INGENIERIA

SISTEMA INTEGRADOR DE RECURSOS EMPRESARIALES

Configuración APIKey V1.02

Manual de configuración

Contenido

[Introducción 3](#_Toc27743811)

[Crear las llaves pública y privada para el cliente 4](#_Toc27743812)

[Generar firma para el consumo de las interfaces 7](#_Toc27743813)

[Configuración de SIRESERVER y DBStart.ini 9](#_Toc27743814)

[Exportar información de la llave API 11](#_Toc27743815)

[Configuración de autentificación básica para acceder al web service 14](#_Toc27743816)

# Introducción

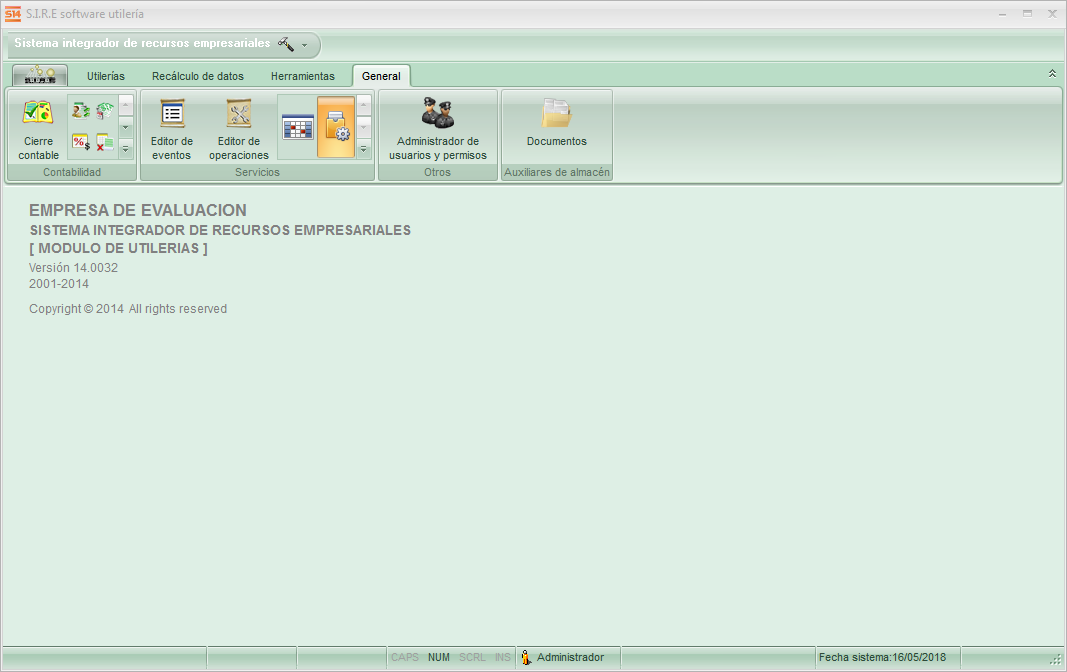
El presente documento tiene como finalidad explicar, de manera práctica como configurar o dar de alta un registro de APIKey o de usuario y password para conceder acceso a la interconexión entre sistemas o aplicaciones.

## Crear las llaves pública y privada para el cliente

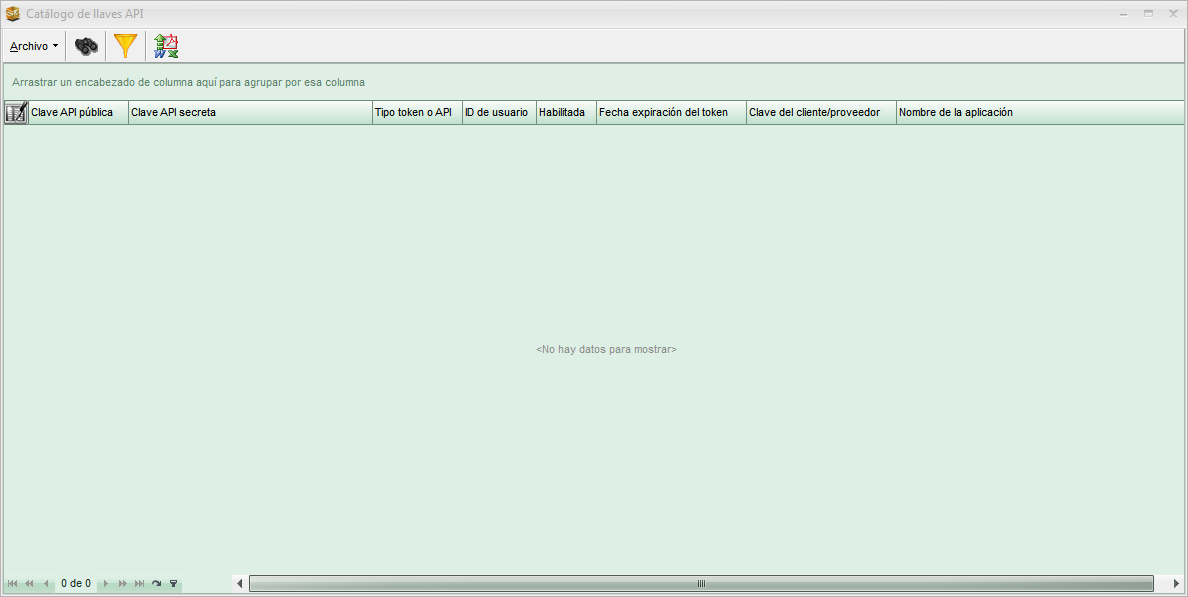
Para realizar el proceso de Interconexión entre la plataforma SIRE y el sistema interno, se deben generar dos llaves en la base de datos de la plataforma SIRE: una privada y una pública; esto con el fin de que el servidor pueda autentificar al sistema interno que envía la petición y saber si se encuentra registrado; si se encuentra registrado regresa la información solicitada, en caso contrario omite la petición. Esta funcionalidad se llama APIKey.

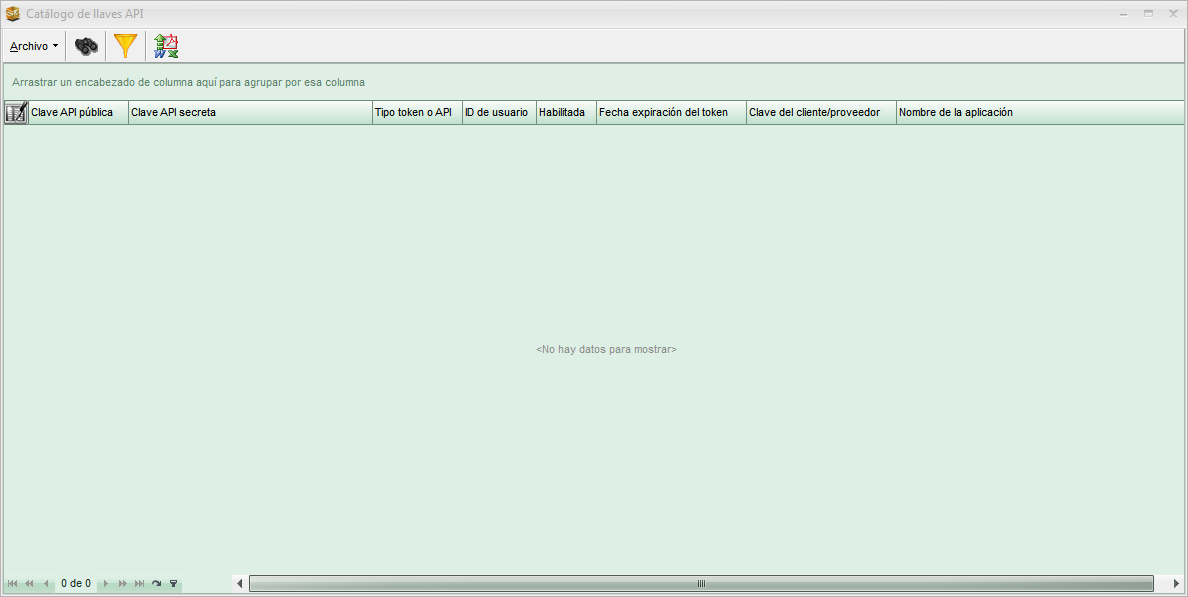
Para generar las APIKey’s de él o los sistemas a conectarse, se hará lo siguiente:

1. Se levantará la utilería de tres capas cliente y servidor, y en la pestaña “General” en la sección “Servicios”, se ejecutará la opción “Generar llaves API”.

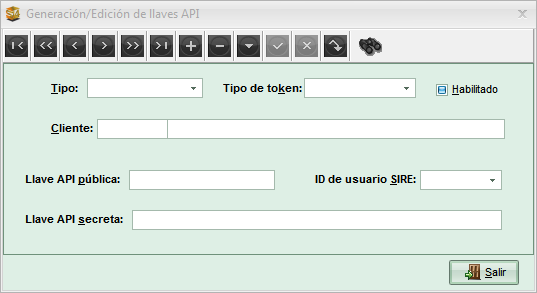


1. Aparecerá una pantalla con las ApiKey generadas anteriormente (en caso de que haya alguna registrada) y cada una está asociada a un cliente diferente. Para generar una nueva ApiKey se pulsará el botón “Edición”.





1. En la siguiente ventana que aparecerá están los campos necesarios para dar de alta una llave API, se pulsará el botón de “Insertar” para registrar una nueva llave.



1. Se llenarán los campos con la información correspondiente para generar la llave. En el campo *Tipo* se especifica que es para **Cliente**, en *Tipo de token* se selecciona la opción **Llave API**, en el campo cliente se **digita o busca la clave del cliente** que se registró en la segunda sección del manual y por último el *ID de usuario SIRE* que se utilizará para loguearse en el Servidor para realizar los pedidos o ventas que se realicen cuando se envíe una petición con la llave api que se está configurando, en este caso es el usuario Administrador con ID 1. Una vez capturada la información necesaria, se finaliza el registro de la llave.



1. Automáticamente, al guardar el registro se generan tanto la llave API pública como la llave API secreta (privada). Estas llaves se le brindan al cliente para que este se pueda autentificar en el servidor y pueda sincronizar el inventario.



A continuación se enlistarán los catálogos así como sus permisos correspondientes para poder realizar el proceso completo de SIRE vs SIRE:

* 1. **Catálogo de API Keys y Tokens:**
     1. Acceso.APIKeys: Acceso al catálogo de API keys y tokens.
     2. APIKeys.Insertar: Permiso para generar nuevas llaves API y tokens.
     3. APIKeys.Modificar: Permiso para modificar API keys y tokens
     4. APIKeys.Borrar: Permiso para borrar API keys y tokens
  2. **Catálogo de restricción de IP de APIKeys**
     1. Acceso.APIKeys\_FiltrosIP:
     2. APIKeys\_FiltrosIP.Insertar: Insertar un nuevo rango permitido de IP.
     3. APIKeys\_FiltrosIP.Modificar: Modificar el raqngo de IP’s.
     4. APIKeys\_FiltrosIP.Borrar: Borrar rango de IP’s.
  3. **Listado de métodos habilitados para el APIKey de SIRE**
     1. Acceso.B2BMetodos: Acceso aL listado de métodos habilitados para el APIKey de SIRE.
     2. B2BMetodos.Editar: Editar restricciones de API por método.

## Generar firma para el consumo de las interfaces

Para el uso de las interfaces que SIRE se encargó de realizar es necesario generar una firma la cual es necesario tomar en cuenta los datos que se generaron en el apartado anterior los cuales son: Llave API pública, Llave API secreta y el nombre del método que se va a utilizar.

A continuación, se muestra como se calcula la firma en código:

(El ejemplo del código es para Pascal)

Procedure TForm1.cxButton2Click(Sender: TObject);

var

fecha, HMAC: String;

begin

try

fecha:= FormatDateTime('yyyyMMddHHmmss', Now); // Se obtiene la fecha actual en formato año mes día hora minutos y segundos

fechaSolic.Text:= fecha; // Se asigna la fecha a componente para visualizarla

HMAC:= GeneraHMAC(Trim(ApiPublic.Text),Trim(ApiSecret.Text),fecha,Trim(Metodo.Text)); // Se consume el método para generar la firma

HMACBox.Text:= HMAC; // Se asigna la firma al componente para visualizarla

cxMemo1.Clear; // Se limpia el componente donde se visualizara el nodo con los datos de acceso

cxMemo1.Lines.Add('<Acceso>'); // Se genera el nodo de apertura para el nodo de acceso

cxMemo1.Lines.Add(' <ApiPublic>'+Trim(ApiPublic.Text)+'</ApiPublic>'); // Se agrega el nodo donde se asigna la apipublica

cxMemo1.Lines.Add(' <Firma>'+HMAC+'</Firma>'); // Se agrega el nodo donde se agrega la firma

cxMemo1.Lines.Add(' <Fecha>'+fecha+'</Fecha>'); // Se agrega el nodo para la fecha de la firma

cxMemo1.Lines.Add('</Acceso>'); // Se cierra el nodo de acceso

except on E:Exception do begin

ShowMessage(E.message);

end;

end;

end;

function TForm1.GeneraHMAC(Const ApiPublic, ApiSecret, FechaHoraSolicitud, MetodoRemoto: String): String;

var AHMAC: TIdBytes;

Sha1: TIdHashSHA1;

Cadena: String;

begin

Result:= ''; // Inicializa la variable Result

try

Cadena:= Trim(FechaHoraSolicitud)+Trim(MetodoRemoto)+Trim(ApiPublic); // Crea la cadena para firmar con la llave API

try

Sha1:= TIdHashSHA1.Create; // Inicializa objeto para encriptar

Cadena:= Sha1.HashStringAsHex(Cadena); // Se encripta la cadena

finally

Sha1.Free; // Libera objeto

end;

IdSSLOpenSSL.LoadOpenSSLLibrary; // Abre la libreria IdSSLOpenSSL

with TIdHMACSHA1.Create do // Con TIdHMACSHA1

try

Key:= IndyTextEncoding\_UTF8.GetBytes(ApiSecret); // Asigna el valor de la Llave API Secreta a Key

AHMAC:= HashValue(IndyTextEncoding\_UTF8.GetBytes(Cadena)); // Asina el valor de la cadena a encriptar a AHMAC

finally

free; // Libera el objeto

end;

Result := TIdEncoderMIME.EncodeBytes(AHMAC); // Codifica y asigna el valor del HMAC a la variable ApiKeyAux

except on e:Exception do // Regresa un error si es encontrado

Result:= e.Message; // Regresa un error si es encontrado

end;

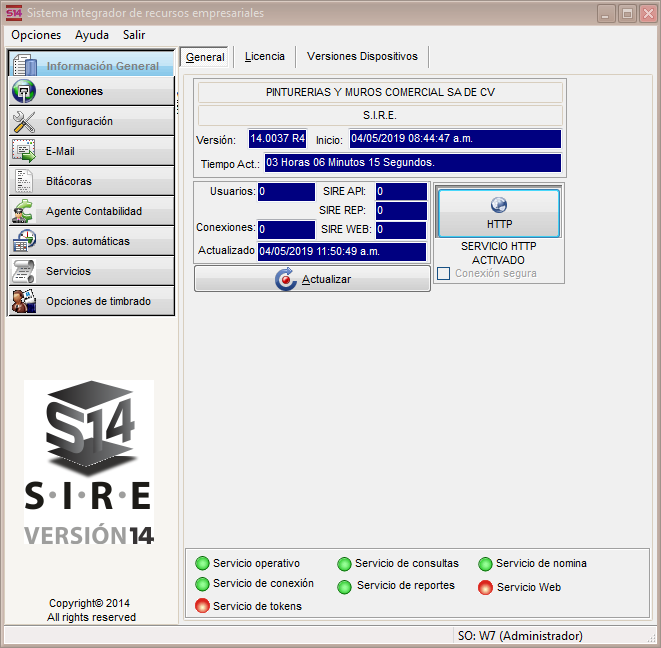
end;

La firma debe generarse por cada petición y no es posible reutilizarla, debe replicarse este algoritmo en el lenguaje de programación donde se realizarán las peticiones

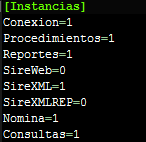
## Configuración de SIRESERVER y DBStart.ini

Para realizar las peticiones a los métodos para la consulta de catálogos que se ponen a disposición para ser consumido abra que realizar una configuración en el SIRESERVER para poder hace uso de estos la cual es la siguiente:

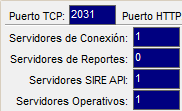
Activar el servicio de HTTP:



En el DBStart.ini tener activado el uso de XML en el apartado de [Instancias]:



***NOTA: Para realizar esta configuración debe ser necesario tener configuración en la llave física de SIRE Api en caso de no tener esta configuración, aunque se configure por dbstart no se crearán instancias para su atención en la sección correspondiente Servidores SIRE API y no se podrán realizar las peticiones correspondientes***

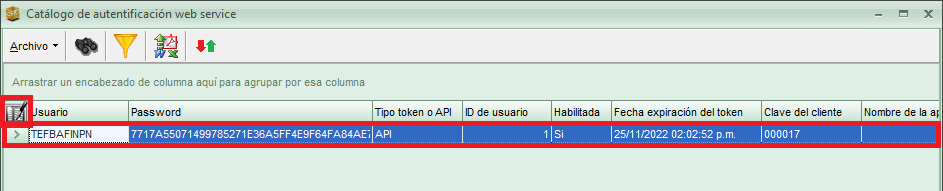


## Exportar información de la llave API

Se agregó la funcionalidad en el módulo de llaves API que permite exportar la información registrada de la llave API generada. Para acceder a esta funcionalidad se ejecutará el módulo de “Autentificación Webservice” que se encuentra en la pestaña GENERAL->SERVICIOS de la utilería de tres capas.



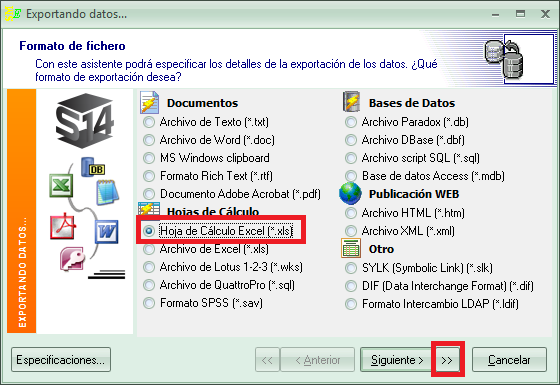
A continuación, se mostrará el listado de las llaves API que se hayan generado en la plataforma. Para exportar la información de una de ellas se seleccionará la llave API deseada y se dará clic en el botón “Edición” de la esquina superior izquierda del listado.



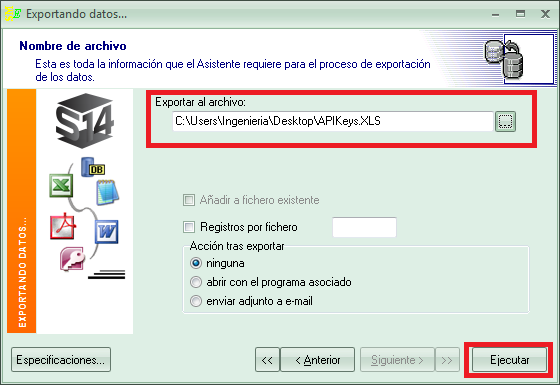
A continuación, se mostrará la ventana con la información desglosada de la llave API seleccionada en el listado. Para exportar dicha información se dará clic en el botón “Exportar datos” que se encuentra en la barra de navegación de la ventana.



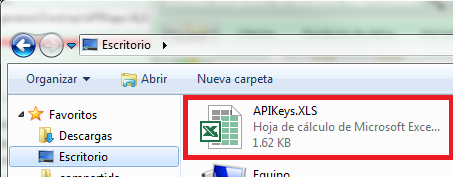
En la siguiente ventana se seleccionará el tipo de archivo al que se exportará la información de la llave API, y a continuación se dará clic en el botón “Ir al último paso”.



En la siguiente ventana se seleccionará la ruta y el nombre donde se guardará el archivo, para finalmente dar clic en “Ejecutar” para iniciar el proceso.



Por último, se tiene el archivo generado con la funcionalidad.



## Configuración de autentificación básica para acceder al web service

En el presente apartado se tiene la finalidad de instruir en el proceso de configuración para acceder por autentificación básica a los métodos de webservice.

A continuación, se indican los parámetros generales y su descripción para entender y elegir la configuración adecuada:

|  |  |  |
| --- | --- | --- |
| Página | Parámetro General | Descripción |
| 31.- Ctrl. de accesos | **Utiliza autenficiación básica por usuario y password en Web Service** | Este parámetro indica que todas las peticiones a los Web Service’s de la plataforma SIRE se autentificarán con un usuario y password enviado en la petición SOAP, de manera que cuando se active este parámetro no se validará la firma correspondiente al API Public y API Secret. |

Cuando se habilite este parámetro en la interfaz se modificará el nombre de la ventana por autentificación web service y los componentes correspondientes al API Key cambiarán a usuario y password.



Este usuario y password deberá ser compartido con los clientes que se conectarán al web service para que se envíen los datos en la petición como **“Autentificación básica” indicando el usuario y password ambos datos codificados usando base64**, en esta funcionalidad no se requiere enviar los nodos firma y fecha, correspondientes al nodo acceso de las peticiones, pero si el nodo ApiPublic como otro mecanismo de control de acceso por parte de los métodos.