

PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS PER A LA PRESTACIÓ D'UN SERVEI DE PAGAMENT DE PREMIS DE LOTERIA DE CATALUNYA A TRAVÉS DE LA XARXA D'OFICINES DEL CONTRACTISTA. (exp. V0950-ECO-25-0003)

1. CONCRECIÓ DE L'OBJECTE DE LA CONTRACTACIÓ

Realitzar el pagament dels premis dels jocs comercialitzats per Loteries de Catalunya, SAU (en endavant LCAT), a través de les oficines del contractista interconnectant telemàticament el Sistema de LCAT, operat actualment per Pollard Digital Solutions GmbH (d'ara endavant PDS), amb un node central del contractista per tal de permetre les operacions bàsiques de validació i pagament de premis de bitllets de loteria.

2. CARACTERÍSTIQUES DEL SERVEI

2.1 Pagament de premis.

El contractista assumeix l'obligació de pagament de premis en els termes previstos per Loteries de Catalunya, SAU.

La Resolució ECO/1851/2021, d'11 de juny, determina els llocs de pagament de premis de les loteries de la Generalitat i preveu, en el seu apartat 1.c), que poden pagar premis les *“Entitats financeres concertades, que paguen els premis d'un import superior a cent vint (120) euros i fins a cent cinquanta mil euros (150.000), llevat de la Grossa (loteria passiva) en què paguen premis de quantia igual o superior a cinquanta euros (50)”*.

2.2 Forma de pagament dels premis.

El contractista seguirà el següent protocol:

- a) La persona beneficiària presentarà el bitllet premiat a les oficines del contractista.
- b) El contractista remetrà de forma telemàtica a LCAT les dades del bitllet acordades en el flux del Web Service creat a tal efecte entre LCAT i el contractista.
- c) LCAT autoritzarà el pagament del premi a través de la mateixa via que en el punt anterior.
- e) El contractista realitzarà l'abonament del premi a la persona beneficiària en efectiu (amb les limitacions d'import que fixi la legislació vigent en cada moment) o mitjançant abonament en compte o transferència bancària.

2.3. Informació sobre nous sistemes de pagament.

El contractista informará a LCAT de les novetats en els sistemes de pagament que sorgeixin durant l'execució del contracte.

3. CARACTERÍSTIQUES TÈCNIQUES DEL SERVEI

3.1 Tecnologia d'Interconnexió.

LCAT exposarà i allotjarà el servei per fer la comprovació i pagament de tiquets premiats de loteria. El contractista desenvoluparà l'aplicació client per fer la crida a aquests serveis.

La interconnexió es realitza en base a un interfase dinàmica basada en les següents especificacions tècniques:

- Web Service SOAP
- SOAP Versió 1.2
- Descripció Interfase mitjançant WSDL
- Protocol HTTPS
- Autenticació SSL en dues direccions (Two-Way SSL authentication)

Veure el Punt 3.6 per més detalls tècnics en la part de seguretat.

3.2. Arquitectura de Connexió al Sistema.

La connexió telemàtica es realitzarà de forma centralitzada des de un sol punt de la xarxa del contractista.

3.3. Operacions Publicades al Interfase.

Les úniques operacions publicades a la interfase són aquelles que han de permetre als operadors de El contractista la validació del premi i el posterior pagament.

A continuació es resumeix els dos missatges que es defineixen:

- Consulta de Premis

Camp	Descripció
Petició	
Entitat - Sucursal	Codis per identificar la sucursal que realitza la petició
Id. Resguard	Identificador del resguard de loteria per localitzar el bitllet premiat al sistema. (veure Punt 3.4)
Resposta Satisfactòria	
Imports Premi	L'import brut del premi més el detall de tots els imports necessaris segons la fiscalització del premi.
Id Fiscal	Indicador de si es necessària la identificació de beneficiaris a efectes fiscals
Respost Errònia	
Codi – Desc. Error	Codi + descripció del error en la consulta del premi.

- Pagament de Premis

Camp	Descripció
Petició	

Id Transacció	Identificador únic de la transacció generat per la entitat bancaria
Entitat - Sucursal	Codis per identificar la sucursal que realitza la petició
Id. Resguard	Identificador del resguard de loteria per localitzar el bitllet premiat al sistema. (veure Punt 3.4)
Resposta Satisfactòria	
Imports Premi	L'import brut del premi més el detall de tots els imports necessaris segons la fiscalització del premi.
Id Fiscal	Indicador de si es necessària la identificació de beneficiaris a efectes fiscals
Respost Errònia	
Codi – Desc. Error	Codi + descripció del error en pagament del premi.

3.4. Identificació Resguards Loteria - Codis de Barres.

Els bitllets de loteria i les participacions de la loteria col·lectiva permeten la seva identificació de forma inequívoca al sistema mitjançant els uns codis de barres.

Segons els tipus de jocs aquest codis de barres poden ser de diversos tipus:

- Jocs Online

Tipus Codi Barres	EAN 128 Alfanumèric
Longitud	23
Jocs als quals aplica	La 6/49 El Trio L'Express Loteria passiva (La Grossa electrònic)

- Jocs Passius Pre-Impressos

Tipus Codi Barres	EAN 128 Alfanumèric
Longitud	27
Jocs als que aplica	Loteria passiva (La Grossa)

- Jocs de Loteria instantània

Tipus Codi Barres	Standard-128 Numèric
Longitud	27
Jocs als que aplica	El Rasca Ràpid

3.5. Interfases de Conciliació.

Adicionalment existiran 2 mecanismes de conciliació diàries entre el contractista i LCAT.

1) Conciliació Banc – Fitxer Premis Autoritzats

LCAT generarà un fitxer a diari amb la relació de premis autoritzats a pagar a l'entitat bancaria.

El fitxer serà enviat al contractista per la seva conciliació i auditoria pròpia.

Format:

- Text pla
- Registre capçalera
- Registre totals
- Longitud fixe dels camps (Total 168 posicions)

2) Conciliació Loteria – Fitxer Comptes de Pagament

El contractista haurà de reportar diàriament un fitxer amb la relació de moviments en el compte de pagament de LCAT.

Format:

- Fitxer que s'ajusta a la norma bancaria 43 en la seva Modalitat 3ª
- Longitud dels registres de 80 posicions

3.6. Segurització de la comunicació

Aquest punt descriu les mesures a prendre en quant a segurització de la comunicació entre els sistemes de LCAT i els del contractista, per tal de dur a terme el pagament de premis.

▪ **Segurització SSL de la comunicació en dues direccions entre LCAT i el contractista.**

Les dues parts implicades desenvoluparan l'aplicació fent ús de SOAP (Simple Object Access Protocol). SOAP és un protocol de missatgeria que permet a les aplicacions en diverses plataformes per a la comunicació mitjançant l'intercanvi de missatges XML. Es farà ús de la versió 1.2 del protocol SOAP.

Per a l'autenticació de LCAT a través del banc es farà ús del protocol HTTPS amb certificats SSL. El certificat SSL assegura autenticació del servidor (actualment NGL SOAP) amb el que el banc es comunica. El certificat SSL fixa un domini a una clau pública. El protocol HTTPS assegura l'encriptació bidireccional dels missatges SOAP XML entre el banc client i el servidor de LCAT.

L'ús del certificat SSL garanteix que el banc client s'està comunicant únicament amb el servidor de LCAT que el banc pretenia comunicar-se i no amb una entitat impostora.

El protocol HTTPS encripta la comunicació i assegura que els continguts dels missatges de comunicació XML entre el banc client i el servidor NGL SOAP no poder ser llegits o falsificats per cap altra part.

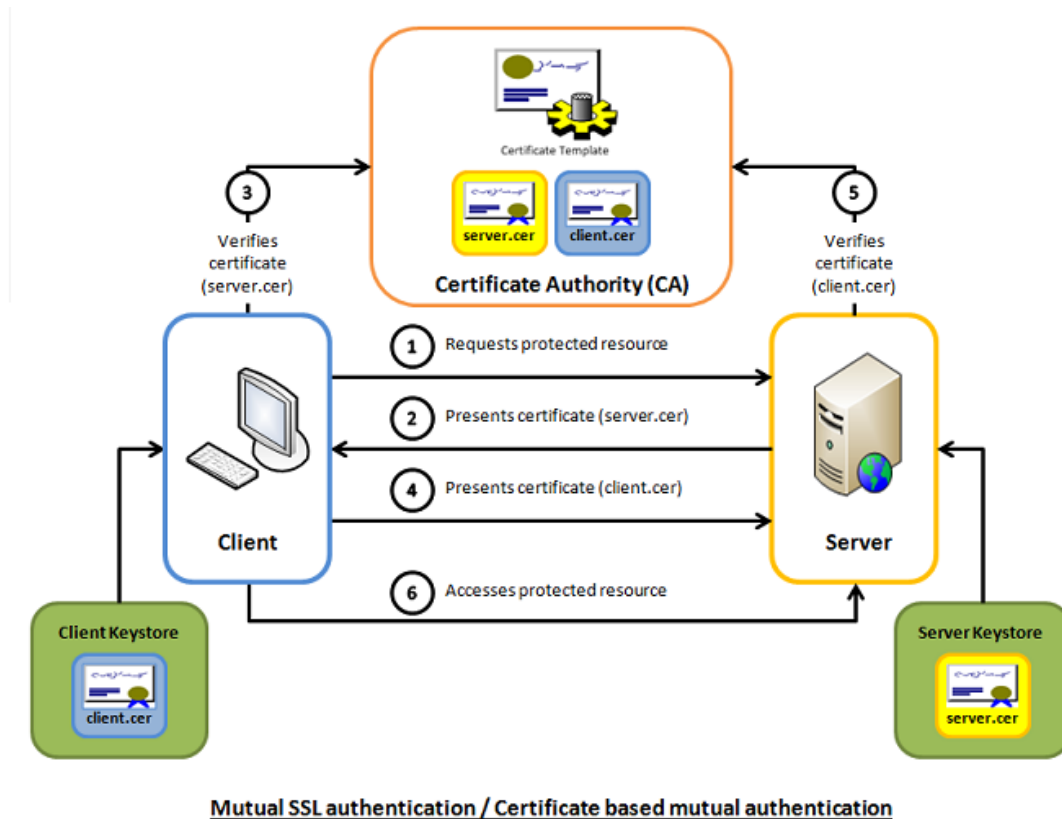
Per tal d'habilitar el protocol HTTPS en el servidor SOAP, LCAT (directament o mitjançant una empresa contractista) comprarà un certificat SSL vàlid signat per una autoritat certificada (CA). Els certificats són elements d'una infraestructura PKI que associen noms de domini (les entitats) amb una clau pública concreta, per tant, garantint la identitat del propietari de la clau pública.

Per tal d'autenticar la petició del banc amb la resposta XML dels missatges de LCAT, es consideren les dues mesures següents:

1) Autenticació SSL en dues direccions (two-way SSL authentication)

L'autenticació SSL en dues direccions o certificat basat en autenticació de client, fa referència

a dues parts autenticant-se una a l'altra mitjançant la verificació del certificat del proveïdor de manera que les dues parts s'asseguren de l'identitat de l'altra part. Així doncs, l'autenticació SSL en dues direccions no només verifica l'identitat del servidor, sinó que el servidor també verifica l'identitat del client. En aquest cas, LCAT o l'empresa contractista que gestioni aquest servei serà l'autoritat certificadora (CA) a qui el banc client entregarà peticions de certificats signats (CSR) pels sistemes de test i producció. LCAT o l'empresa contractista que gestioni aquest servei signarà certificats de client i acceptarà crides al servei desde el banc únicament quan es s'enviïn certificats de client correctes.



2) Creació de llistes d'adreces IP, des de les que els missatges del banc s'enviaran.

PDS mantindrà el llistat de les IPs dels sistemes de tests i producció des de les que el pagament de premis serà possible. Aquesta mesura de seguretat addicional estarà en vigor en el improbable cas que un atacant s'apoderi de la clau privada del banc.

A la data de la signatura electrònica de la cap de l'Àrea Econòmica i Financera, amb el vistiplau del director