Especificación del servicio de Consulta Alternativa de Interdictos (CAI-REST)

Versión 1.3

Marzo de 2013

Contenido

1 Objetivos

El Real Decreto 1613/2011, de 14 de noviembre, por el que se desarrolla la Ley 13/2011, de 27 de mayo, regulación del juego, en lo relativo a los requisitos técnicos de las actividades de juego, establece que los operadores de juego deben verificar la identidad y edad de los participantes así como consultar, en tiempo real, el Registro General de Interdicciones de Acceso al Juego (RGIAJ) para la activación de las cuentas de juego.

Además, la DGOJ facilita a cada operador los cambios que se hayan podido producir en el RGIAJ cada hora, al objeto de que pueda incorporarlos a su base de datos de clientes y realizar las comprobaciones necesarias antes del pago de los premios.

La DGOJ facilita mediante servicios web dicho servicio, así como el servicio de verificación de identidad del participante.

En este último caso, en caso de caídas de los sistemas de la DGOJ o de los Servicios de Intermediación de la Secretaría de Estado para Administraciones Públicas o de la Dirección General de la Policía que presta en último término el servicio de verificación de identidad, la normativa de juego permite demorar dicha identificación durante tres días, si bien las normas técnicas recomiendan el reintento en 30 minutos.

Sin embargo, y atendiendo a los apartados Undécimo y Doudécimo de la Resolución de 12 de julio de 2012, de la Dirección General de Ordenación del Juego, por la que se aprueba la disposición que desarrolla los artículos 26 y 27 del Real Decreto 1613/2011, de 14 de noviembre, en relación con la identificación de los participantes en los juegos y el control de las prohibiciones subjetivas a la participación, la comprobación en RGIAJ debe hacerse en tiempo real.

Por ello, y al objeto de no perjudicar los intereses de los operadores y el derecho de los participantes a tomar parte en actividades de juego, se precisa un sistema de consulta alternativo de interdicciones de acceso al juego (CAI) que complemente a los servicios web facilitados por la DGOJ. En caso de caída de estos sistemas, se puede seguir manteniendo al menos la verificación del estado del participante en el RGIAJ, dentro del Plan de Contingencias establecido para esta circunstancia.

Este sistema de Consulta Alternativa de Interdicciones se activará por la DGOJ en el caso de una caída prolongada de sus sistemas mediante el procedimiento indicado en el punto 3.4.

Es necesario recalcar que dado que el sistema principal de la DGOJ estará caído cuando se active el servicio de CAIREST, no se podrá producir ningún cambio respecto del estado RGIAJ de los usuarios por los que anteriormente había preguntado el operador. Ello implica que, al no existir cambios de estado RGIAJ, la última información descargada en la operación VerificarCambiosRGIAJ será válida durante todo el tiempo en el que servicio de CAIREST esté activo. Por lo tanto, únicamente se debería utilizar el servicio de CAIREST en la comprobación de estado RGIAJ de aquellos usuarios que nunca antes fueron comprobados por el operador en cuestión.

Por otra parte, recordar, que el sistema de verificación de identidad, al ser un servicio de uso opcional por parte de los operadores y dado que la legislación permite a la DGOJ poder diferir hasta en tres días las peticiones de identificación recibidas, no tendrá un servicio alternativo de consulta en el caso de caída grave de los sistemas de la DGOJ. Cuando ello suceda, los operadores podrán activar los servicios de verificación documental de identidad que estimen oportunos.

2 Control de cambios del documento

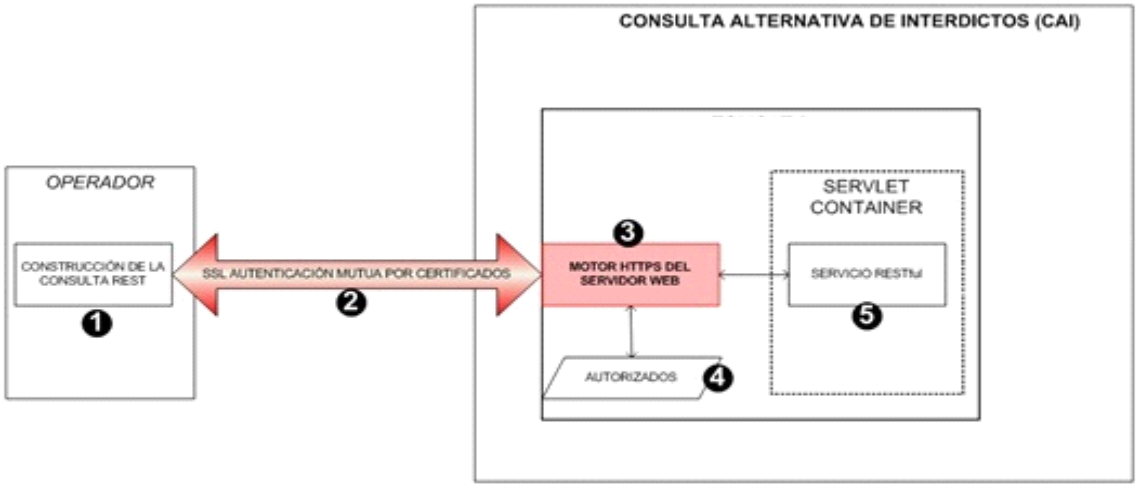
Versión	Fecha	Descripción
0.1	SEP 2012	Versión inicial.
0.2	OCT 2012	Corrección de errores. Donde se indica algoritmo de cifrado HMAC MD5 debe decir HMAC SHA1
0.3	ENE 2013	Aclaración sobre el uso de certificados y suministro del fichero de claves en el periodo de pruebas.
1.0	FEB 2013	Activación del entorno de pruebas del CAIREST
1.1	FEB 2ª 2013	Detalle de los DNI's/NIE's a consultar cuando el servicio CAIREST está activo (punto 4.5) Acciones a realizar una vez recuperado el servicio convencional RGIAJ tras la activación del RGIAJ (punto 4.6)

1.2	MARZ 2013	Información sobre cuando se debe utilizar el servicio CAIREST (punto 1) Los DNIs/NIEs utilizados en el proceso de cifrado deben tener siempre 9 caracteres, por lo que será necesario completar con 0 hasta conseguir esa número de caracteres (punto 4.3)
1.3	MARZ 2ª 2013	Los DNIs/NIEs utilizados en el proceso de cifrado deben tener los caracteres no numéricos en mayúsculas (punto 4.3)

3 Especificación funcional

El sistema ofrece un servicio de consulta del fichero General de Interdicciones de Acceso al Juego mantenido por la DGOJ para informar a los operadores del estado (status) de los jugadores cuando estos se registran en los sistemas de juego on line.

3.1 Descripción del sistema



3.2 Conexión segura

- El operador se conectará mediante canal SSL. Todos los accesos serán auditados por parte de la DGOJ.

- Las peticiones deben utilizar el canal SSL (HTTPS) de forma que deben construirse con el certificado del operador para que el servidor Web establezca correctamente la comunicación; el servidor a su vez también se identifica con un certificado. Los operadores deberán utilizar el mismo certificado (dependiente del entorno) que utilizan para conectarse al servicio de verificación de jugadores

3.3 Peticiones de consulta

- Establecida la conexión, el operador debe construir una petición para el recurso; esta petición es simplemente una petición GET al recurso con protocolo HTTPS, es decir una petición similar a la siguiente:

  https://cairest.dgojuego.es/CAIREST/rest/getStatus?id=DDDOTivMPqI9dchUNKFtyJH6lEU=

  El valor de id es la representación BASE64 del resultado de aplicar el algoritmo de composición de la clave de búsqueda que se construye con un HASH mediante un algoritmo HMAC SHA1 con contraseña. http://en.wikipedia.org/wiki/HMAC.

- El servidor web dirige la petición al motor de servlets (al no estarse solicitando un recurso estático). Este servlet usará JAX-RS y la implementación de referencia (Jersey) de RESTful services.

3.4 Respuestas del servicio de Consulta Alternativa de Interdictos (CAI-REST).

El servicio recibe la clave de búsqueda construida por el operador, comprueba la identidad el operador y si el operador es válido realiza la búsqueda en el fichero de interdicciones. Construye una respuesta en formato JSON. Las posibles respuestas del sistema son las siguientes:

Código de respuesta	Significado
{"Code":"COD001"}	El usuario está inscrito en el RGIAJ
{"Code":"COD002"}	El usuario no está inscrito en el RGIAJ
{"Code":"ERR001"}	Error técnico (error interno)
{"Code":"ERR002"}	Operador no autorizado
{"Code":"COD006"}	La petición no tiene certificado

3.5 Descripción del formato del fichero XML de clave

La clave se facilitará en un fichero xml con la siguiente estructura:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
 <key>
 <value>06tVCeX2RAFnwHBfucBvNQY4cI1UJZc/DxwqI2XoG++oViOSEabLUwY/HwyT5
qrSvVxY2SquiyDMekqBTIt4Gg==</value>
 </key>
```

Tiene como elemento root el elemento key, con un elemento value cuyo valor indica la key que se ha utilizado para generar el cifrado HMAC SHA1.

4 Anexos

4.1 Alta en el servicio.

Todos los operadores que hayan solicitado el alta a los web services de producción tendrán acceso al servicio CAI-REST.

Previamente a poder utilizar el servicio deberán enviar un correo a dgoj.soporteoperadores@minhap.es indicando en el asunto del mensaje ALTA-CAI-REST.

El correo de solicitud de alta deberá proceder de la cuenta de correo del operador a donde este desee recibir la notificación de la activación del Plan de Contingencia. Preferiblemente debe tratarse de una cuenta de correo específica para esta función y no una cuenta personal.

En el caso de activación del Plan, la DGOJ enviará a dicha cuenta de correo la notificación de activación del mismo y un fichero adjunto con la clave de cifrado para el HASH.

En el correo de respuesta se comunicará la clave a utilizar en ambos entornos. En el entorno de preproducción la clave no variará. En el entorno de producción la clave se modificará cuando se active la contingencia real, comunicando la nueva clave a través de un correo electrónico enviado a la dirección notificada en la solicitud de alta.

4.2 Descripción de los entornos

Existen dos entornos para acceder al servicio de CAIREST:

- preproducción: invocación a través de la URL https://cairest.dgojuego.es:1443/CAIREST/rest/getStatus?id=DDDOTivMPqI9dchUNKFtyJH6lEU=
- producción: invocación a través de la URL https://cairest.dgojuego.es/CAIREST/rest/getStatus?id=DDDOTivMPqI9dchUNKFtyJH6lEU=

En el entorno de preproducción se podrá operar utilizando aquellos certificados comunicados a la DGOJ para interoperar con el entorno de preproducción de verificación de jugadores.

En el entorno de producción se podrá operar utilizando aquellos certificados comunicados a la DGOJ para interoperar con el entorno de producción de verificación de jugadores.

Mientras no esté activado el plan de contingencia se podrá preguntar por los siguientes DNI's/NIE's en ambos entornos. El sistema deberá responder con COD0001

00000034B
00000048W
X0000019L
00000024R
00000057B
X0000052Y
00000001R

NOTA: al realizar las comprobaciones de presencia en RGIAJ a partir de un hash del DNI/NIE, es importante recalcar que:

- observar que los documentos utilizados vienen determinados por un identificador de 9 caracteres, rellenando con ceros a la izquierda hasta completar ese número
- observar que los caracteres no numéricos se utilizan en formato mayúsculas, ya que la operación de cálculo de hash da un resultado distinto para el DNI

Las dos condiciones anteriores son debidas a que el resultado del cálculo de un hash es distinto para cada uno de los casos siguientes, siendo solo válido el primer ejemplo de cada bloque

- 00000034B
- 00000034b
- 034B
- 034B

- X0000052Y
- X0000052y
- x0000052Y
- X52Y

El fichero con la clave para calcular el hash indicado en el apartado 3.5 será facilitada por la DGOJ durante el periodo de pruebas.

Una vez activado el plan de contingencias, el entorno de producción responderá a peticiones reales de los operadores teniendo en cuenta el estado real de los mismos en la base de datos RGIAJ. Cuando se

desactive el plan, se volverán a cargar los datos de prueba en el entorno de producción.

4.3 Cálculo del hash de un DNI/NIE

El DNI/NIE del participante a consultar se cifrará mediante un algoritmo de cifrado HMAC SHA1 con clave. Esta clave se facilitará en un fichero xml adjunto en el correo en que se comunica la activación del Plan de Contingencia.

El DNI/NIE deberá contar siempre con 9 caracteres, teniendo que completar con tantos 0 a la izquierda como sean necesarios para alcanzar esa cifra.

Los caracteres no numéricos utilizados en el DNI/NIE deberán estar siempre en mayúsculas.

4.4 Activación del Plan de Contingencia

Cuando no sea posible la verificación del estado de los jugadores en el RGIAJ a través de los servicios web durante un plazo prolongado debido a problemas técnicos, la DGOJ activará el plan de contingencia para permitir la consulta alternativa al fichero de Interdictos (CAI). Para ello levantará los servicios correspondientes en el servidor de emergencia en el entorno de producción, subirá los identificadores Hash de todos los inscritos en RGIAJ hasta la hora anterior y comunicará a los operadores mediante correo electrónico la activación del servicio y la clave de cifrado de los identificadores (DNI/NIE). Este Plan no se activará en el caso de que los servicios web permitan la consulta del estado en el RGIAJ, aunque no funcione la consulta de verificación de identidad.

4.5 Funcionamiento con el Plan de Contingencia activado

Cuando el servicio CAIREST está activo, sólo se deberán consultar aquellos DNI's/NIE's por los que con anterioridad a la activación del servicio CAIREST nunca se haya consultado el estado RGIAJ (servicios de consulta de estado RGIAJ convencionales).

Aquellos DNI's/NIE's por los que se preguntó previamente su estado RGIAJ no habrán variado su estado su estado, siendo válida la información obtenida en el momento de la consulta, así como las correspondientes actualizaciones disponibles a través de la operación VerificarCambiosRGIAJ.

4.6 Desactivación del Plan de Contingencia

Una vez recuperada la posibilidad de consulta del RGIAJ a través de los servicios web, la DGOJ comunicará por correo electrónico la desactivación del mismo, procediendo a deshabilitar la consulta de datos reales a través del sistema de contingencia.

Para asegurar que aquellos DNI's/NIE's que fueron consultados a través del servicio de CAIREST pasan a ser incorporados al sistema de información de la DGOJ de forma que sean considerados en el mecanismo de alerta de los cambios de estado en RGIAJ (operación VerificarCambiosRGIAJ de los servicios web convencionales), es necesario que los operadores, una vez el servicio convencional se ha recuperado, vuelvan a preguntar por el estado de RGIAJ de todos aquellos DNI's/NIE's por los que preguntaron cuando el servicio de CAIREST estuvo activo. De no hacerlo, posibles cambios de estado de esos clientes (y en especial aquellos que proporcionaron una respuesta negativa de presencia en RGIAJ (COD002) no serán tenidos en cuenta en el proceso VerificarCambiosRGIAJ).

4.7 Simulacros del Plan de Contingencia

La DGOJ realizará con la periodicidad que se estime en su plan de seguridad un simulacro de activación del Plan de Contingencia que incluirá la activación de este servicio, así como cualquier otro procedimiento que se puedan incorporar en el futuro. Dicha activación no afectará al servicio convencional de consulta RGIAJ o de identidad, afectando únicamente al servicio de contingencia. Se trata pues de responder con datos reales a través de este sistema. Los operadores serán avisados del inicio y fin del simulacro con el fin de que puedan probar sus sistemas.

4.8 Ejemplo para utilización del servicio CAIREST

El desarrollo del cliente para consultar el servicio CAI es responsabilidad de los operadores de juego.

No obstante, la DGOJ facilita un API, con sus dependencias, para que el operador desarrolle un cliente en tecnología java disponible en http://www.ordenacionjuego.es/es/servicio-web-verificacion-jugadores sección Consulta Alternativa al Registro General de Interdicciones de Acceso al Juego.

La DGOJ no da soporte sobre dicho software ni asume ninguna responsabilidad sobre el funcionamiento del mismo. Así mismo no se proporcionará soporte sobre el contenido del mismo ni se tiene la responsabilidad de solucionar los problemas que se puedan detectar en su funcionamiento.

Este cliente está diseñado para ser integrado dentro de un desarrollo en Java.

El jar proporcionado (API) provee de funcionalidad, tanto para codificar el id buscado en hmac, como para realizar la llamada SSL al servicio de CAIREST.

Debemos colocar el jar proporcionado en el CLASSPATH de la aplicación.

Para realizar la conversión a formato HMAC realizamos los siguientes pasos.

Se importa la clase HmacUtils

```
import com.dgoj.crypto.utils.HmacUtils;
```

Realizamos una invocación al método estático HmacUtils.generateHMAC con los parámetros adecuados.

```
HmacUtils.generateHMAC(idToConvert, new FileInputStream(keyFilePath));
```

O

```
HmacUtils.generateHMAC(idToConvert, key);
```

A continuación se describen los parámetros:

idToConvert: Se trata de un String cuyo valor es el id que queremos convertir a formato HMAC.

keyFilePath: Se trata de un String cuyo valor es el path del fichero que contiene la key(proporcionado por la DGOJ).

o

key: Se trata de un String cuyo valor es la clave secreta para generar el HMAC.

Para realizar la llamada al servicio REST se realiza de la siguiente manera.

Se importan las clases CAIRESTService y ConnectionParameters.

```
import com.dgoj.toolkit.net.CAIRESTService;
import com.dgoj.toolkit.params.ConnectionParameters;
```

Creamos una instancia de dichas clase e invocamos el método searchRestService con los parámetros adecuados.

```
ConnectionParameters conParams = new ConnectionParameters(restHost, restHostSSLPort, hmacId, keyStorePath, keyStorePass, trustStorePath, trustStorePass);

CAIRESTService caiService = new CAIRESTService();
String caiResponse = caiService.searchRestService(conParams);
```

A continuación describimos los parámetros.

restHost: Dirección (ip o nombre DNS) del servidor donde está instalada la aplicación Web CAIREST.

restHostSSLPort: Puerto SSL habilitado en el servidor 443 (producción) o 1443 (preproducción).

hmacId: Identificador a buscar en el fichero de interdicciones, este debe ir en formato HMAC SHA1.

keyStorePath: Ruta del keyStore.

keyStorePass: Password del keyStore.

trustStorePath: Ruta del trustStore.

trustStorePass: Password del trustStore

4.9 Requisitos.

Es necesario disponer de un certificado para el cliente dentro de un almacén de claves de tipo JKS.

Es necesario disponer de un almacén de certificados de confianza de tipo JKS, en el que guardaremos la parte pública del certificado del servidor o el certificado de la CA que lo firmo.

4.10 Ejemplos.

Ejemplo llamada a un cliente que utiliza la API. (disponible en http://www.ordenacionjuego.es/es/servicio-web-verificacion-jugadores sección Consulta Alternativa al Registro General de Interdicciones de Acceso al Juego)

Produccion.

java -jar ClienteCairest.jar cairest.dgojuego.es 443 00000015S Mikeystore.jks miclavekeystore MItrustore.jks miclavetrustore key.xml

Preproduccion.

java -jar ClienteCairest.jar cairest.dgojuego.es 1443 00000015S Mikeystore.jks miclavekeystore MItrustore.jks miclavetrustore key.xml

Ejemplo codigo fuente de utilizacion de la API.

```
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import javax.xml.bind.JAXBException;
import com.dgoj.crypto.utils.HmacUtils;
import com.dgoj.toolkit.error.SSLUtilsError;
import com.dgoj.toolkit.net.CAIRESTService;
import com.dgoj.toolkit.params.ConnectionParameters;
public class Main  {
public static void main(String[] args) throws SSLUtilsError, FileNotFoundException, JAXBException {
        String restHost = args[0];
        int restHostSSLPort = Integer.valueOf(args[1]).intValue();
        String idToSearch = args[2];
        String keyStorePath = args[3];
        String keyStorePass = args[4];
```

```
        String trustStorePath = args[5];
        String trustStorePass = args[6];
        String keyFilePath = args[7];
        String hmacId = HmacUtils.generateHMAC(idToSearch, new FileInputStream(keyFilePath));
        System.out.println(hmacId);
        ConnectionParameters conParams = new ConnectionParameters(restHost, restHostSSLPort, hmacId, keyStorePath, keyStorePass, trustStorePath, trustStorePass);
        CAIRESTService caiService = new CAIRESTService();
        String caiResponse = caiService.searchRestService(conParams);
        System.out.println(caiResponse);
    }
```

4.11 Dependencias

Las librerías a incorporar al proyecto son las siguientes

- log4j-1.2.16.jar
- commons-codec-1.6.jar
- commons-logging-1.1.1.jar
- httpclient-4.2.jar
- httpcore-4.2.jar

Estas librerías pueden ser obtenidas por el operador a través de Internet o descargarlas de un fichero .zip facilitado por la DGOJ en http://www.ordenacionjuego.es/es/servicio-web-verificacion-jugadores sección Consulta Alternativa al Registro General de Interdicciones de Acceso al Juego