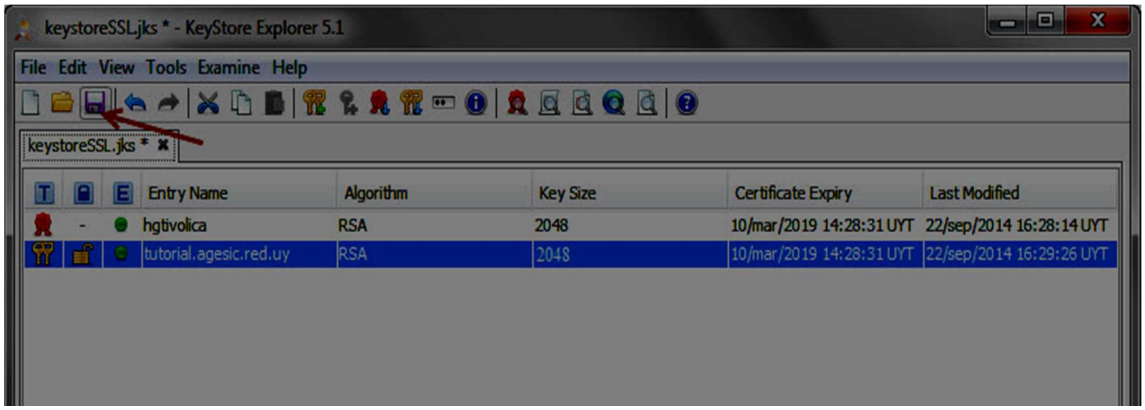
se presentan los pasos necesarios para importar el certificado emitido por la CA de AGESIC:

2. Abrir el truststore creado desde donde se emitió la solicitud de firma de la CA.

3. Hacer clic derecho sobre el certificado creado y seleccionar la opción “Import CA Reply”. Luego, seleccionar el certificado firmado por la CA de AGESIC enviado por el equipo de mesa de ayuda.



4. Guardar las modificaciones realizadas sobre el keystore:

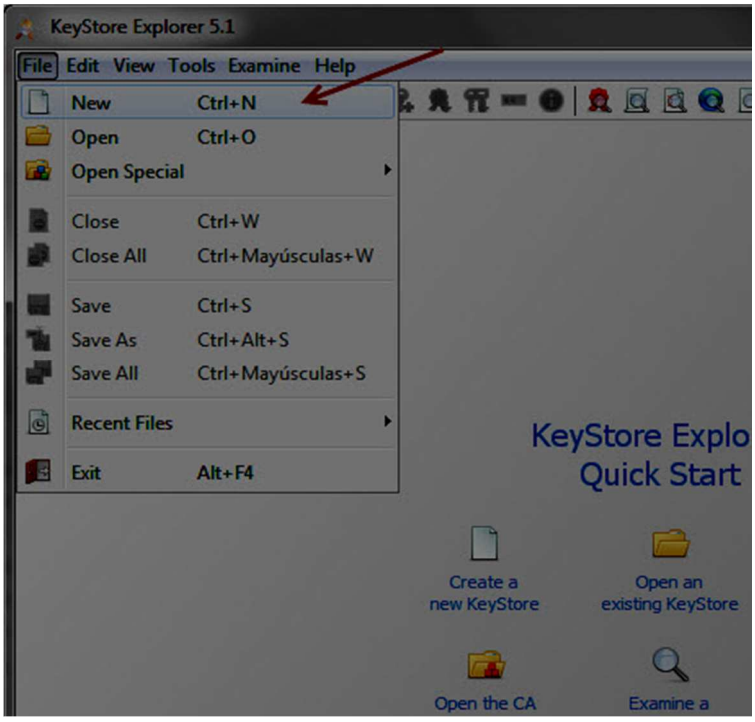


1.8 -
1.9 - Creación del almacén de confianza (truststore de SSL)

Además de generar un par de claves, solicitar la firma de las mismas y la instalación de la respuesta en el repositorio de certificados, es necesario crear otro almacén de certificados que contendrá la clave pública de la PGE, utilizada para confiar en el certificado que entregue la PGE al cliente cuando éste intente establecer la comunicación segura. En el caso del ambiente de testing el certificado a importar es *testservicios.pge.red.uy.cer* y para el caso del ambiente de producción el certificado es *servicios.pge.red.uy.cer* [2].

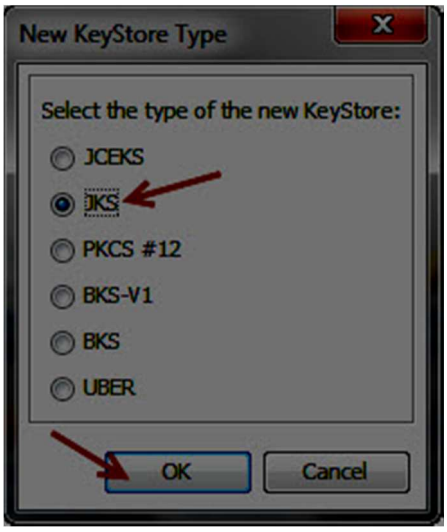
Nuevamente se utilizará la herramienta *Keystore Explorer.*

[2]Los certificados ya sea para el ambiente de testing o producción pueden ser descargados de ftp://ftp.agesic.gub.uy/CertificadosPGE/ (usuario: agesic, contraseña: publico).

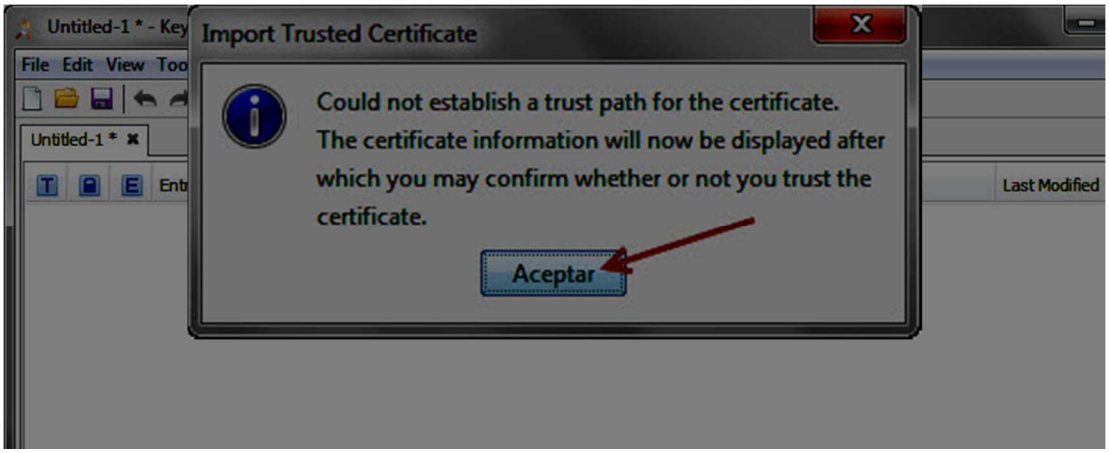


A continuación se presentan los pasos necesarios para crear el almacén de confianza:

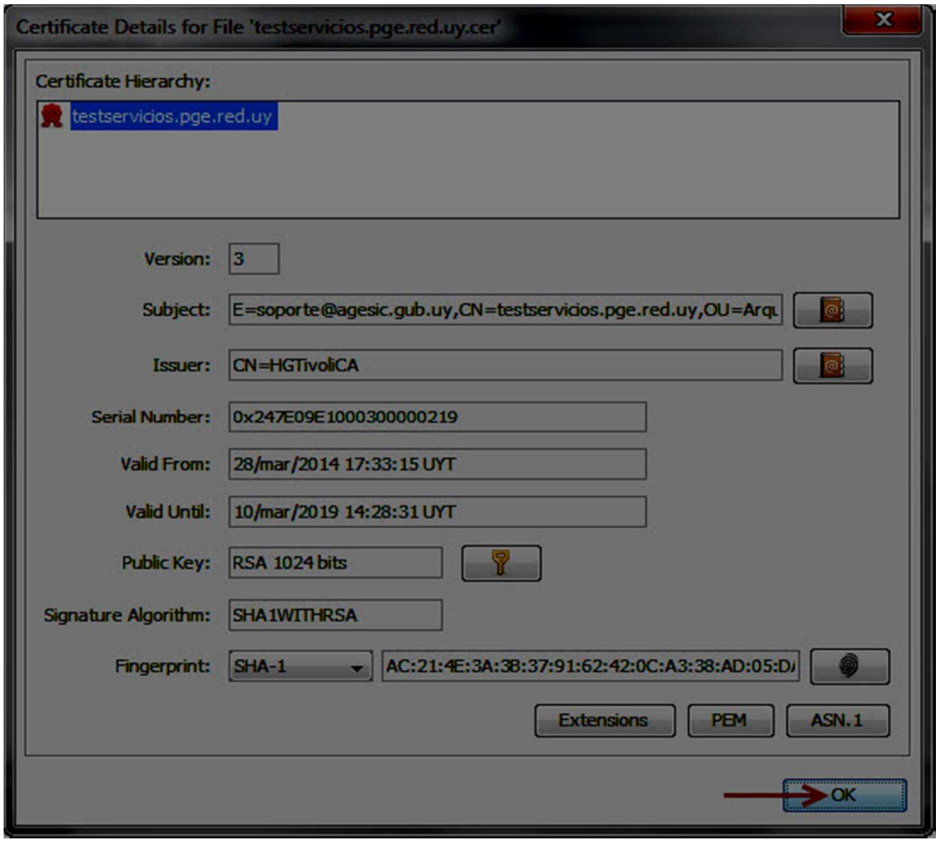
1. Crear almacén de claves de tipo JKS:

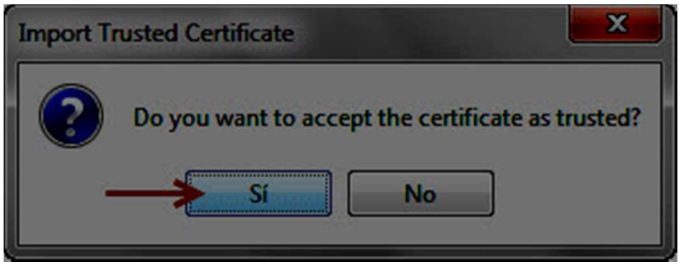


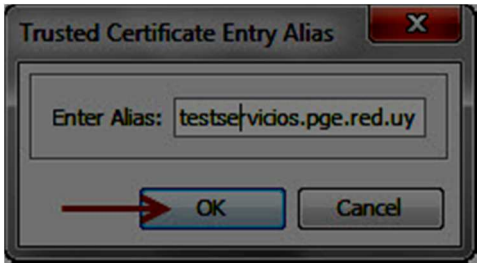
2. Seleccionar la opción “Import Trusted Certificate”

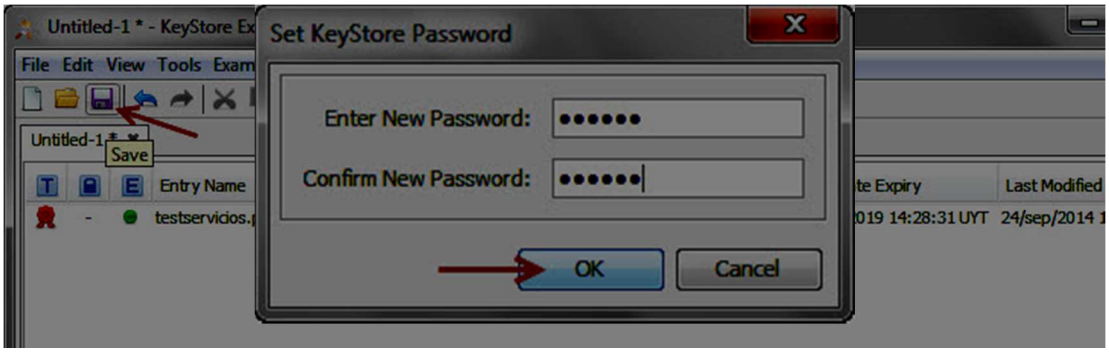


3. Seleccionar la clave pública de Plataforma (testservicios.pge.red.uy.cer en el caso de Testing, o servicios.pge.red.uy en el caso de Producción) y setear el alias del mismo dentro del almacén de certificados:


Certificate Details for File 'testservicios.pge.red.uy.cer'
Certificate Hierarchy:
testservicios.pge.red.uy
Version: 3
Subject: E=soporte@agesic.gub.uy,CN=testservicios.pge.red.uy,OU=Arq
Issuer: CN=HGTivoliCA
Serial Number: 0x247E09E1000300000219
Valid From: 28/mar/2014 17:33:15 UYT
Valid Until: 10/mar/2019 14:28:31 UYT
Public Key: RSA 1024 bits
Signature Algorithm: SHA1WITHRSA
Fingerprint: SHA-1 AC:21:4E:3A:3B:37:91:62:42:0C:A3:38:AD:05:D
Extensions
PEM
ASN.1
OK


Import Trusted Certificate
Do you want to accept the certificate as trusted?
Sí
No


Trusted Certificate Entry Alias
Enter Alias: testservicios.pge.red.uy
OK
Cancel



4. Guardar el almacén de certificados creado y ponerle en el nombre la extensión ".truststore" (ejemplo: agesicTesting.trustsotre"). Al guardar se solicitará setear una contraseña para el almacén:

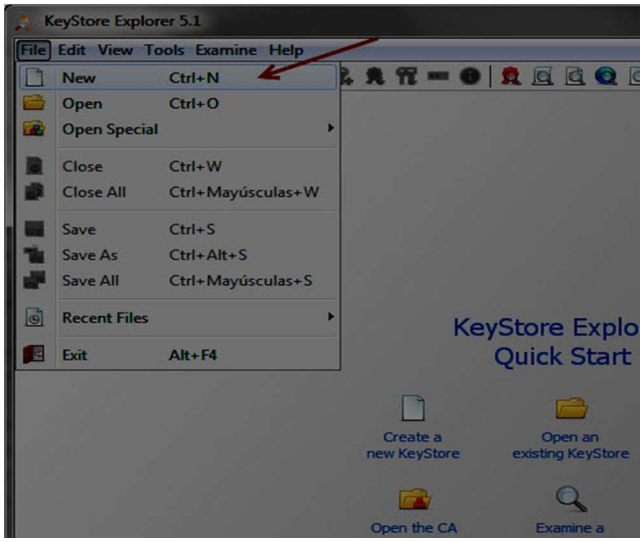
Obtención y configuración de certificados de persona jurídica

1.10 - Objetivo

En esta sección se describirá el proceso de configuración de los certificados digitales para que el cliente pueda identificarse como Persona Jurídica ante la PGE para poder realizar la invocación de servicios.

Como se explicó anteriormente, para esto se requerirá un certificado digital que identifique al cliente como una Persona Jurídica reconocida por el Estado, el cual deberá ser solicitado por el propio cliente a una autoridad certificadora reconocida por el Estado (por ejemplo El Correo).

Este documento no describe el proceso para solicitar un certificado digital dado que eso es específico a cada Autoridad Certificadora. El Correo por ejemplo,

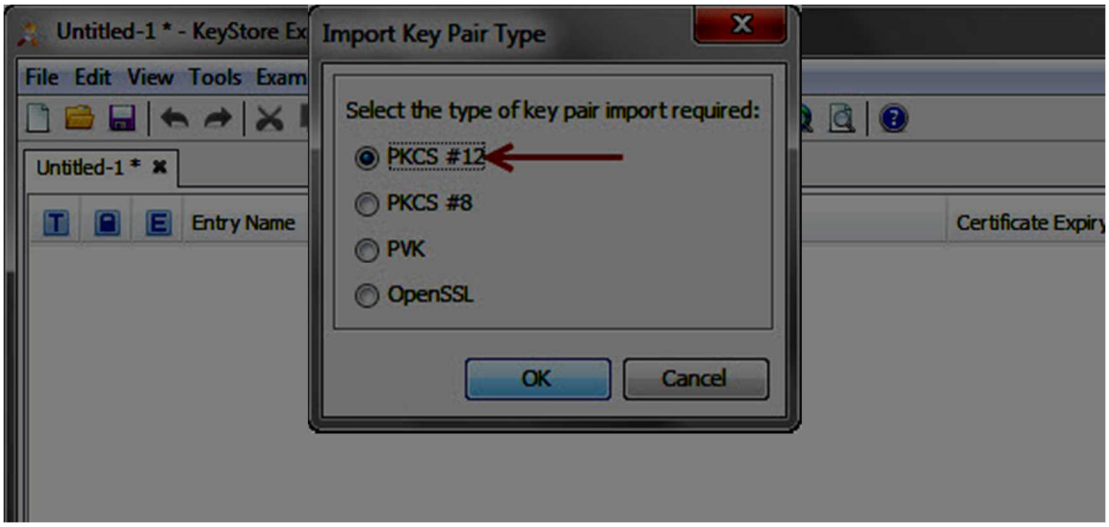


permite hacer esta solicitud a través de su sitio web (http://www.correo.com.uy) en la sección Servicios Electrónicos . En lo que sigue, se asume que ya se cuenta con el certificado firmado por una CA reconocida (típicamente, un archivo con extensión .pfx), y se conoce la contraseña del mismo. A continuación se detalla el procedimiento para importar el archivo .pfx en un almacén de claves (keystore).

1.11 - Importar PFX firmado por la CA en el almacén de claves

Al igual que para el caso de SSL, se utilizará la herramienta *Keystore Explorer.* A continuación se presentan los pasos necesarios para importar el PFX correspondiente al Certificado de Persona Jurídica:

1. Crear almacén de claves de tipo JKS:



2. Ejecutar la acción “Import Key Pair” y seleccionar el tipo PKCS #12:

3. Seleccionar el archivo .pfx recibido por la CA que emitió el certificado, junto con la password correspondiente del mismo:

4. Introducir el alias que tendrá el certificado dentro del almacén de claves, y luego configurar una nueva Password para el certificado:

5. Guardar el almacén de claves creado en un archivo con extensión ".keystore", por ejemplo, PruebaEmpresa.keystore. Luego setear la Password que tendrá el almacén de claves. **Es importante que la passwore sea exactamente la misma que la seteada en el paso anterior para el pfx.**