INVOCACION DEL SERVICIO WEB DE INTEGRACION DE ESECURITY

CONFIGURACIÓN BASE DE DATOS ESECURITY

Aquí se describirán las firmas de las operaciones que ofrece el servicio Web de integración de la plataforma eSecurity.

Primero hacemos la actualización de la base de datos eSecurity para compatibilidad con estos Servicios ejecutando el siguiente comando:

```
-- Creación de la Tabla donde se almacenan los Token

CREATE TABLE [ApplicationUserByToken] (
  [Id] [int] IDENTITY (1, 1) NOT NULL ,
  [IdApplicationUser] [int] NOT NULL ,
  [Token] [varchar] (50) COLLATE Modern_Spanish_CI_AS NULL ,
  [CreateTime] [datetime] NULL ,
  [ExpiredTime] [datetime] NULL ,
  [Enabled] [varchar] (1) COLLATE Modern_Spanish_CI_AS NULL
 ) ON [PRIMARY]

-- Actualización de las entidades

 ALTER TABLE [ApplicationUserByToken] WITH NOCHECK ADD
 CONSTRAINT [PK_ApplicationUserByToken] PRIMARY KEY CLUSTERED
 (
  [Id]
 ) ON [PRIMARY]

-- Actualizacion de la configuración

ALTER TABLE [Settings] ADD [ExpiredToken] [int]
UPDATE [Settings] SET ExpiredToken = '600'
```

Nota: *Los token generados tiene vigencia en el tiempo, esta determinada por la información de la tabla* ***[settings]*** *en la columna* **`ExpiredToken`** `= 600` *la cual indica la duración máxima en segundo de un Token generado.*

DESCRIPCION DEL SERVICIO WEB

En segundo lugar, se describe el XML de retorno a la invocación del Servicio Web.

Hay 4 elementos esenciales para el XML, el elemento <operationResult>, <operationType>, <operationResponse>, <errorMessage> que describiremos a continuación.

- <operationResult> [Resultado de la operación]
  - True = Validación Correcta
  - False = Error en la validación

- <operationType> [Tipo de operación]
  Compuesta por los nodos
  - Code = Código de operación en eSecurity [1 – Entrar al sistema]
  - Name = Nombre del método ejecutado [UserLogin]

- <operationResponse> [Contiene el resultado de la operación]
  Compuesta por los nodos

  - UserInfo = Información básica del usuario
    Compuesta por los nodos
    - Id = Identificador único del usuario
    - Code = Login
    - Name = Nombre
    - DaysToExpiration= Días restantes de vigencia
    - Identification= Identificación
    - LastLogin= Ultimo ingreso a los sistemas
    - PositionName= Cargo
    - eMail= Correo electrónico
    - Password = Contraseña
    - Enabled= Estado [Activo o Inactivo]

  - UserGroups = Grupos en lo que se encuentra asociado
    Compuesta por los nodos
    - Id = Identificador único del grupo
    - Code = Código del grupo
    - Name = Nombre

  - UserCompanies= Empresas en las que se encuentra asociado
    Compuesta por los nodos
    - Id = Identificador único de la empresa
    - Code = Código de la empresa
    - Name = Nombre

  - UserModules= Módulos en los que se encuentra asociado
    Compuesta por los nodos
    - Id = Identificador único del modulo
    - Code = Código del modulo

        - `Name` = Nombre

- `<errorMessage>` [Mensajes de error]
  `Compuesta por los nodos`
    - `Code` = Código de operación en eSecurity [1 – Entrar al sistema]
    - `Message` = Descripción del suceso

Cuando el valor de `<operationResult>` es igual a `False` indica que el ***Token*** no cumplió con una validación y la descripción del mensaje se adjunta en el `message` del nodo.

CREACIÓN AUTOMATICA DEL TOKEN

En tercer lugar, ejecutamos la página de Login de ejemplo, donde nos retorna la información del Usuario como se muestra a continuación.

```
Dim AuthenticationMode As String = "2"
Dim oUser As Gattaca.Entity.eSecurity.ApplicationUserEntity

oUser = oSecurity.UserLogin(AppCredentials, Usr, Pwd, AuthenticationMode)
```

En la Entidad ***oUser***, se retorna la información del usuario, para obtener el ***token*** generado basta con solo llamarlo de la siguiente forma:

```
Dim UserToken As String = oUser.Token
```

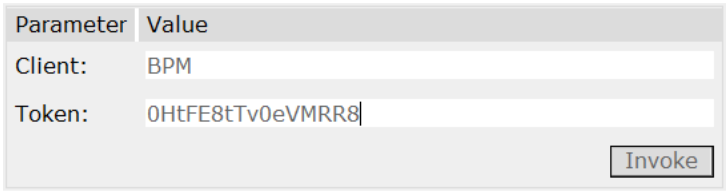
Nota: *La invocación del método **UserLogin** genera automáticamente el **Token** compuesto por 16 caracteres aleatorios alfanuméricos en la base de datos.*

Id	IdApplicationUser	Token	CreateTime	ExpiredTime	Enabled
1	1	0HtFE8tTv0eVMRR8	16/12/2009 03:16:18 p.m.	16/12/2009 03:26:18 p.m.	T

CONSUMO DEL SERVICIO WEB

En cuarta instancia, para consumir el servicio ingresamos a la URL: ***http://<dominio>/eSecurity/Services/SecurityServices.asmx*** donde obtenemos la siguiente pantalla.

Ejecutamos la función ***GetUserInfoByToken,*** pasándole como parámetros el ***Cliente*** [Nombre con el cual se realizó la licencia] y ***Token*** [Llave generada al momento de loguearse]



Al invocar el servicio, obtenemos la respuesta que veremos en el siguiente apartado.

Nota: *Una vez consumido el servició, el* ***token*** *queda deshabilitado automáticamente.*

RESPUESTA DEL SERVICIO WEB DE RESULTADO TRUE

Si el resultado de la operación es **True** se genera el siguiente XML:

```
<?xml version="1.0" encoding="utf-8"?>
<response>
    <operationResult>True</operationResult>
    <operationType>
        <code>1</code>
        <name>GetUserInfoByToken</name>
    </operationType>
    <operationResponse>
        <UserInfo>
            <Id>1</Id>
            <Code>administrator</Code>
            <Name>Alejandro Chaparro</Name>
            <DaysToExpiration>9453</DaysToExpiration>
            <Identification>80459000</Identification>
            <LastLogin>16/12/2009 03:16:19 p.m.</LastLogin>
            <PositionName>Administrador General</PositionName>
            <eMail>test@e-gattaca.com</eMail>
            <Password>XXXXXXXXXX</Password>
            <Enabled>T</Enabled>
        </UserInfo>
        <UserGroups>
            <Group Id="1" Code="ADMIN">
                <Id>1</Id>
                <Code>ADMIN</Code>
                <Name>Administradores Generales</Name>
            </Group>
            <Group Id="4" Code="UProcesosI">
                <Id>4</Id>
                <Code>UProcesosI</Code>
                <Name>Usuarios de Procesos</Name>
            </Group>
            <Group Id="7" Code="UStartProcess">
                <Id>7</Id>
                <Code>UStartProcess</Code>
                <Name>Grupo de Procesos Internos</Name>
            </Group>
        </UserGroups>
        <UserCompanies>
            <Company Id="2" Code="">
                <Id>2</Id>
                <Code></Code>
                <Name>Empresa</Name>
            </Company>
        </UserCompanies>
        <UserModules>
            <Module Id="1" Code="ESECURITY">
                <Id>1</Id>
                <Code>ESECURITY</Code>
                <Name>Security Manager</Name>
            </Module>
            <Module Id="7" Code="WORKFLOW">
                <Id>7</Id>
```

```
                <Code>WORKFLOW</Code>
                <Name>WorkFlow</Name>
            </Module>
            <Module Id="8" Code="FORMBUILDER">
                <Id>8</Id>
                <Code>FORMBUILDER</Code>
                <Name>FormBuilder</Name>
            </Module>
        </UserModules>
    </operationResponse>
    <errorMessage>
        <code></code>
        <message></message>
    </errorMessage>
</response>
```

RESPUESTA DEL SERVICIO WEB DE RESULTADO FALSE

Cuando el ***token*** ingresado y o la ***licencia*** no pasan la validación, el resultado de la operación es **`False`** y se genera el siguiente XML indicando el motivo del rechazo:

```
<?xml version="1.0" encoding="utf-8"?> <response>
    <operationResult>False</operationResult>
    <operationType>
        <code>1</code>
        <name>UserLogin</name>
    </operationType>
    <operationResponse/>
    <errorMessage>
        <code>Token expirado el 2009-12-16 15:26:18</code>
        <message>Token expirado el 2009-12-16 15:26:18</message>
    </errorMessage>
</response>
```

POSIBLES MENSAJES DE RESULTADO FALSE

- Token no habilitado
- Token expirado el 2009-12-16 15:26:18
- Su usuario ha sido deshabilitado o su contraseña se ha vencido.
- Su usuario se encuentra activo desde otro sitio.
- Su dirección IP y/o Usuario ha sido bloqueada por intentos fallidos de acceso.