Specifications of the Alternative Ban Check service (CAI-REST)

Version 1.3

March 2013

Content

1 Objectives 3
2 Monitoring changes in the document 4
3 Functional specifications 6
3.1 Description of the system 6
3.2 Secure connection 7
3.3 Consultation requests 7
3.4 Responses of the Alternative Ban Check service (CAI-REST). 7
3.5 Description of the format of the XML key file 8
4 Appendices 9
4.1 Registration for the service. 9
4.2 Description of the environments 9
4.3 Calculation of the hash of a DNI/NIE 11
4.4 Activation of the Contingency Plan 11
4.5 Functioning with the Contingency Plan activated 11
4.6 Deactivation of the Contingency Plan 12
4.7 Contingency Plan drills 12
4.8 Example use of the CAIREST service 12
4.9 Requirements. 14
A certificate must be available for the client in a JKS type keystore. 14
4.10 Examples. 14
4.11 Dependencies 17

1 Objectives

Royal Decree 1613/2011, of 14 November, implementing Law 13/2011 of 27 May on the regulation of gaming, regarding the technical requirements of gaming activities, establishes that gaming operators must verify the identity and age of participants and consult, in real time, the General Register of Gaming Access Bans (RGIAJ) when activating gaming accounts.

Also, the DGOJ will provide operators with a list of changes to the RGIAJ once an hour, which they can add to their client database and use for running the necessary checks before paying out prizes.

The DGOJ will provide this service online as a web service, as well as the participant identity verification service.

In this latter case, if there should be a failure in the systems of the DGOJ, the Intermediary Services of the Secretary of State for Public Administrations or the Directorate General of the Police, which ultimately provides the identity verification service, the gaming regulations allow this identification to be delayed for three days, although the technical regulations recommend trying again after 30 minutes.

However, and in accordance with sections 11 and 12 of the Directorate General for the Regulation of Gambling's Resolution of 12 July 2012, approving the provision implementing Articles 26 and 27 of Royal Decree 1613/2011 of 14 November, regarding the identification of participants in games and monitoring individual gambling bans, the RGIAJ check must be in real time.

Thus, in order not to prejudice the interests of the operators and the right of participants to take part in gaming activities, an alternative system is needed for checking gambling bans (CAI) which complements the web services provided by the DGOJ. If there should be a failure of this system, at least the verification of the participant's RGIAJ status can be maintained, as part of the Contingency Plan established for these circumstances.

This Alternative Ban Check system will be activated by the DGOJ in the case of a prolonged failure of its systems, using the procedure indicated in point 3.4.

It must be stressed that as the main DGOJ system will be down when the CAIREST service is activated, no changes can be made to the users' RGIAJ status which the operator had been consulting. This means that, as there are no changes to RGIAJ status, the latest information downloaded in the VerifyChangesRGIAJ operation will be valid throughout the time the CAIREST service is active. Thus, the CAIREST service should be used only to check the RGIAJ status of users who have never previously been checked by the operator in question.

Also, it should be remembered that the identity verification system, being an optional service offered to the operators, and given that the legislation permits the DGOJ to delay its response to identification requests by up to three days, no alternative service can be consulted in the case of a serious failure of the DGOJ's systems. When this happens, the operators may activate the documentary identity verification services they deem advisable.

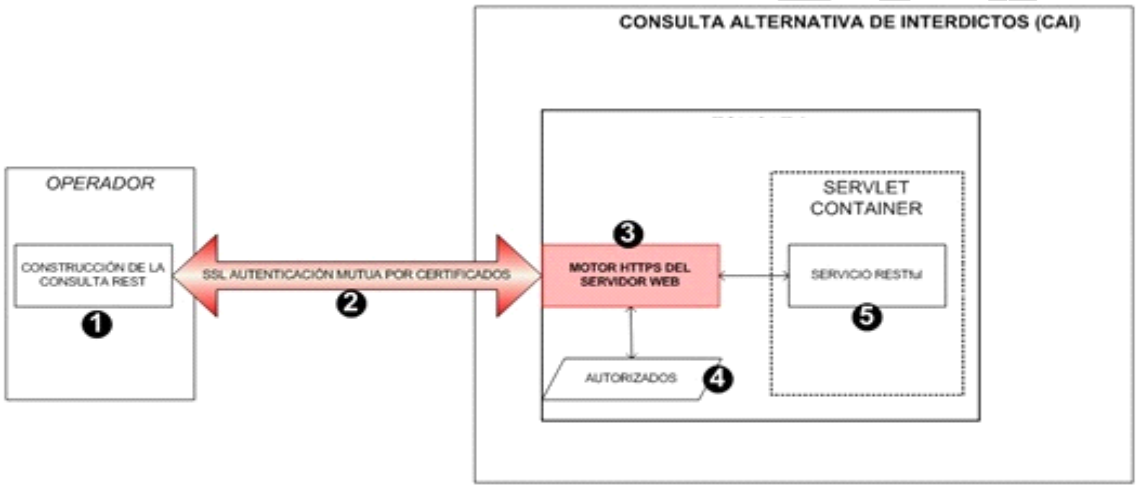
2 Monitoring changes in the document

Version	Date	Description
0.1	SEP 2012	Initial version.
0.2	OCT 2012	Errata. Where the encryption algorithm is given as HMAC MD5 this should read HMAC SHA1
0.3	JAN 2013	Clarification on the use of certificates and the supply of the key file in the testing period.
1.0	FEB 2013	Activation of the CAIREST test environment
1.1	FEB.2 2013	List of the DNI/NIE numbers to be consulted when the CAIREST service is active (point 4.5) Actions to be taken after the recovery of the conventional RGIAJ service (point 4.6)
1.2	MAR 2013	Information on when the CAIREST service should be used (point 1) The DNI/NIE numbers used in the encryption process must always have 9 characters, and must be completed with 0 to reach that number of characters (point 4.3)
1.3	MAR.2 2013	The DNI/NIE numbers used in the encryption process must have non-numerical characters in upper case (point 4.3)

3 Functional specifications

The system offers a lookup service using the General Gaming Ban file kept by the DGOJ to inform operators of the status of players who register in online gaming systems.

3.1 Description of the system



Operator	
CONSTRUCTION OF THE REST CHECK	
MUTUAL SSL CERTIFICATE AUTHENTICATION	
ALTERNATIVE BAN CHECK (CAI)	
HTTPS WEB SERVER ENGINE	
SERVLET CONTAINER	
REST SERVICE	
AUTHORISED	

3.2 Secure connection

- The operator will connect via SSL channel. All access will be audited by the DGOJ.

- Requests must use the SSL channel (HTTPS), which must be constructed with the operator's certificate so that the web server can establish communications correctly; in turn, the server is identified with a certificate. Operators must use the same certificate (depending on the environment) that they use to connect to the player verification service.

3.3 Consultation requests

- When the connection is established, the operator must construct a request for the resource; this request is simply a GET request for the resource with an HTTPS protocol, similar to this one:

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

  The ID value is the BASE64 representation of the result of applying the composition algorithm of the hashed search key generated using an HMAC SHA1 algorithm with password. http://en.wikipedia.org/wiki/HMAC.

- The web server sends the request to the servlets engine (if it is not requesting a static resource). This servlet will use JAX-RS and the reference implementation (Jersey) of RESTful services.

3.4 Responses of the Alternative Ban Check service (CAI-REST).

The service receives the search key generated by the operator, checks the identity of the operator, and if the operator is valid, searches the ban file. It constructs a response in JSON format. The possible responses of the system are as follows:

{"Code":"COD001"}	The user is registered with the RGIAJ
{"Code":"COD002"}	The user is not registered with the RGIAJ
{"Code":"ERR001"}	Technical error (internal error)
{"Code":"ERR002"}	Operator not authorised
{"Code":"COD006"}	The request is not certified

3.5 Description of the format of the XML key file

The key will be supplied in an XML file with the following structure:

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

The root element is the key element, with a value element indicating the key used to generate the HMAC SHA1 encryption.

4 Appendices

4.1 Registration for the service.

All the operators who have requested registration for production web services will have access to the CAI-REST service.

Before they can use the service they must email dgoj.soporteoperadores@minhap.es with ALTA-CAI-REST in the subject line.

The email requesting registration must come from the operator's email account where it wants to receive notification of the activation of the Contingency Plan. Preferably, this will be a specific email address for this purpose, and not a personal account.

If the Plan is activated, the DGOJ will send an email to this address with the notification of activation and an attached file with the encryption key for the HASH.

The reply email will include the key to be used in both environments. In the preproduction environment the key will not change. In the production environment the key will be changed when the real contingency is activated, and the new key will be sent by email to the address given in the registration request.

4.2 Description of the environments

There are two environments for accessing the CAIREST service:

- preproduction: invocation via the URL https://cairest.dgojuego.es:1443/CAIREST/rest/getStatus?id=DDDOTivMPqI9dchUNKFtyJH6lEU=
- production: invocation via the URL https://cairest.dgojuego.es/CAIREST/rest/getStatus?id=DDDOTivMPqI9dchUNKFtyJH6lEU=

Operation is possible in the preproduction environment using the certificates sent to the DGOJ for interoperating with the preproduction player verification environment.

Operation is possible in the production environment using the certificates sent to the DGOJ for interoperating with the production player verification environment.

While the contingency plan is not activated, the following DNI/NIE numbers can be asked about in both environments. The system should respond with COD0001

00000034B
00000048W
X0000019L
00000024R
00000057B
x0000052Y
00000001R

NOTE: When the RGIAJ inclusion checks are run based on a hash of the DNI/NIE, it is important to:

- make sure that the documents used are determined by an identifier of 9 characters, adding zeros to the left until the number is reached.
- make sure that non-numerical characters are in upper case, as the hash calculation operation gives a different result for the DNI

Both the above conditions are needed because the result of a hash calculation is different for each of the following cases, with only the first example in each block being valid.

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

- x0000052Y
- x0000052Y
- x0000052Y
- X52Y

The file with the key for calculating the hash indicated in section 3.5 will be provided by the DGOJ during the test period.

Once the contingency plan is activated, the production environment will respond to the real requests of the operators, taking into account their real status in the RGIAJ database. When the plan is deactivated, the test data will be loaded in the production environment again.

4.3 Calculation of the hash of a DNI/NIE

The DNI/NIE of the participant to be checked will be encrypted using a HMAC SHA1 encryption algorithm with key. This key will be provided in an XML file attached to the email reporting the activation of the Contingency Plan.

The DNI/NIE must always have 9 characters, and must be completed with as many 0s to the left as needed to reach that number.

Non-numerical characters used in the DNI/NIE must always be in upper case.

4.4 Activation of the Contingency Plan

When the RGIAJ status of the players cannot be checked using the web services for a long period due to technical problems, the DGOJ will activate the contingency plan to allow checking with the alternative ban file (CAI). To do this it will enable the corresponding services on the emergency server in the production environment, upload the Hash identifiers of everyone registered with the RGIAJ up to the last hour, and inform the operators by email that the service is activated, giving them the encryption key of the identifiers (DNI/NIE). This Plan will not be activated if the web services allow the status to be checked at the RGIAJ, even if the identity check is not working.

4.5 Functioning with the Contingency Plan activated

When the CAIREST service is active, RGIAJ status checks should be run only on DNI/NIE numbers which have never been checked in the conventional RGIAJ status checks before the CAIREST activation.

The DNI/NIE numbers whose RGIAJ status has already been checked will not have changed status, and the information obtained at the time of checking will be valid, as will the updates available via the operation VerifyChangesRGIAJ.

4.6 Deactivation of the Contingency Plan

Once it is again possible to consult the RGIAJ using the web services, the DGOJ will send emails reporting the deactivation of the plan and disable the real data checks through the contingency system.

To ensure that the DNI/NIE numbers which were checked using the CAIREST service are added to the DGOJ's computer system and are included in the mechanism reporting changes in RGIAJ status (operation VerifyChangesRGIAJ in the conventional web services), once the conventional service has been recovered the operators must request the RGIAJ status of all the DNI/NIE numbers they requested while the CAIREST service was active. If not, any changes in the status of these clients (especially those who gave a negative RGIAJ presence (COD002) will not be taken into account in the process VerifyChangesRGIAJ).

4.7 Contingency Plan drills

The DGOJ will run drills, as often as stated in its security plan, in which the Contingency Plan is activated, including the activation of this service and any other procedure which might be added in the future. This activation will not affect the conventional RGIAJ or identity checking services, and affect the contingency service only. The drills will respond with real data through this system. Operators will be advised at the start and end of the drill so that they can test their systems.

4.8 Example use of the CAIREST service

Gaming operators are responsible for developing a client for checking the CAI service.

However, the DGOJ will provide an API with dependencies so that operators can develop a client using Java technology, available at http://www.ordenacionjuego.es/es/servicio-web-verificacion-jugadores in the section Alternative Gambling Ban Check.

The DGOJ will not provide support for the software or accept any liability for its functioning. No support will be provided for its content and no responsibility will be taken for solving any problems in its functioning.

This client is designed to be integrated in a Java development.

The Jar provided (API) supplies functionality for coding the ID in HMAC or making SSL calls to the CAIREST service.

The Jar provided must be placed in the CLASSPATH of the application.

To convert it to HMAC format follow these steps.

Import the class HmacUtils

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

Invoke the static method HmacUtils.generateHMAC with the correct parameters.

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

O

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

The parameters are described below:

idToConvert: This is a String, the value of which is the ID we want to convert to HMAC format.

keyFilePath: This is a String, the value of which is the path of the file containing the key (provided by the DGOJ).

o

key: This is a String, the value of which is the secret key for generating the HMAC.

To call the REST service proceed as follows.

Import the classes CAIRESTService and ConnectionParameters.

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

Create an instance of these classes and invoke the searchRestService method with the correct parameters.

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


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

The parameters are described below:

restHost: Address (IP or DNS name) of the server where the CAIREST application is installed.

restHostSSLPort: SSL Port enabled in server 443 (production) or 1443 (preproduction).

hmacId: Identifier to find in the ban file. This must be in HMAC SHA1 format.

keyStorePath: keyStore path.

keyStorePass: keyStore password.

trustStorePath: trustStore path.

trustStorePass: trustStore password

4.9 Requirements.

A certificate must be available for the client in a JKS type keystore.

A store of JKS type trust certificates will be necessary, where we will store the public part of the server certificate or the certificate of the CA that signed it.

4.10 Examples.

Example calling a client using the API. (available at http://www.ordenacionjuego.es/es/servicio-web-verificacion-jugadores in the section Alternative Gambling Ban Check)

Production.

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

Preproduction.

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

Example source code for using the 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 Dependencies

The libraries to be incorporated in the project are as follows:

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

These libraries can be obtained by the operator on the Internet or downloaded in a .zip file provided by the DGOJ at http://www.ordenacionjuego.es/es/servicio-web-verificacion-jugadores in the section Alternative Gambling Ban Check