# Autenticación de Usuarios

## Aprovisionar Usuario

El aprovisionamiento del Usuario se realiza a través del sistema de Clientes utilizando el correo que proporciono el Cliente durante el proceso de compra.

El Flujo es el siguiente:

1. El sistema de Clientes solicita la creación del usuario en el sistema de Seguridad(Single Sign On) con el correo que proporciono el Cliente durante el proceso de compra.
2. El sistema de seguridad envía un correo al Usuario con una liga donde podrá definir su contraseña.



## Definición de Contraseña

El usuario utilizando la liga que se le envio por correo define su contraseña.

## Aprovisionar Token

El aprovisionamiento del Token se realiza a través del sistema de Clientes, enviando el token al correo que proporciono el Cliente durante el proceso de compra.

El Flujo es el siguiente:

1. El sistema de Clientes solicita la creación del Token en el sistema de seguridad.
2. El sistema de seguridad envía el Token vía correo electrónico.



## Registro de la Clave Publica de la FIEL y Certificado de Sello Digital

Para implementar el mecanismo de **no repudio de transacciones** es necesario registrar la Clave Pública de la FIEL y para poder sellar los documentos digitalmente es necesario registrar el Certificado de Sello Digital el flujo es el siguiente:

1. El usuario se autentica utilizando su usuario y contraseña
2. Selecciona la opción Registro de la Clave Publica de la FIEL y Certificado de Sello Digital.
3. El sistema le muestra la opción para que pueda capturar
   1. la ruta del archivo .cer del CFE.
   2. la ruta del archivo .cer del CSD
   3. la ruta del archivo .key del CSD
   4. la clave de acceso del CSD
4. El sistema genera una masterkey nueva
5. El sistema encripta la clave de acceso del CSD con la masterkey y almacena los archivos .cer, .key y la clave de acceso del CSD encriptada.
6. El sistema genera una sessionkey nueva
7. El sistema encripta la masterkey con la sessionkey y la almacena encriptada
8. El sistema encripta la sessionkey con la clave publica de la FIEL y la almacena encriptada.
9. El sistema guarda la clave publica de la FIEL.



## Autenticación

Para autenticar a los usuarios dentro del sistema se utilizara un mecanismo de usuario y contraseña, una vez autenticado se utilizara la FIEL para implementar el mecanismo de **no repudio de transacciones.**

El Flujo es el siguiente:

1. El usuario se autentica
2. El usuario solicita autenticar con la FIEL.
3. El sistema solicita la autorización utilizando la FIEL
   1. El sistema obtiene la sessionkey encriptada y la envía del lado del servidor(navegador)
   2. El usuario captura
      1. Clave privada de la FIEL
      2. Clave de acceso de la FIEL
   3. Dentro del navegador utilizando la clave privada y clave de acceso de la FIEL se desencripta y se envía de regreso al servidor
   4. El sistema con la sessionkey desencripta la masterkey
      1. El sistema genera una sessionkey nueva
      2. El sistema encripta la masterkey con la sessionkey nueva y la almacena en base de datos
      3. El sistema encripta la sessionkey con la clave publica de la FIEL y la almacena encriptada.
   5. El sistema con la masterkey desencripta la clave de acceso del CSD
   6. El sistema realiza la transacción
   7. El sistema mantiene la masterkey mientras dure la sesión



## Autenticación via token

Para autenticar a un sistema cliente se utilizara el token proporcionado, una vez autenticado se utilizara la FIEL para implementar el mecanismo de **no repudio de transacciones.**

El Flujo es el siguiente:

1. El sistema cliente se autentica utilizando el token que se le entrego en el aprovisionamiento
2. El sistema solicita autenticar con la FIEL
3. EL sistema solicita la autorización utilizando la FIEL
   1. El sistema obtiene la sessionkey encriptada y la envía al sistema cliente
   2. El sistema cliente usando la Clave Privada y Clave de acceso de la FIEL desencripta la sessionkey y la envía de regreso al servidor
   3. El sistema con la sessionkey desencripta la masterkey
   4. El sistema genera una sessionkey nueva
      1. La sessionkey nueva tendrá una vigencia, incluirá el RFC del Cliente
   5. El sistema encripta la masterkey con la sessionkey nueva y la almacena en base de datos
   6. El sistema envía el token para realizar transacciones al sistema cliente
      1. El token incluye la sessionkey
4. El sistema cliente envía una solicitud de transacción con el token incluido
5. El sistema con el token obtiene el sessionkey y desencripta la masterkey
6. El sistema con la masterkey desencripta la clave de acceso del CSD
7. El sistema realiza la transacción



## Glosario

FIEL: Firma Electronica

CFE: Certificado de Firma Electronica

CSD: Certificado de Sello Digital

.CER: Clave publica

.KEY: Clave privada

masterkey: Clave de acceso al CSD

Sistema Cliente: Sistema que se conecta via WebServices