PFC SEGURETAT

Sistema de joc electrònic remot de BlackJack amb seguretat similar a la dels casinos tradicionals

Estudiant: **Josep Lluís Ribas Gracia**
Titulació: **Enginyeria Informàtica**
Consultor: **Jordi Castellà Roca**

Data: **2 de Gener de 2006**

Dedicatòria i agraïments

Dedico el projecte a tota la meva família i amics, especialment a Made, per haver-me acompanyat durant tot el semestre en el desenvolupament del projecte, i haver estat comprensius en la meu aïllament per enllestir-lo.

Agraeixo l'ajuda aportada per el consultor Jordi Castellà en el curs del semestre.

Resum

L'objectiu d'aquest PFC és dissenyar, i implementar, un sistema de joc electrònic de BlackJack remot, que ofereixi als jugadors un nivell de seguretat similar al que es pot tenir quan juguem en un casino tradicional.

Per aconseguir-ho hem de garantir una sèrie de propietats, que en el cas dels jocs de cartes descobertes són:

- La unicitat de les cartes durant el joc. No hi poden haver duplicats.
- La distribució uniforme de les cartes barrejades
- La detecció de jugadors deshonestos.
- L'absència d'una tercera part de confiança.

Durant una partida de es produeixen apostes, que cal garantir amb:

- Autenticitat. S'ha de poder demostrar quin jugador l'ha realitzada.
- Integritat. No es poden manipular un cop realitzades.
- No-repudi. Ni jugador ni gestor poden repudiar les apostes un cop fetes.
- Seqüència de Joc. Una aposta ha d'incloure: la partida, l'instant de temps, la quantitat apostada, i el concepte.

Per a dur a terme tots aquests objectius farem ús de les següents eines:

- Java. Llenguatge de programació multi-plataforma.

- Eclipse. Editor de Java.

- MagicDraw. Eina de diagrames UML, que utilitzarem per representar el disseny dels programes.

- PKI i IAIK. Utilitzarem una infrastructura de clau pública (PKI) per implementar els esquemes criptogràfics necessaris. La biblioteca de Java IAIK, implementa els algorismes que necessitem.

- XML i JDOM. Utilitzarem XML per representar les dades que s'envien els jugadors i el gestor del casino. Utilitzarem la biblioteca JDOM per manipular XML amb Java.

- RMI. Amb el sistema RMI podrem implementar la comunicació entre el programa dels jugadors i el del gestor.

- MySQL.Amb aquest gestor gestionarem les dades que necessiten persistència.

Paraules clau.

BlackJack
Certificat
Compromís
Criptografia
Eclipse
IAIK
Java
JDOM
MySQL
PKI
RMI
Seguretat
SQL
UML
XML

Àrea

Aquest projecte s'emmarca en l'àrea de Seguretat.

Índex de continguts

Índex de figures

Capítol 1. Introducció.

Justificació del PFC.

Els sistemes de joc que hi ha actualment a la xarxa Internet, tenen una gran mancança en quant a seguretat es refereix, aportant solament el xifrat de la comunicació entre els jugadors i els casinos.

En aquest projecte desenvolupem un sistema que s'aproxima en quant a seguretat als casinos "físics". Per tant, la feina feta és d'aplicació immediata en aquests sistemes de joc.

Context en el qual es desenvolupa: punt de partida i aportació del PFC.

Aquest projecte es realitza com a projecte final de carrera d'Enginyeria Informàtica a la Universitat Oberta de Catalunya, el primer semestre del curs 2005-2006.

Aporta el disseny i implementació de nivells de seguretat similars als d'un casino real, en els casinos "online".

Objectius del PFC.

L'objectiu d'aquest PFC és dissenyar, i implementar, un sistema de joc electrònic de BlackJack remot, que ofereixi als jugadors un nivell de seguretat similar al que es pot tenir quan juguem en un casino tradicional.

Enfocament i mètode seguit.

S'ha dividit el projecte en diferents fases que s'han executat una darrera l'altre, de forma que es fa una implementació incremental:

1. Instal·lació IAIK i PKI.
2. Esquema criptogràfic.
3. Representació de dades: XML.
4. Comunicació dels components: RMI.
5. Gestió de la informació: BD.
6. Interfície del jugador.
7. Interfície del gestor del Joc.
8. Documentació.

Planificació del projecte.

Instal·lar IAIK							PAC1
PKI	openssl					setmana 1	
	objectiu	disseny	Implementació	test	documentació		PAC 2
Protocol compromís	criptografia					setmana 2	
Protocol d'autenticació							
Protocol inici de partida							
Protocol increment dipòsit							
Protocol fer una aposta							
Protocol de joc						setmana 5	
	objectiu	disseny	Implementació	test	documentació		PAC 3
Protocol compromís	XML					setmana 6	
Protocol d'autenticació							
Protocol inici de partida							
Protocol increment dipòsit							
Protocol fer una aposta							
Protocol de joc						setmana 7	
	objectiu	disseny	Implementació	test	documentació		PAC 4
Servidor RMI	RMI					setmana 8	
Client base RMI							
Protocol compromís							
Protocol d'autenticació							
Protocol inici de partida							
Protocol increment dipòsit							
Protocol fer una aposta							
Protocol de joc						setmana 9	
	objectiu	disseny	Implementació	test	documentació		PAC 5
BD servidor	model					setmana 10	
Registre jugador						setmana 11	
	objectiu	disseny	Implementació	test	documentació		PAC 6
Vista jugador	aplicatiu jugador					setmana 12 setmana 13	
	objectiu	disseny	Implementació	test	documentació		PAC 7
Vista gestor	aplicatiu gestor					setmana 14 setmana 15	
	objectiu			test	documentació		PAC 8
Documentacio	conclusions					setmana 16	

Calendari.

Setmana	dilluns	dimarts	dimecres	dijous	divendres	dissabte	diumenge	
1			14	15	16	17	18	setembre
2	19	20	21	22	23	24	25	
3	26	27	28	29	30	1	2	octubre
4	3	4	5	6	7	8	9	
5	10	11	12	13	14	15	16	
6	17	18	19	20	21	22	23	
7	24	25	26	27	28	29	30	
8	31	1	2	3	4	5	6	novembre
9	7	8	9	10	11	12	13	
10	14	15	16	17	18	19	20	
11	21	22	23	24	25	26	27	
12	28	29	30	1	2	3	4	desembre
13	5	6	7	8	9	10	11	
14	12	13	14	15	16	17	18	
15	19	20	21	22	23	24	25	
16	26	27	28	29	30	31	1	gener
17	2							

	Dia festiu
	Lliurament PFC

Productes obtinguts.

- Programari jugador.
  Producte desenvolupat amb Java, que disposa d'una interfície que permet als jugadors participar en el BlackJack amb el casino.

- Programari gestor.
  Producte també desenvolupat en Java, que permet gestionar el programari del servidor de BlakJack.

Breu descripció dels altres capítols de la memòria.

- Capítol 2. BlackJack.
  Explicació del joc.

- Capítol 3. IAIK i PKI.
  Descripció del procés d'instal·lació de IAIK i la generació dels certificats de PKI amb OpenSSL.

- Capítol 4. Criptografia.
  Descripció i la implementació de l'esquema criptogràfic del BlackJack.

- Capítol 5. XML.
  Descripció dels documents XML utilitzats per fer les transferències de dades que s'envien durant l'execució dels protocols criptogràfics.

- Capítol 6. RMI.
  Descripció de la comunicació dels diferents components del sistema mitjançant RMI.

- Capítol 7. Base de dades.
  Disseny de la base de dades utilitzada per emmagatzemar les dades de les partides. Aquesta informació és essencial per fer una auditoria del joc.

- Capítol 8. Interfície jugador.
  Descripció i anàlisi de la interfície que permet als jugadors participar en el BlackJack.

- Capítol 9. Interfície gestor.
  Descripció i anàlisi de la interfície que permet utilitzar les funcionalitats del gestor.

- Capítol 10. Valoració econòmica.

- Capítol 11. Conclusions.

Capítol 2. BlackJack.

El BlakJack, també conegut com a vint-i-u, és un dels jocs de cartes de casino més populars en tot el mon. El seu precursor va ser el "vingt-et-un" originat als casinos francesos al voltant del 1700. Molta de la popularitat del BlackJack es deu a la barreja d'oportunitat amb elements d'habilitat i decisió, i la publicitat que envolta la pràctica de comptar cartes, una habilitat amb la que els jugadors poden prendre avantatge de les peculiaritats del joc fent les apostes basant-se en les cartes que queden a la baralla.

Les mans de BlackJack es compten per la seva puntuació total. La ma amb el total més alt guanya sempre que no passi de 21, el que s'anomena "trencar". Les cartes del 2 al 10 valen el seu número en punts, i les figures valen 10. Un "as" compte com a 11 a no ser que trenqui la ma, llavors val 1.

L'objectiu de cada jugador es superar a la banca, treien un ma no trencada més alta. Cal tenir en compte que si el jugador trenca la ma perd, encara que la banca trenqui la seva. Si el jugador i la banca treuen la mateixa puntuació, es produeix un empat, i cap dels dos guanya la ma.

Després de les apostes inicials, el croupier reparteix les cartes. En dona dos a cada jugador, incloent-se ell mateix. Una de les cartes que es reparteix es mostra cara amunt, de forma que els jugadors la poden veure, i l'altre tapada.

Una ma de dos cartes que fan 21 s'anomena BlackJack o "natural", i es automàticament guanyadora. S'acostuma a pagar 2:3 aquest tipus de mans.

Aquest és el sumari de com es procedeix després del repartiment:

- Si el repartidor te BlackJack i el jugador no, el repartidor guanya automàticament.
- Si el jugador te BlackJack i el repartidor no, el jugador guanya automàticament.
- Si el jugador i el repartidor tenen BlackJack, es produeix un empat.
- Si cap part te BlackJack, llavors el primer jugador juga completament la seva ma, seguit del següent jugador, i així anar fent.
- Quan tots els jugadors han acabat el repartidor juga la seva ma.

Les opcions que te el jugador per jugar la seva ma són:

- Demanar una altra carta ("hit").
- Plantar-se. Es a dir, no agafar mes cartes.
- Demanar una carta més i plantar-se.

- Dividir. Si el jugador te cartes amb idèntic valor (p.e. dos vuits), pot fer una aposta nova, i fer que cada una de les cartes sigui la primera en una nova ma.
- Rendir-se. Perdre la meitat de la posta i deixar la ma. No es pot fer a la majoria de casinos.

El torn del jugador finalitza quan:

- Decideix plantar-se.
- Trenca la ma.
- Demana una carta més i es planta.

Després de que tots els jugadors hagin pres les seves decisions, el repartidor revela la seva carta tapada. Les regles de la casa diuen que el repartidor ha d'agafar cartes fins que te almenys 17 punts, independentment del que tinguin els jugadors.

Si el repartidor es passa, tots els jugadors guanyem. Les apostes es paguen normalment 1 a 1.

Capítol 3. IAIK i PKI.

Per a implementar tot el protocol ens fa falta un seguit de criptosistemes que no es troben en el SDK de SUN (biblioteca de classes base de Java), i per aquest motiu utilitzarem la biblioteca criptogràfica IAIK.

Que és IAIK

IAIK Java Cryptography Extension (IAIK-JCE) és un conjunt d'APIs (Application Programming Interfaces) i implementacions de funcionalitats criptogràfiques, incloent funcions de hash, codis d'autenticació de missatges, encriptació simètrica, asimètrica, de flux, i de bloc, així com gestió de claus i certificats. Suplementa les funcions de seguretat bàsiques del JDK de Java.

Passos per instal·lar IAIK

- Descarregar la versió última del JDK de SUN i instal·lar-lo.

- Descarregar la última versió de IAIK. Cal registrar-se però no suposa cap cost. Si voleu descarregueu únicament l'arxiu iaik_jec_full.jar, que és la versió complerta signada.

- Descarregar les polítiques de seguretat de java que permeten emprar qualsevol longitud de clau, Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 5.0 RC

- (Windows) Copiar l'arxiu iaik_jce_full.jar als directoris:
  - c:\Archivos de Programa\Java\jdk1.5.0\jre\lib\ext
  - c:\Archivos de Programa\Java\jre1.5.0\lib\ext

- (Linux) Copiar l'arxiu iaik_jce_full.jar al directori:
  - $JAVA_HOME/jre/lib/ext

- (Windows) dins de l'arxiu jce_policy-1.5.0-beta2.zip hi ha els arxius:
  - local_policy.jar
  - US_export_policy.jar

  Copiar-los a:
  - c:\Archivos de Programa\Java\jdk1.5.0\jre\lib\security
  - c:\Archivos de Programa\Java\jre1.5.0\lib\security

- (Linux) dins de l'arxiu jce_policy-1.5.0-beta2.zip hi els arxius:
  - local_policy.jar
  - US_export_policy.jar

  Copiar-los a:
  - $JAVA_HOME/jre/lib/security

PKI

Que és PKI

Cada esquema criptogràfic implementat en aquest projecte necessita que els jugadors i gestor del joc disposin d'una parella de claus i el seu corresponent certificat.

Per tal de gestionar els certificats (emissió, revocació, etc.) d'un grup d'usuaris s'empra una infraestructura de clau pública. Típicament per fer referència a una infraestructura s'utilitzen les sigles PKI, que corresponen al terme en anglès Public Key Infrastructure.

Una PKI consta d'una autoritat de certificació notada amb CA, aquestes sigles corresponen al terme en anglès Certification Authority. Un altre component de la PKI són les autoritats de registre, notades amb les sigles RA (Registry Authority). Quan un usuari vol obtenir un certificat normalment realitza els passos següents. En un primer pas crea una parella de claus i realitza una petició de certificat mitjançant una RA. La RA valida la identitat de l'usuari que ha demanat el certificat i envia la petició a la CA. La CA rep les peticions de les RA i emet els certificats. La clau privada de la CA és una peça d'informació molt sensible, i per això està en un entorn amb un alt nivell de seguretat.

En el nostre cas utilitzarem OpenSSL per a construïr una petita PKI, ja que és es de lliure distribució i funciona perfectament.

Que és OpenSSL

El projecte OpenSSL és un esforç col·laboratiu per desenvolupar una llibreria que implementi els protocols SSL v2/v3 i TLS v1, i una funcions criptogràfiques generals, essent robusta, de nivell comercial, amb totes les característiques necessàries i de codi obert.

Està basada en l'excel·lent llibreria SSLeay desenvolupada per Eric A. Young i Tim J. Hudson.

Generació de certificats

El procés per a generar tots els certificats necessaris per al projecte es descriu a continuació. Utilitzarem "uoc2005" com a contrassenya.

1. Generar la parella de claus de 2048 bits de la CA (CA.key):

   openssl genrsa -des3 -out CA.key 2048

2. Generar un certificat autosignat amb la parella de claus de la CA. Aquest serà el certificat de la CA. (CA.crt):

openssl req -new -sha1 -x509 -key CA.key –out CA.crt –days 365

3. Generar una parella de claus de 1024 bits pel jugador (JUGADOR.key):
   openssl genrsa -des3 -out JUGADOR.key 1024

4. Emetre una petició de certificat (JUGADOR.scr):

   openssl req -new -sha1 -config openssl.cnf -key JUGADOR.key –out JUGADOR.csr

5. Emetre el certificat (JUGADOR.crt):

   openssl ca –config openssl.cnf -out JUGADOR.crt –infiles JUGADOR.csr

6. Generar l'arxiu PKCS12 (JUGADOR.p12) que contindrà la parella de claus del jugador, el certificat del jugador, i el certificat de la CA:

   openssl pkcs12 -export -in JUGADOR.crt -inkey JUGADOR.key -certfile CA.crt -out JUGADOR.p12

7. Generar una parella de claus de 1024 bits pel gestor (GESTOR.key):

   openssl genrsa -des3 -out GESTOR.key 1024

8. Emetre una petició de certificat (GESTOR.scr):

   openssl req -new -sha1 -config openssl.cnf -key GESTOR.key –out GESTOR.csr

9. Emetre el certificat (GESTOR.crt):

   openssl ca –config openssl.cnf -out GESTOR.crt –infiles GESTOR.csr

10. Generar l'arxiu PKCS12 (GESTOR.p12) que contindrà la parella de claus del gestor, el certificat del gestor, i el certificat de la CA:

    openssl pkcs12 -export -in GESTOR.crt -inkey GESTOR.key -certfile CA.crt -out GESTOR.p12

Capítol 4. Criptografia.

Requisits de seguretat.

Com ja hem vist en el resum del projecte, per a fer el joc segur necessitem que es compleixin les següents propietats:

- La unicitat de les cartes durant el joc. No hi poden haver duplicats.
- La distribució uniforme de les cartes barrejades
- La detecció de jugadors deshonestos.
- L'absència d'una tercera part de confiança.

A més, pel que fa les a postes, cal garantir:

- Autenticitat. S'ha de poder demostrar quin jugador l'ha realitzada.
- Integritat. No es poden manipular un cop realitzades.
- No-repudi. Ni jugador ni gestor poden repudiar les apostes un cop fetes.
- Seqüència de Joc. Una aposta ha d'incloure: la partida, l'instant de temps, la quantitat apostada, i el concepte.

Notació emprada en els protocols

En la descripció dels protocols s'empra la notació següent:

- ($P_{Entitat}$, $S_{Entitat}$): parella de claus asimètriques propietat d'Entitat,on P correspon a la clau pública, i S a la privada.

- $S_{Entitat}$ [M]: Signatura digital del missatge M amb la clau privada S d'Entitat.

- $E_{Entitat}$ (M): Xifratge del missatge M amb la clau asimètrica pública $P_{Entitat}$ d'Entitat.

- H(M): sortida d'una funció resum criptogràfica del missatge M, aquestes funcions reben el nom de funcions hash.

Protocols per garantir els requisits de seguretat.

Protocol de compromís

Els esquemes que es presenten a continuació tenen com a peça clau un protocol de compromís. En la literatura els trobarem amb el terme anglès de compromís de bit, bit commitment.

Aquests protocols tenen dues fases: la fase de lliurament del compromís, i la fase d'obertura del compromís. Anem a explicar el seu funcionament amb l'ajuda de dos usuaris; l'Anna i en Bernat.

Suposem que l'Anna es vol comprometre davant d'en Bernat a un cert valor c. En la fase de lliurament del compromís l'Anna calcula un cert valor c* a partir de c, i l'envia a en Bernat. Aquesta transformació té les propietats següents:

- En Bernat no pot saber res de c a partir de c*.
- L'Anna un cop ha enviat c* no pot trobar un altre valor c'<> c tal que es pugui obtenir c* a partir de c' . En unes altres paraules, l'Anna no pot canviar el seu compromís.

A la fase d'obertura del compromís l'Anna lliura c a en Bernat i aquest verifica que s'obté c* a partir de c. Aquest protocol té molta utilitat quan dues parts volen intercanviar-se certa informació de forma simultània. Per aquest mateix motiu l'utilitzarem en els protocols de joc.

En una partida I_P dos jugadors, P_1 i P_2, es comprometen a un valor c_1 i c_2 respectivament. Suposem que cada jugador té una parella de claus.

Protocol 1 $[(c_1, c_2, I_P)]$

1. P_1 calcula $c^*_1 = H(c_1)$;
2. P_1 signa c^*_1, amb la seva clau privada, $S_{P1}[I_P , c^*_1]$;
3. P_1 envia c^*_1 i $S_{P1}[I_P , c^*_1]$ a P_2;
4. P_2 calcula $c^*_2 = H(c_2)$;
5. P_2 signa c^*_2, amb la seva clau privada, $S_{P2}[I_P , c^*_2]$;
6. P_2 envia $S_{P2}[I_P , c^*_2]$ i c^*_2 a P_1;
7. P_1 verifica la signatura $S_{P2}[I_P , c^*_2]$ i la guarda juntament amb c^*_2 ;
8. P_2 verifica la signatura $S_{P1}[I_P , c^*_1]$, i la guarda juntament amb c^*_1 ;

El protocol d'obertura del compromís del jugador P_1 al jugador P_2 és com segueix:

Protocol 2 $[P_1, P_2, I_P]$

1. P_1 signa c_1, amb la seva clau privada, $S_{P_1}[I_P, c_1]$;
2. P_1 envia c_1 i $S_{P_1}[I_P, c_1]$ a P_2;
3. P_2 recupera c^*_1.
4. P_2 verifica la signatura digital $S_{P_1}[I_P, c_1]$;
5. P_2 verifica $c^*_1 \stackrel{?}{=} H(c_1)$.

Cas d'us protocol de compromís.

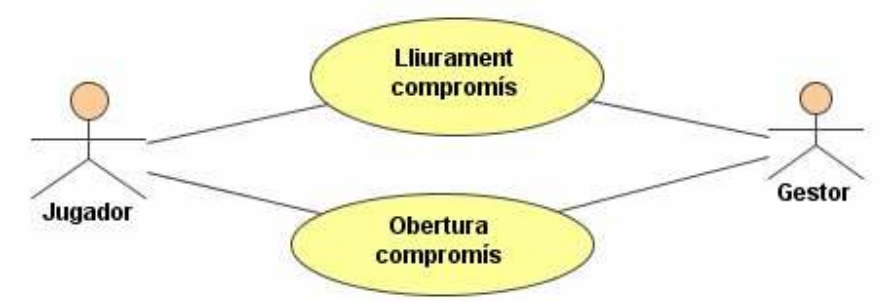
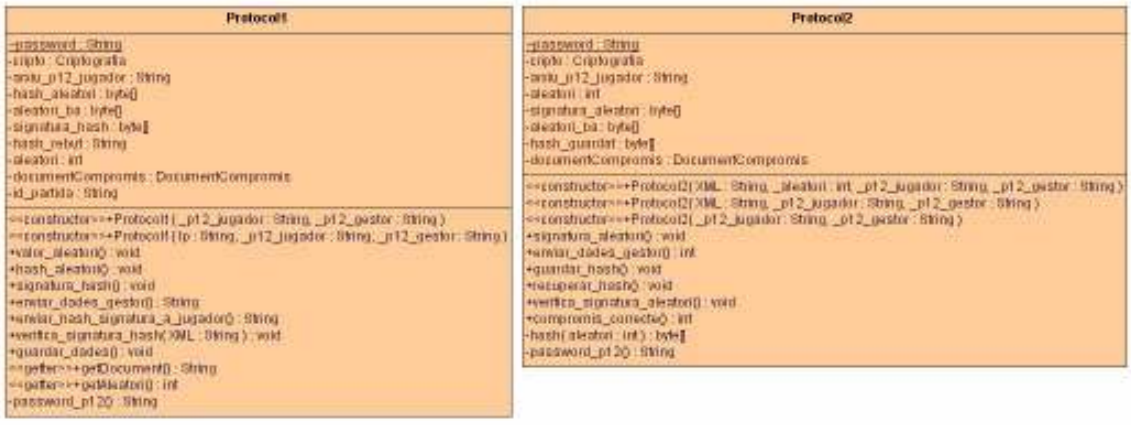


Diagrama de classes protocol de compromís.



Protocol d'autenticació

Suposem que en el joc hi participen n jugadors. Cada jugador Pi disposa d'una parella de claus (P_{Pi} , S_{Pi}). El gestor del joc també disposa d'una parella de claus (P_G, S_G). Definim I_G com l'identificador del gestor del joc.

Un jugador Pi per accedir als jocs ha d'estar registrat. En el procés de registre es recullen les dades següents:

IPi: Identificador de jugador. En el nostre cas aquest valor serà el hash del certificat;

Certi: Certificat digital de la parella de claus de Pi;

DPi: Diners de que disposa l'usuari per fer les seves apostes. Aquest valor inicialment és zero.

Aquestes dades són emmagatzemades a la BD.

Els usuaris per autenticar-se davant del gestor del joc empraran el protocol de Needham-Schroeder. Anem a veure el seu funcionament en el cas d'un jugador P_i i el gestor del joc G.

Protocol 3

1. P_i realitza les operacions següents:
   (a) obtenir un valor de forma aleatòria, N_i.
   (b) xifrar N_i i I_{Pi} amb la clau pública de G, $E_G(N_i, I_{Pi})$. I_{Pi} és l'identificador de P_i;
   (c) enviar $E_G(N_i, I_{Pi})$ a G;
2. G realitza les operacions següents:
   (a) desxifrar $E_G(N_i, I_{Pi})$ amb S_G, i obtenir; N_i i I_{Pi} ;
   (b) obtenir el certificat de P_i amb I_{Pi} . A partir del certificat obtindrà P_{Pi} ;
   (c) obtenir un valor de forma aleatòria, N_G.
   (d) xifrar N_i, N_G, I_G, amb la clau pública P_{Pi} de P_i, $E_{Pi}(N_i, N_G, I_{Pi})$;
   (e) enviar $E_{Pi}(N_i, N_G, I_{Pi})$ a G;
3. P_i realitza les operacions següents:
   (a) desxifrar $E_{Pi}(N_i, N_G, I_G)$ amb la clau privada S_{Pi} , i obtenir N_G, N_i i I_G;
   (b) xifrar N_G amb la clau pública P_G de G, $E_G(N_G)$;
   (c) enviar $E_G(N_G)$ a G;

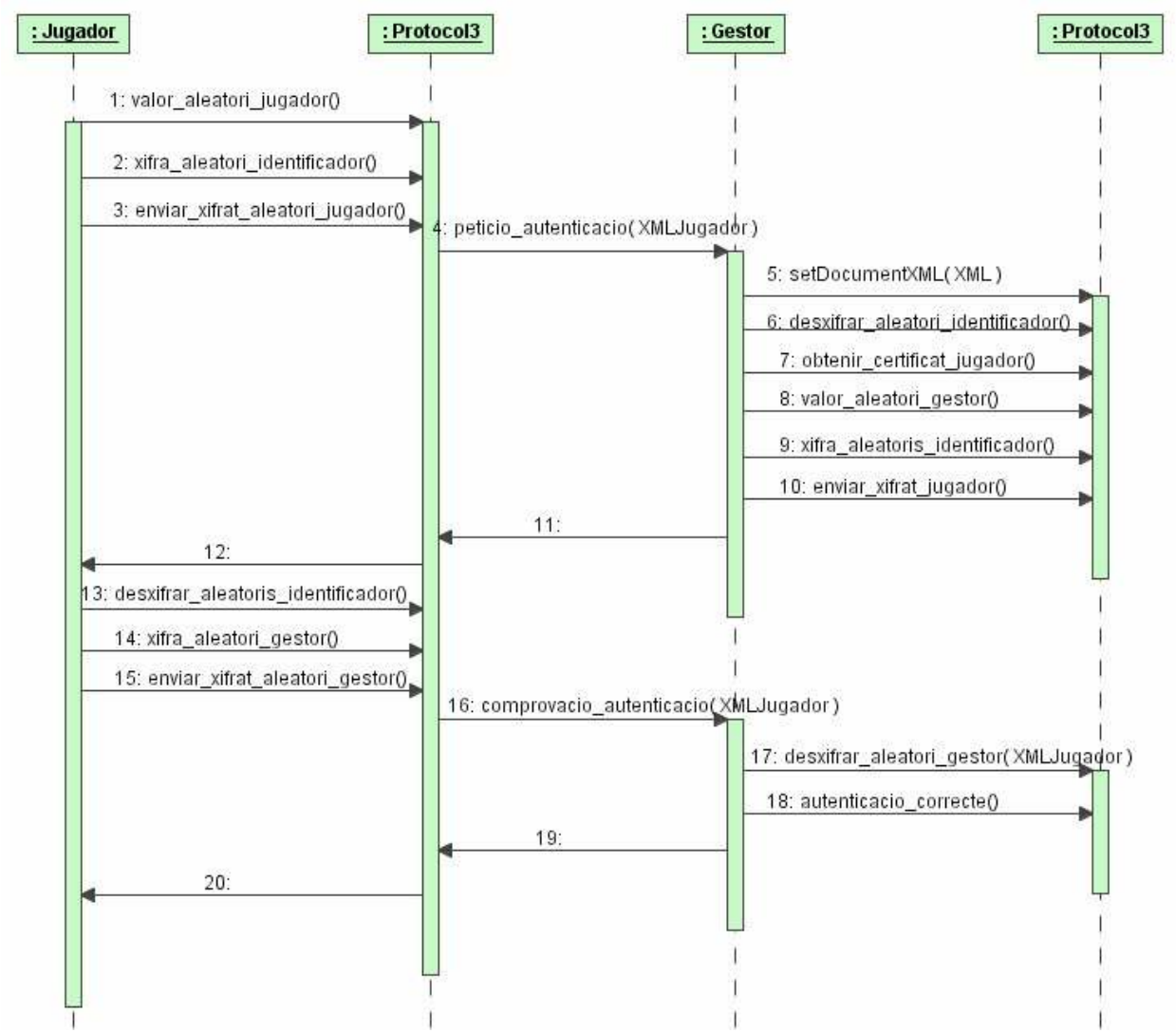
4. G realitza les operacions següents:

   (a) desxifrar $E_G(N_G)$ amb la clau privada S_G, i obtenir N'_G.
   (b) si $N'_G \stackrel{?}{=} N_G$, G i P_i estan autenticats bilateralment.

Cas d'ús autenticació.

Diagrama de classes autenticació.

Diagrama de seqüència autenticació.



Protocol iniciar partida

Un cop el jugador ha estat registrat ja pot iniciar una partida per un joc J. Per iniciar la partida empra el Protocol 4.

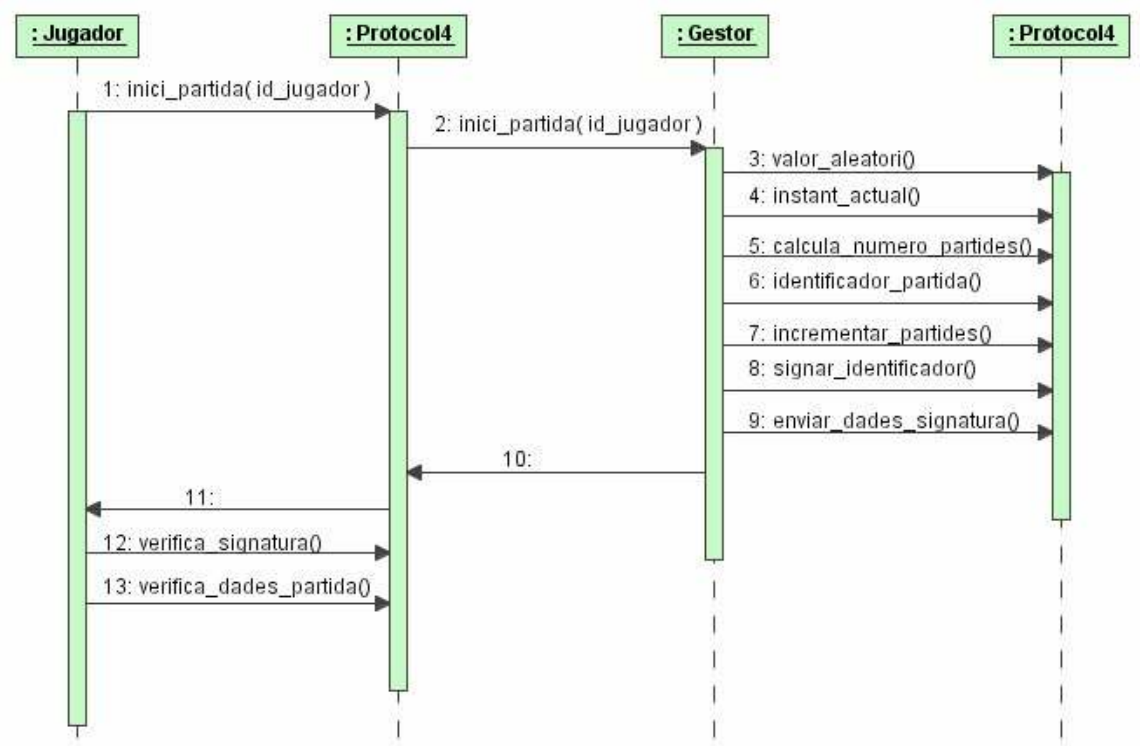
Protocol 4 [J]

1. P_i i G s'autentiquen amb el Protocol 3;
2. G calcula un identificador de partida I_P amb els passos següents:
   (a) obtenir de forma aleatòria un valor r;
   (b) obtenir l'instant actual T ;
   (c) obtenir el número de partides realitzades N;
   (d) calcular $I_P = J|r|T|N + 1$;
   (e) incrementar N en una unitat;
3. G signa I_P amb la clau privada $S_G[I_P]$;
4. G envia I_P i $S_G[I_P]$ a P_i;
5. P_i verifica la signatura $S_G[I_P]$;
6. P_i verifica que les dades de la partida, J i T , són correctes.

Cas d'us inici partida.

Diagrama de classes inici partida.

Diagrama de seqüència inici partida.



Protocol incrementar dipòsit

El jugador P_i ha d'ingressar diners al seu compte per tal de fer les apostes. L'increment del seu dipòsit es fa amb el Protocol 5.

Protocol 5

1. P_i realitza les operacions següents:
   (a) obtenir de forma aleatòria un valor r;
   (b) obtenir l'instant de temps, T ;
   (c) obtenir el valor que es vol afegir al dipòsit, V ;
   (d) obtenir les dades de la targeta de crèdit, B;
   (e) calcular l'identificador del dipòsit, A = r|T |V |B;
   (f) signar A amb la clau privada S_{P_i}, $S_{P_i}[A]$;
   (g) enviar A i S_{P_i} al gestor del joc G;
2. G realitza les operacions següents:
   (a) verificar la signatura $S_{P_i}[A]$;
   (b) verificar les dades del dipòsit: T , V i B;
   (c) calcular el nou dipòsit D'_{P_i} del jugador P_i, $D'_{P_i} = D_{P_i} + V$;
   (d) calcular el rebut del crèdit disponible R_D, $R_D = S_G[I_{P_i}|D_{P_i}]$;
   (e) enviar $D^0_{P_i}$ i R_D a P_i;
3. P_i realitza les operacions següents:
   (a) verificar la signatura digital de R_D;
   (b) verificar que el crèdit D'_{P_i} és correcte.

Cas d'us increment dipòsit.

Diagrama de classes increment dipòsit.

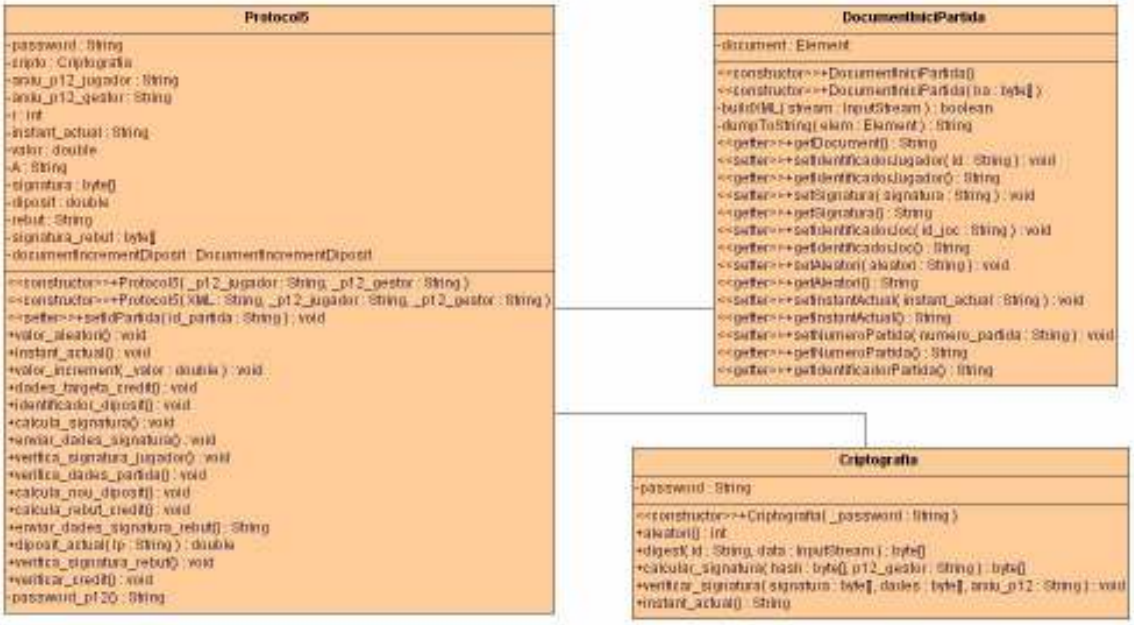
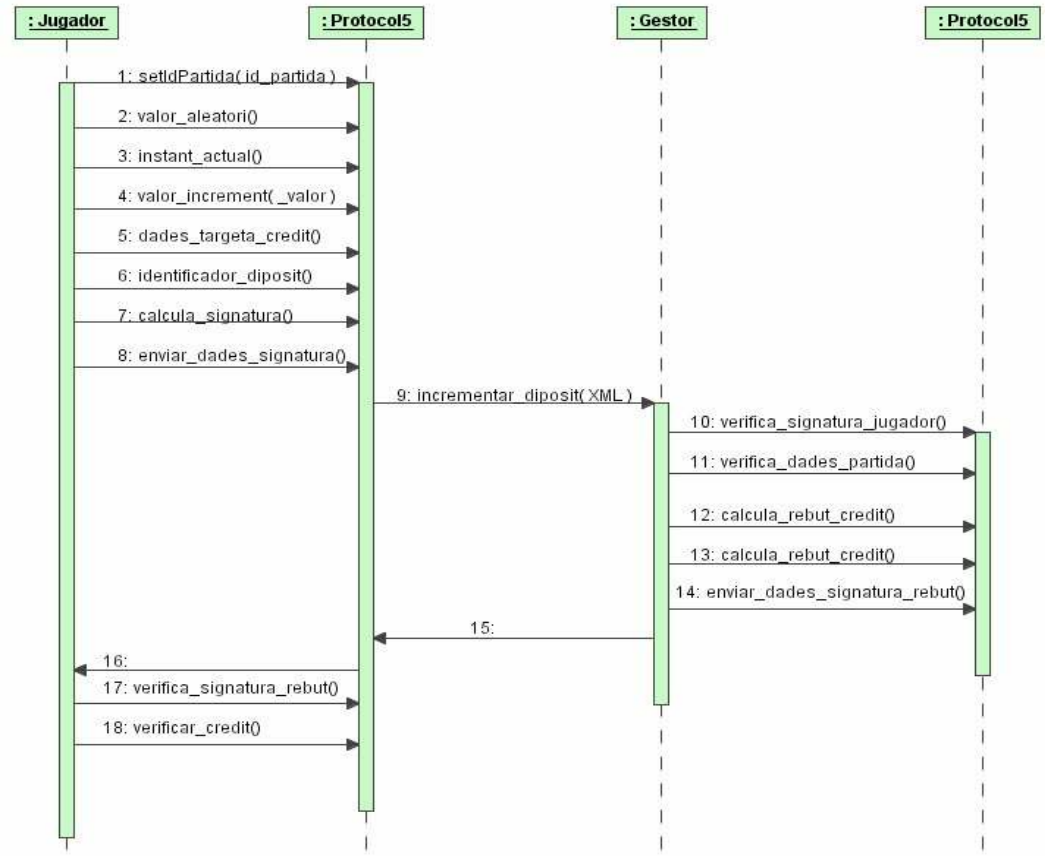


Diagrama de seqüència increment dipòsit.



Protocol apostar

Un jugador P_i realitza una aposta en una partida I_P mitjançant el protocol següent:

Protocol 6 [I_P]

1. P_i realitza els passos següents:
   (a) obtenir l'identificador de la partida, I_P ;
   (b) obtenir de forma aleatòria un valor r;
   (c) obtenir l'instant de temps actual, T ;
   (d) obtenir la quantitat de diners de l'aposta V ;
   (e) obtenir el concepte de l'aposta C;
   (f) calcular l'identificador de l'aposta $I_A = \{I_P | r | T | V | C\}$;
   (g) signar I_A amb la clau privada S_{P_i}, $I^*_A = S_{P_i}[I_A]$
   (h) enviar (I_A, I^*_A) al gestor del joc;
2. el gestor del joc G realitza els passos següents:
   (a) verificar la signatura digital I^*_A amb la clau pública de P_i;
   (b) verificar les dades de l'aposta: I_P ,T ,C.
   (c) verificar que P_i disposa de crèdit suficient, $D_{P_i} - V \geq 0$;
   (d) si disposa de crèdit:
      i. actualitzar el crèdit del que disposa el jugador, $D'_{P_i} = D_{P_i} - V$;
      ii. calcular el rebut R_A de l'aposta I_A, $R_A = S_G[I^*_A]$;
      iii. calcular el rebut del crèdit disponible R_D, $R_D = S_G[I_{P_i} | D'_{P_i}]$;
      iv. enviar D'_{P_i}, R_A i R_D a P_i.
   (e) si no disposa de crèdit no s'accepta l'aposta.
3. P_i realitza els passos següents:
   (a) verificar la signatura digital de R_A;
   (b) verificar la signatura digital de R_D;
   (c) verificar que el crèdit D'_{P_i} és correcte.

Cas d'us apostar.

Diagrama de classes apostar.

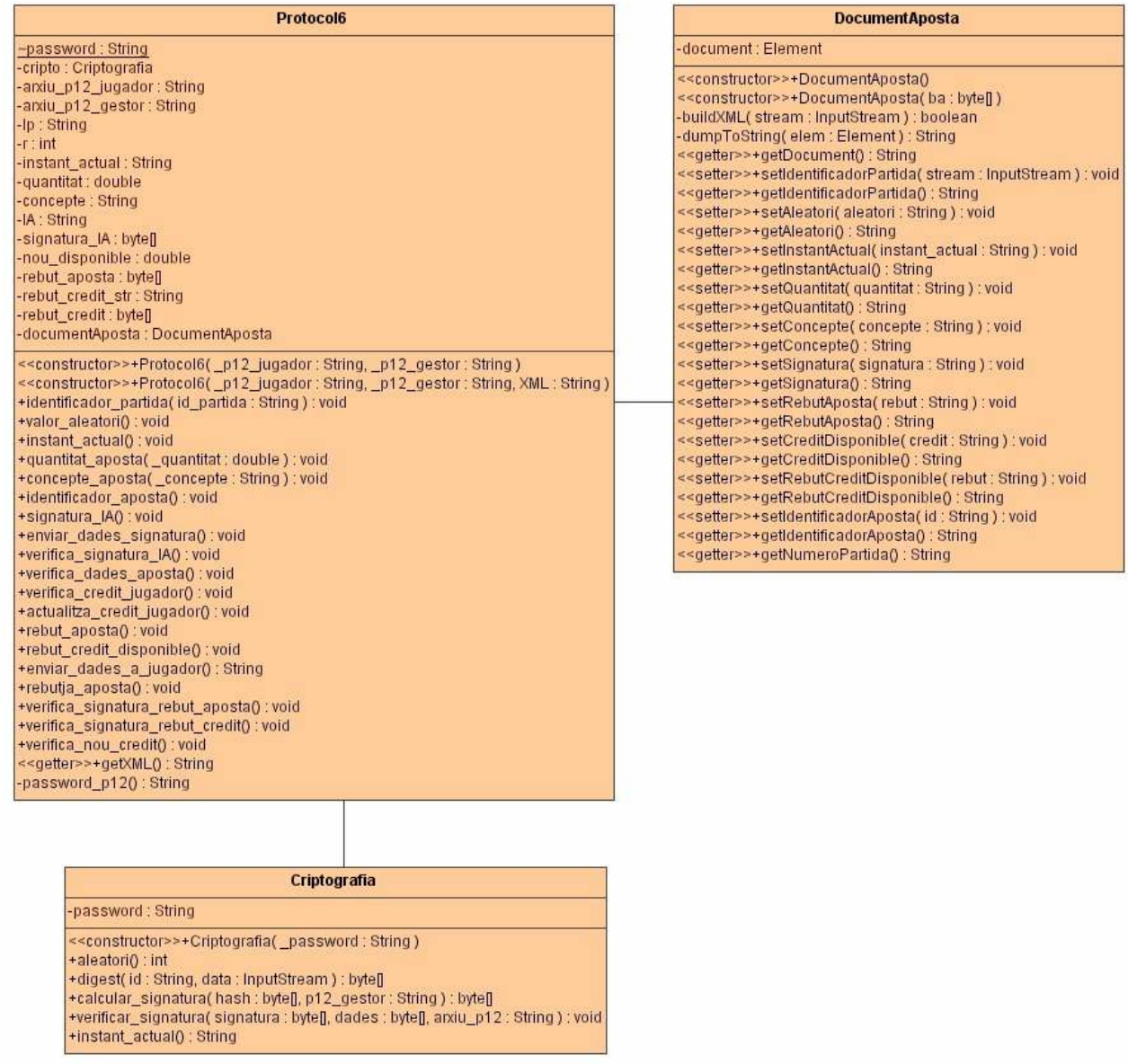
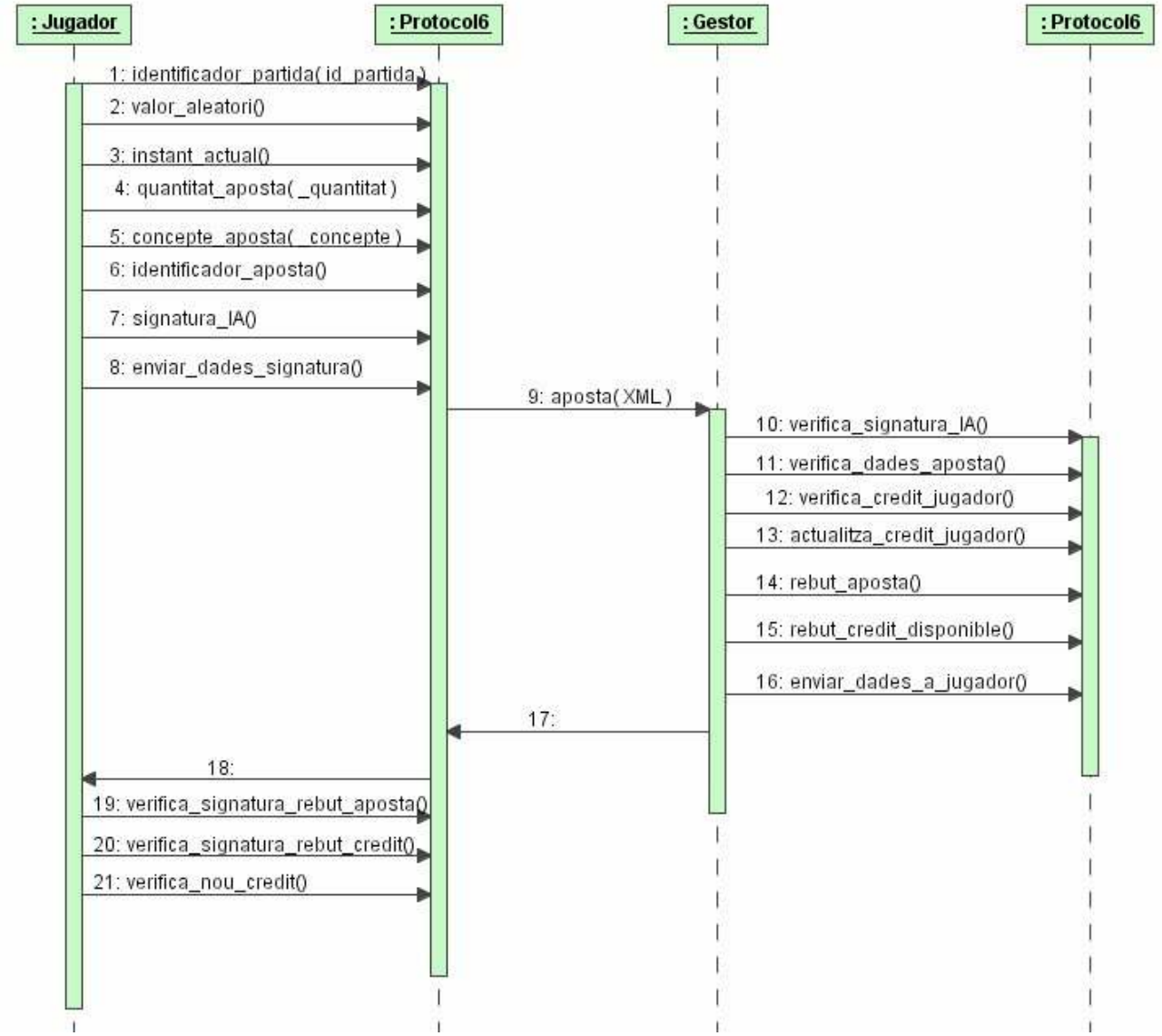


Diagrama de seqüència apostar.



Protocol cobrament

Al finalitzar una partida un jugador P_i cobra una aposta amb el següent protocol:

Protocol 7 $[(I_A, I^*_A, R_A)]$

1. G realitza les operacions següents:
   (a) verificar la signatura del rebut de l'aposta, R_A i l'aposta I^*_A;
   (b) calcular els guanys g del jugador P_i a la partida I_P amb l'aposta I_A;
   (c) calcular el nou crèdit disponible del jugador $D'_{P_i} = D_{P_i} + g$;
   (d) calcular el rebut del crèdit disponible R_D, $R_D = S_G[I_{P_i}|D'_{P_i}]$;
   (e) enviar R_D a P_i;
2. P_i realitza les operacions següents:
   (a) verificar la signatura de R_D;
   (b) verificar que el nou crèdit $D^0_{P_i}$ és correcte.

Cas d'us cobrament.

Diagrama de classes cobrament.

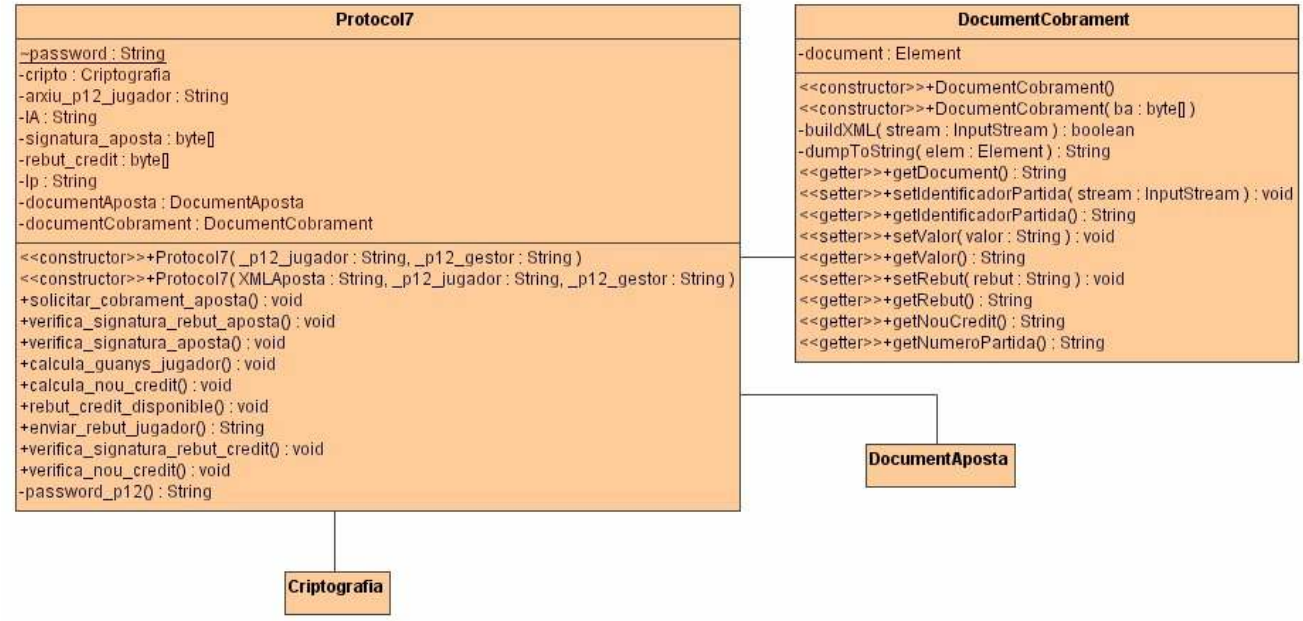
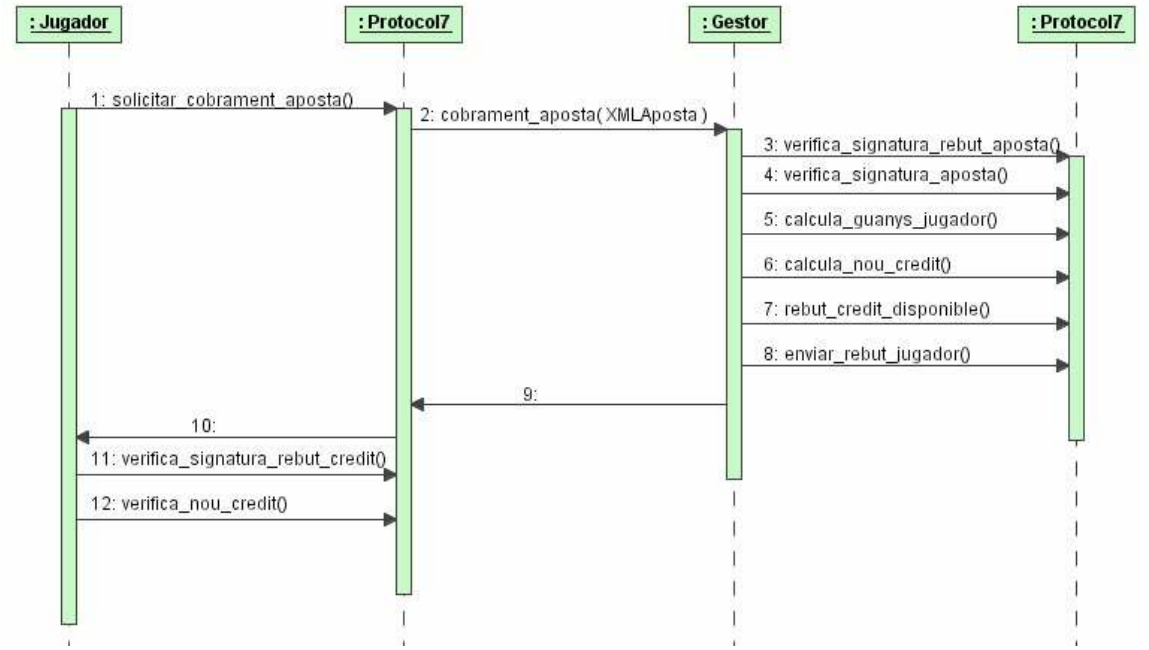


Diagrama de seqüència cobrament.



Protocol per a jugar al BlackJack.

En els jocs de cartes descobertes cada jugador obté diverses cartes, on cada carta és un esdeveniment. El jugador pot fer una aposta cada cop que obté una nova carta. El joc és honest si el jugador no té cap mena de coneixement de quin serà el nou esdeveniment (carta).

En aquest tipus de jocs el casino hi participa com un jugador més. En el nostre cas el gestor del joc G serà qui representarà al casino en el joc. Definim τ com el conjunt de cartes que han estat extretes. Inicialment aquest conjunt és buit.

Protocol 12

1. P_i i G s'autentiquen amb el Protocol 3;
2. P_i i G inicien un partida amb el Protocol 4;
3. P_i fa una aposta β amb el Protocol 6.
4. si P_i vol una carta descoberta executa conjuntament amb G el Protocol 13
5. si P_i vol una carta tapada executa conjuntament amb G el Protocol 14;
6. si P_i ha obtingut un guany G paga l'aposta de P_i amb el Protocol 7.

G i P_i empren el Protocol 13 per obtenir una carta descoberta. Suposem que el nombre de cartes d'una baralla és 52.

Protocol 13

1. P_i obté de forma aleatòria un valor c_1;
2. G obté de forma aleatòria un valor c_2;
3. P_i i G es comprometen a c_1 i c_2 respectivament, utilitzant el Protocol 1;
4. P_i lliura c_1 a G amb el Protocol 2;
5. G lliura c_2 a P_i amb el Protocol 1;
6. P_i i G realitzen els passos següents:
   (a) calcular $c = c_1 \otimes c_2$;
   (b) calcular $\tau_i = c \bmod 52$;
   (c) mentre $\tau_i \in \tau$ fer:
      i. $\tau_i := \tau_i + 1 \bmod 52$;
7. afegir τ_i a τ;
8. retornar τ_i;

P_i empra el Protocol 13 per obtenir una carta tapada. P_i només pot tenir una carta tapada.

Protocol 14

1. P_i obté de forma aleatòria un valor c_1;
2. G obté de forma aleatòria un valor c_2;
3. P_i i G es comprometen a c_1 i c_2 respectivament, utilitzant el Protocol 1;
4. G lliura c_2 a P_i amb el Protocol 1;
5. P_i realitza els passos següents:
   (a) calcular $c = c_1 \otimes c_2$;
   (b) calcular $\tau_i = c \bmod 52$;
   (c) mentre $\tau_i \in \tau$ fer:
      i. $\tau_i := \tau_i + 1 \bmod 52$;
6. afegir τ_i a τ;
7. retornar τ_i;

Cas d'us joc.

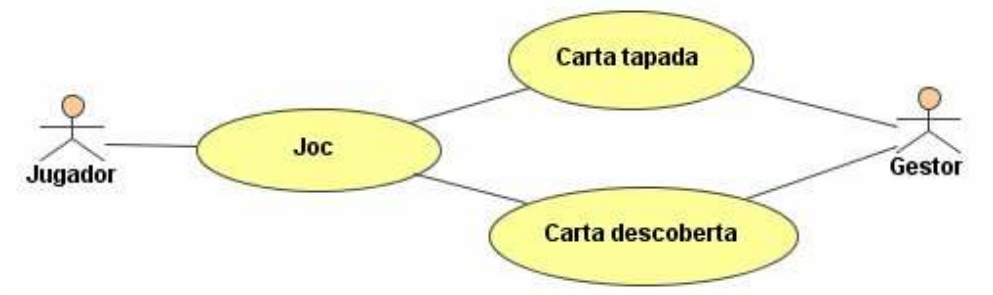


Diagrama de classes joc.

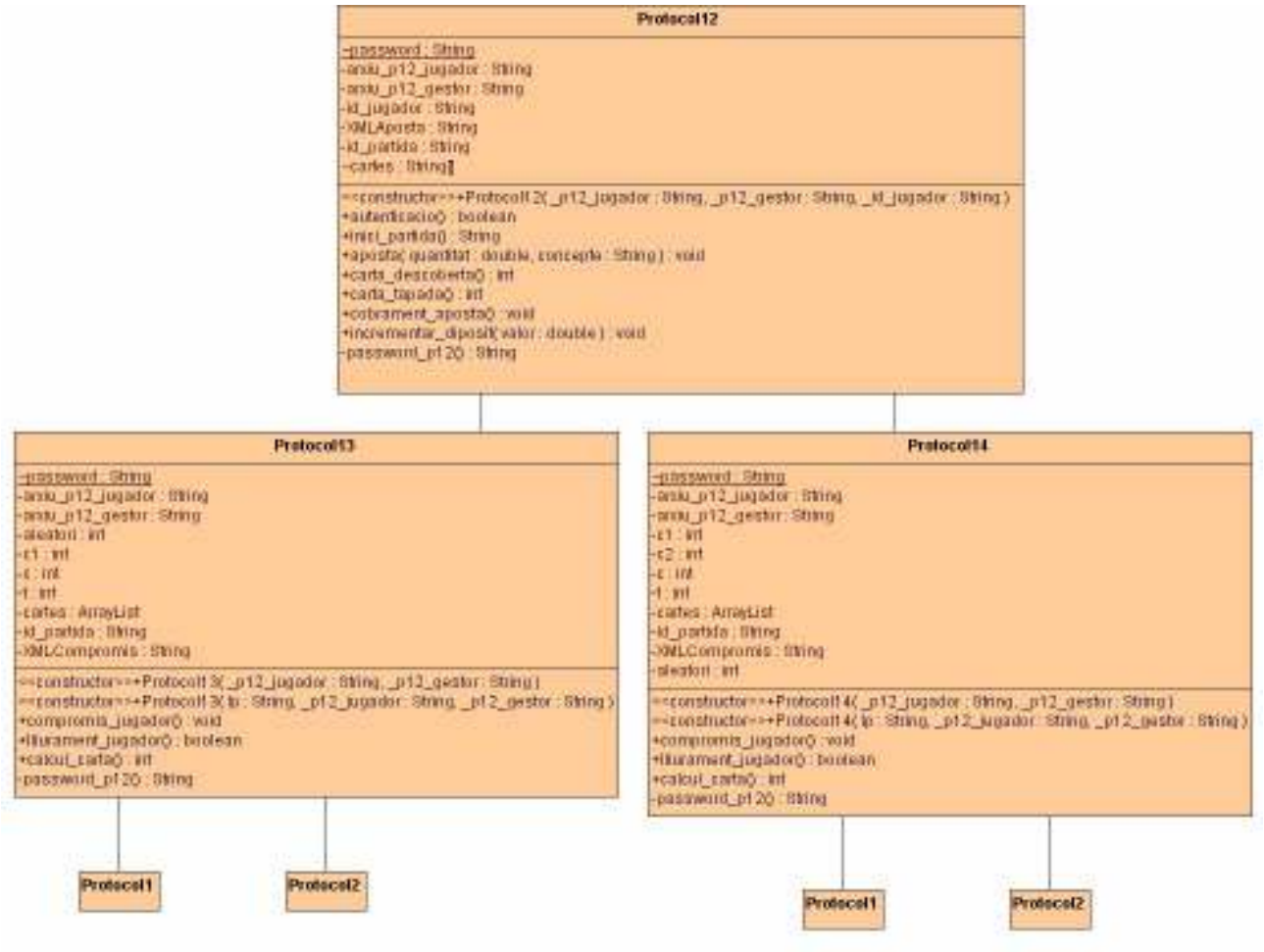


Diagrama de seqüència cartes descobertes.

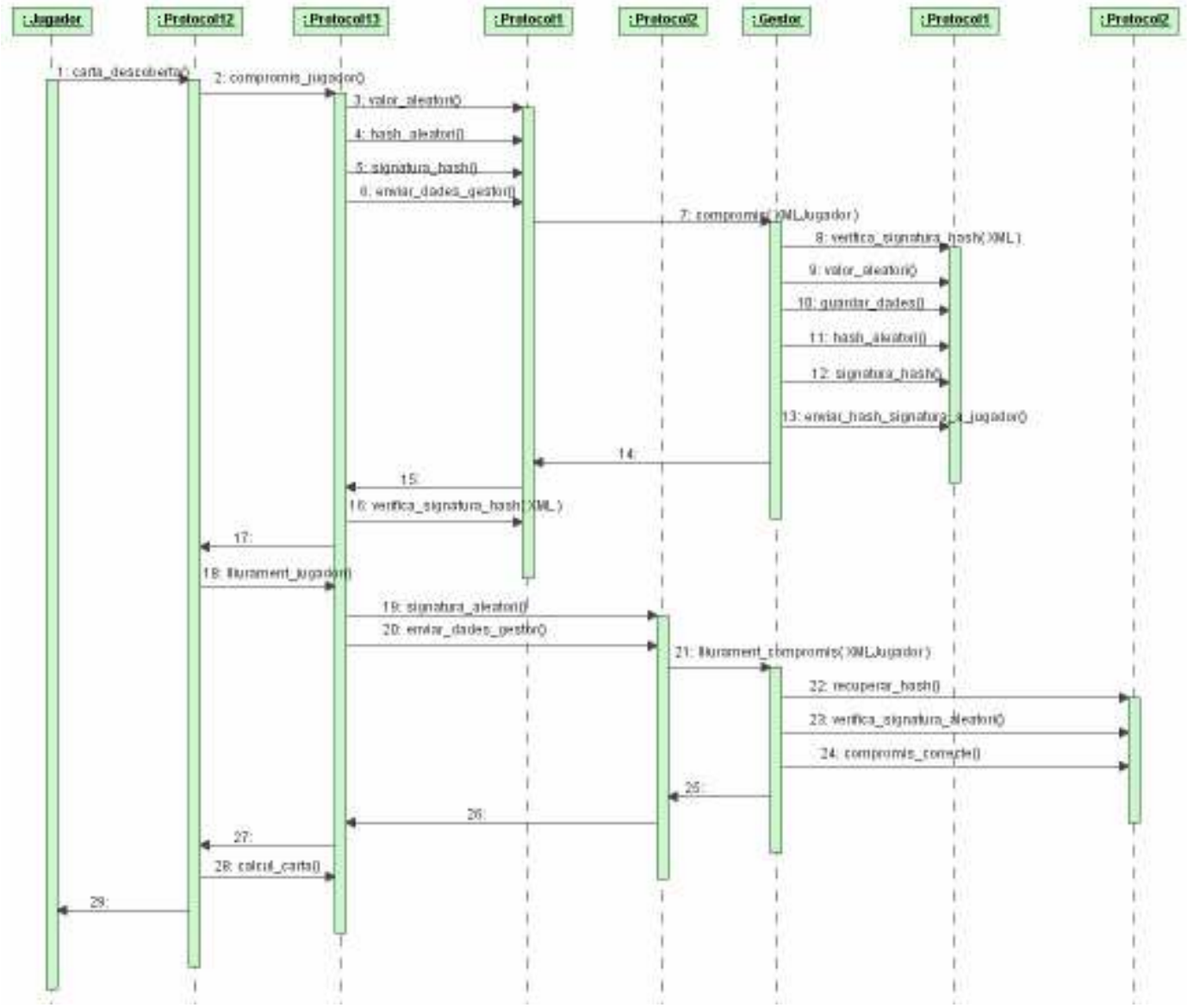
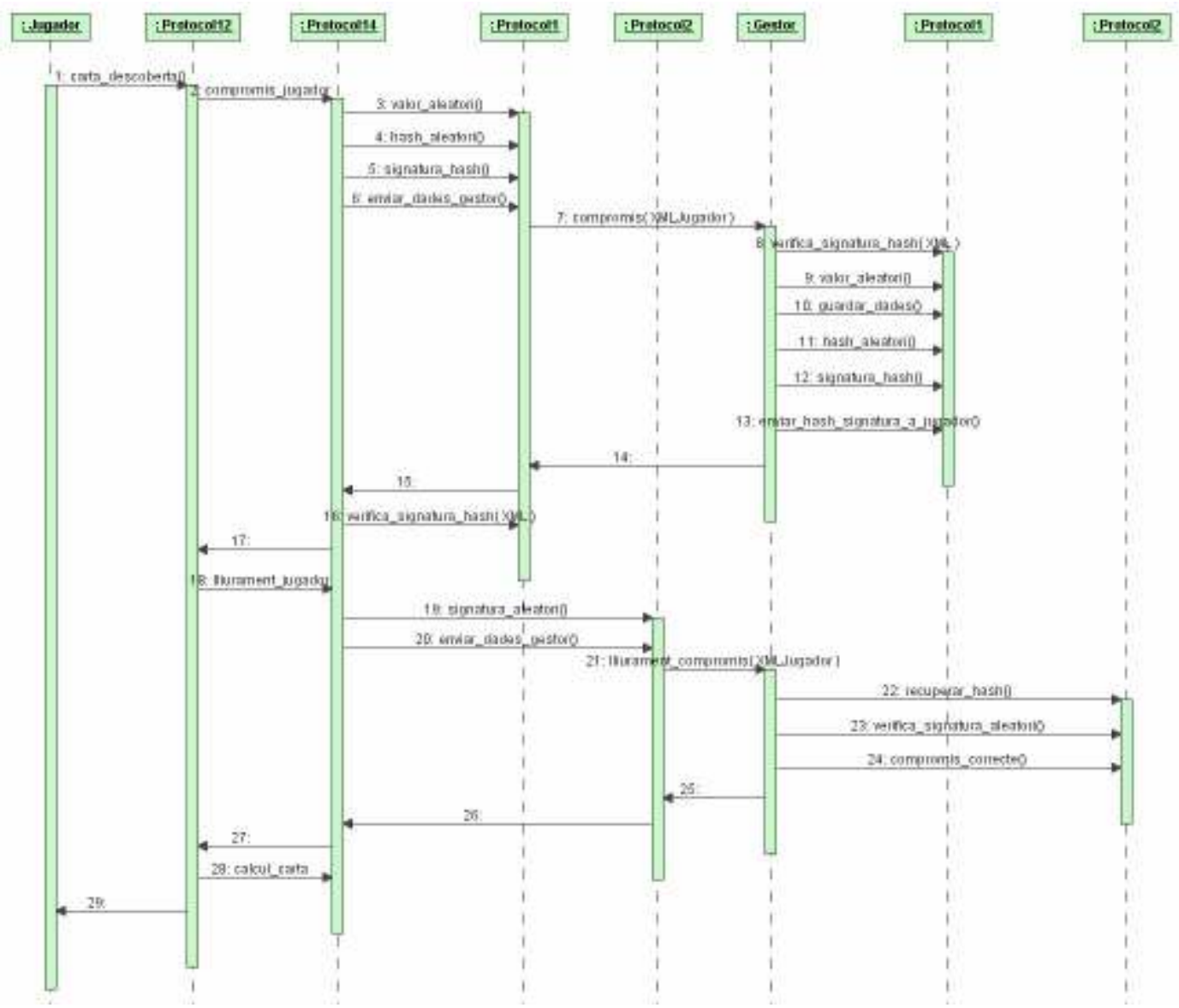


Diagrama de seqüència cartes tapades.



Capítol 5. XML.

Definició de XML.

XML és un llenguatge de marques per a documents que contenen informació estructurada. Te multitud d'aplicacions en diferents camps de la informàtica.

En aquest projecte l'utilitzem per a representar les dades que s'intercanvien els jugadors i el gestor durant el transcurs d'una partida de BlackJack

Documents XML utilitzats en els protocols.

Autenticació.

Documents XML per l'autenticació del jugador i el casino.

Esquema:

```
<Autenticacio>
   <XifratJugador>            </XifratJugador>
    <XifratGestor>            </XifratGestor>
    <XifratAleatoriGestor>    </XifratAleatoriGestor>
</Autenticacio>

<DadesJugador>
  <Aleatori>                  </Aleatori>
  <IdentificadorJugador>      </IdentificadorJugador>
</DadesGestor>

<DadesGestor>
  <AleatoriJugador>           </AleatoriJugador>
  <AleatoriGestor>            </AleatoriGestor>
  <IdentificadorJugador>      </IdentificadorJugador>
</DadesGestor>
```

Exemple:

```
<Autenticacio>
   <XifratJugador>
      MIIDigIBADGCAuUwggEqAgEAMIGSMIGMMQswCQYDVQQGEwJFUzESMBAGA1UECBMJ
      Q2F0YWxvbmlhMRIwEAYDVQQHEwlUYXJyYWdvbmExDDAKBgNVBAoTA1VPQzETMBEG
      A1UECxMKQ29uc3VsdG9yczEPMA0GA1UEAxMGQ0EgUEZDMSEwHwYJKoZIhvcNAQkB
      FhJqY2FzdGVsbGFyQHVvYy5lZHUCAQEwDQYJKoZIhvcNAQEBBQAEgYDDEoZXDRyF
      CF0bnRfG1ojzEbDEJV/TpoR9zslzsC1MquYoCN+xUOu2vOEGeNxv9CXCU6bJzSaB
      hysAo3SdqelyR8LL5LggPU6WfNmFmXp5xpZj5urGEelyUz+lxCrZTHwvVNmosJMB
      WVf4WBT2eN4oT/fCynlH0yC5MDwChjPjRDCCAbMCAQAwgZowgYwxCzAJBgNVBAYT
      AkVTMRIwEAYDVQQIEwlDYXRhbG9uaWExEjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoG
      A1UEChMDVU9DMRMwEQYDVQQLEwpDb25zdWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMx
      ITAfBgkqhkiG9w0BCQEWEmpjYXN0ZWxsYXJAdW9jLmVkdQIJAKvDspAutpU4MA0G
      CSqGSIb3DQEBAQUABIIBAFBdYvSNAZUG44dTQGB8KmxCQSFAsjvSHfFFe5b4glcc
      Bd/apJpmSEbg1o0JZMOWwbYZ+kp1xBTSVjClXWHwtLIkGbr7tA6g+yXxtZ0u4fDQ
      Joy8+kXexjw/Qi0L750WKsV8xE5gFzNgCqM2ciilkDfpDYCXBx5pKyGSrOz62Avu
      gOte4xVv7e38r8Tj64wCssBc1+ehInWN09zGiGEWDXmod85TtNmvetNOruomBR/w
      QUh64XJeeINQVn6WY6f37hq816MD4nN96MqfoBAIj8uEs4MRr0/Ofv3ylVk5PirN
      cKCJzCQ010r6jDqnRvoDhick/6zBu0+I+BXvOiUveOUwgZsGCSqGSIb3DQEHATAU
      BggqhkiG9w0DBwQIECBroqrP9omAeEONevqqmt01LJgW5XOHbRVrZuOmEm3O86IA
      bTn4WA5g2AT0YjwLnXonu9ZoPAii2gWXDNF4lJGPgw608/JcohxGNcjJOO7Eq6f3
      CrZQu9FKI6CpjYQwu66vDF8VZ2J/foKy4yGgT5CXhkUxu01Zw1/gzWrInr2FVg==
  </XifratJugador>
  <XifratGestor>
```

```
      MIIDwwIBADGCAuUwggEqAgEAMIGSMIGMMQswCQYDVQQGEwJFUzESMBAGA1UECBMJ
      Q2F0YWxvbmlhMRIwEAYDVQQHEwlUYXJyYWdvbmExDDAKBgNVBAoTA1VPQzETMBEG
      A1UECxMKQ29uc3VsdG9yczEPMA0GA1UEAxMGQ0EgUEZDMSEwHwYJKoZIhvcNAQkB
      FhJqY2FzdGVsbGFyQHVvYy5lZHUCAQIwDQYJKoZIhvcNAQEBBQAEgYBDe6y9zMTM
      rEffRtYYfM6p28wai6IX/bPMjVXshANH6meOtgallVw14fdME7D22FhUxZxfWOZg
      1azK8kctfmpzIq64dYBCeptVlSWC61eBpsQbzwU73rRmtD8/oxJTgKYytDk3+nWg
      auu4U66xUwco2rssiokHmDxAUXPBKB1fMzCCAbMCAQAwgZowgYwxCzAJBgNVBAYT
      AkVTMRIwEAYDVQQIEwlDYXRhbG9uaWExEjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoG
      A1UEChMDVU9DMRMwEQYDVQQLEwpDb25zdWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMx
      ITAfBgkqhkiG9w0BCQEWEmpjYXN0ZWxsYXJAdW9jLmVkdQIJAKvDspAutpU4MA0G
      CSqGSIb3DQEBAQUABIIBABuMbnF2T0U0QXpn15GrMLaJUH1rCiwCf5fsffRCf91z
      PXlsoM0D2SNghl+dxJS+7HpPUMEEV9zPiLx0aLtuA2DpMViYG+vREetUlJAKzXfJ
      2pSGaGBh3ygJtfDV8dYmgLNk2edpjl1yQIefCHBcQzcdHTyqtw0vCyybOwgbaMJz
      9mYe+b38lzhwTe4+hcobx7EDVGK37HmGh6mCEuNrmtKllWvvHiGmeamLlW2acLOq
      5NTeypgR6QKtWX9qE3AQrKPBN1OaszqLzLXNACTU2pxarArHJLwR2NJxW+uCigob
      cblASPBXgBsLrMlYwGNEJbAt3Gtcfa27pC3UD6a5OmQwgdQGCSqGSIb3DQEHATAU
      BggqhkiG9w0DBwQIfYsPRv7aCkSAgbAcEL0ulCdCSqPgCyHqQy1nUL99Nj43h4qK
      THbUVNxnHDPASR27LrTKMCSr2osM45KD5hlrQlp+fyX+HCSsqLJh9ybhGNqEh2ai
      PGL/3UbXs78cXb9dFVe2O1KoLKEI1sY5RzKHLU3cPy/Cyvi2Ftg2tMVBCJF91bUk
      iI4nm+GWq06mKTH9q2g3U1b9rfyVgu15UrvkTnT/VrHJo1fpMQfbaGilQP+JbfRL
      wSFuwuqfvg==
  </XifratGestor>
  <XifratAleatoriGestor>
      MIIDIQIBADGCAuUwggEqAgEAMIGSMIGMMQswCQYDVQQGEwJFUzESMBAGA1UECBMJ
      Q2F0YWxvbmlhMRIwEAYDVQQHEwlUYXJyYWdvbmExDDAKBgNVBAoTA1VPQzETMBEG
      A1UECxMKQ29uc3VsdG9yczEPMA0GA1UEAxMGQ0EgUEZDMSEwHwYJKoZIhvcNAQkB
      FhJqY2FzdGVsbGFyQHVvYy5lZHUCAQEwDQYJKoZIhvcNAQEBBQAEgYA3uBbOcDH9
      3WAIfvjE1ufrsrkrhth2yKVGg5Dgay4VLjmqjpZT8xEjfMusNei1Y26lq7B+NHPJ
      GT3Fxq9pmf3cK+5gAU1RvPRtqlN8oYIqh2eehdSy4oPSQ4HrbUmYivOe9lJ/qch1
      kWSWRxBFzJdJStJtEAuCTFlV0AOJ0UCQ2zCCAbMCAQAwgZowgYwxCzAJBgNVBAYT
      AkVTMRIwEAYDVQQIEwlDYXRhbG9uaWExEjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoG
      A1UEChMDVU9DMRMwEQYDVQQLEwpDb25zdWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMx
      ITAfBgkqhkiG9w0BCQEWEmpjYXN0ZWxsYXJAdW9jLmVkdQIJAKvDspAutpU4MA0G
      CSqGSIb3DQEBAQUABIIBAHFaDpf49RSukw5eElQSuPX6fiH8o2PhWhBS68acFJCy
      NoXLz/YyYO17m3rLfLVpHJYCWmRVl5EVzRLeyflio6xM3N2EcZ/tIPZ549wLwxNh
      AH0v1EHA13k6y+kaNrnJZzDuyQZuqWfB+0zceUmbD13ptpY09kI/RnTpPN+Vr1sD
      ahYyzT55D03bqO6Qqh2JXl4oM3FpmTzBUCaD++kj7YE1k6VDQtt9lg5WGI5jI9GW
      UnwCw2UZrNnV5CuzpscuFJdvRZXy2rcvGsM3IrF645ku4wOj94VMqN/Wipe31NTP
      Jyw5ntoM3ffhNxUDE2gVVHXCjb1/YI/ImhA7e0qTVu0wMwYJKoZIhvcNAQcBMBQG
      CCqGSIb3DQMHBAi2HLRdg7OO2YAQmX7YIQTJJlt+cqmN4yfkhA==
   </XifratAleatoriGestor>
</Autenticacio>


<DadesJugador>
  <Aleatori>763522153</Aleatori>
  <IdentificadorJugador>1</IdentificadorJugador>
</DadesGestor>

<DadesGestor>
  <AleatoriJugador>763522153</AleatoriJugador>
  <AleatoriGestor>131209961</AleatoriGestor>
  <IdentificadorJugador>1</IdentificadorJugador>
</DadesGestor>
```

Iniciar partida.

Document XML iniciar una partida.

Esquema:

```
<IniciPartida>
  <IdentificadorJugador>      </IdentificadorJugador>
  <IdentificadorPartida>
    <IdentificadorJoc>        </IdentificadorJoc>
    <Aleatori>                </Aleatori>
    <InstantActual>           </InstantActual>
    <NumeroPartida>           </NumeroPartida>
```

```
  </IdentificadorPartida>
  <Signatura>                </Signatura>
</IniciPartida>
```

Exemple:

```
<IniciPartida>
  <IdentificadorJugador>1</IdentificadorJugador>
  <IdentificadorPartida>
    <IdentificadorJoc>BlackJack</IdentificadorJoc>
    <Aleatori>191509737</Aleatori>
    <InstantActual>2005-10-29 19:29:25</InstantActual>
    <NumeroPartida>145</NumeroPartida>
  </IdentificadorPartida>
  <Signatura>
      MIIKfQIBATELMAkGBSsOAwIaBQAwCwYJKoZIhvcNAQcBoIIJHzCCBIUwggNtoAMC
      AQICAQEwDQYJKoZIhvcNAQEFBQAwgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlD
      YXRhbG9uaWExEjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMwEQYD
      VQQLEwpDb25zdWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0BCQEW
      EmpjYXN0ZWxsYXJAdW9jLmVkdTAeFw0wNTEwMDQxMTM4MDlaFw0wNjEwMDQxMTM4
      MDlaMIGQMQswCQYDVQQGEwJFUzESMBAGA1UECBMJQ2F0YWx1bnlhMSgwJgYDVQQK
      Ex9Vbml2ZXJzaXRhdCBPYmVydGEgZGUgQ2F0YWx1bnlhMRAwDgYDVQQLEwdBbHVt
      bmVzMQ8wDQYDVQQDEwZHZXN0b3IxIDAeBgkqhkiG9w0BCQEWEWpjYXN0ZWxsYUB1
      b2MuZWR1MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDmtqFKeGB2zGSzQmu5
      m38fZY1Rc8AS8r/QacKxyLNLHxBnPylE+d2BjmnDoSJHlYuV7qkoDaCmHZqRzM22
      kZbdBgpi1akpkStXsDgNqxDBQ5Cz9NvYTqaeUSa/owuHGcsd5VlOwQkGqhQdY9Tv
      gN43fWwR/j8ASF0wQ1nlnF8l+wIDAQABo4IBbjCCAWowCQYDVR0TBAIwADARBglg
      hkgBhvhCAQEEBAMCBaAwCwYDVR0PBAQDAgXgMDEGCWCGSAGG+EIBDQQkFiJTZWd1
      cmV0YXQgZW4gWGFyeGVzIGRlIENvbXB1dGFkb3JzMB0GA1UdDgQWBBQuRbiGe27q
      8EiCxRFYULGz/uVFHTCBwQYDVR0jBIG5MIG2gBTSZ3kYcqekU68MNR97NveA/YWt
      saGBkqSBjzCBjDELMAkGA1UEBhMCRVMxEjAQBgNVBAgTCUNhdGFsb25pYTESMBAG
      A1UEBxMJVGFycmFnb25hMQwwCgYDVQQKEwNVT0MxEzARBgNVBAsTCkNvbnN1bHRv
      cnMxDzANBgNVBAMTBkNBIFBGQzEhMB8GCSqGSIb3DQEJARYSamNhc3RlbGxhckB1
      b2MuZWR1ggkAq8OykC62lTgwHAYDVR0RBBUwE4ERamNhc3RlbGxhQHVvYy5lZHUw
      CQYDVR0SBAIwADANBgkqhkiG9w0BAQUFAAOCAQEAnMZN6KaeEf75VPZtwMbn0dv/
      FKaaHlgbRlIDzbrGGq0aclfNf+3mYv/mR3BcEbn8myJFqDdoU6yzFpYGFr4+ZszC
      kMkyx2GF3gUWqQ2pw/VEqAvj1adoQNR0i9zpdGcFUXO9BOWxprLLgiPP1ME9ulIB
      WgtHii/f9VKitisu0BWGY/4fagfPgGNYyD7AhVNT1AejTPuLCMhSD5XQam4tKvUJ
      6NTWPhcH5uZ6BykeFFOnRew4Y8lCstzJ9He+FQ9U6+lhIt4LkEkhauZcF4o2XtbR
      3EfiU4W2hzGhekGXvxvVgP28gdWXE6pp/hCTY+45b/Fxq7HwoCPPRnkBqMIGkDCC
      BJIwggN6oAMCAQICCQCrw7KQLraVODANBgkqhkiG9w0BAQUFADCBjDELMAkGA1UE
      BhMCRVMxEjAQBgNVBAgTCUNhdGFsb25pYTESMBAGA1UEBxMJVGFycmFnb25hMQww
      CgYDVQQKEwNVT0MxEzARBgNVBAsTCkNvbnN1bHRvcnMxDzANBgNVBAMTBkNBIFBG
      QzEhMB8GCSqGSIb3DQEJARYSamNhc3RlbGxhckB1b2MuZWR1MB4XDTA1MTAwNDEw
      NTUxMloXDTA2MTAwNDEwNTUxMlowgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlD
      YXRhbG9uaWExEjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMwEQYD
      VQQLEwpDb25zdWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0BCQEW
      EmpjYXN0ZWxsYXJAdW9jLmVkdTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
      ggEBALTjkFuSne+TJBFaZL0qDz2889Rx6ErcWLtCK0xz+UPuB9yzd2qHhisRjY+E
      kRnlsXb3p2/1leoTYUGu59bgiIcjMVMNgT/eFRkl9X0oEGZEXHy/4US+w2a4PtGm
      Q7wEyMcSEpkjyfS+GKreynw9VVyWFwAQ9umUVZ28hPrXFt6tbUziYWRB0+ArkGFL
      8e4zYudtzhh1FMFOvW8WOA2VK5zW596ChXbNQ6+i4OZgYmwWPT9f8x2jk+Pf5OGD
      IyjHzBU4xJ6409JgHDsWtm/5SJd+9wC5GYT5K6oNikR718XsV74svAx8bfA11M3n
      LT+jdQ7VuFrrCeNhkpTtlqyjcDMCAwEAAaOB9DCB8TAdBgNVHQ4EFgQU0md5GHKn
      pFOvDDUfezb3gP2FrbEwgcEGA1UdIwSBuTCBtoAU0md5GHKnpFOvDDUfezb3gP2F
      rbGhgZKkgY8wgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlDYXRhbG9uaWExEjAQ
      BgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMwEQYDVQQLEwpDb25zdWx0
      b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0BCQEWEmpjYXN0ZWxsYXJA
      dW9jLmVkdYIJAKvDspAutpU4MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQAD
      ggEBAGdbzQcIddybkIqsAhm+vptcjGHv2ae9aBhQc6PQNJF/IBSuYQVh5Q78mTRO
      l3cTFfkbl2/LaFrx0Ejdb0s69mbRrHMM+VU49SZiJLV+f/A/Pa0xHPTTfAr5rDmO
      BVNO+GFisAJkmZnu+Wd43w/1fnRIxGsf4GP7s+8Sv8FTX9TiQkJicalKPZKl9TyH
      5BOmrPIH2FURov92wQ2/7vbi/vIYDQeiDfoo6mE0PvOdGJvuQbFOt1xSrIHjg1DG
      gv5d+IEjA++Ry+kw3kuX8t82gsW0QjsnA8dzEv8FWT6apGwoZGivBWbgQJ2+F3cR
      Qy5iWMRkOArz/Co++m/3QQ6bZHExggE5MIIBNQIBATCBkjCBjDELMAkGA1UEBhMC
      RVMxEjAQBgNVBAgTCUNhdGFsb25pYTESMBAGA1UEBxMJVGFycmFnb25hMQwwCgYD
      VQQKEwNVT0MxEzARBgNVBAsTCkNvbnN1bHRvcnMxDzANBgNVBAMTBkNBIFBGQzEh
      MB8GCSqGSIb3DQEJARYSamNhc3RlbGxhckB1b2MuZWR1AgEBMAkGBSsOAwIaBQAw
      DQYJKoZIhvcNAQEBBQAEgYAwj9eRY093cpEaNWQEav3KeU6sWPE5iJlDJyzKcU8m
      Y+sb+Mk2kSFnZLvojdcxrjpVTHI39oCsNMql1dG2GRXtqgurmVrnB2eiyf6m0vHT
```

```
      ufmn8t4NVvka8GALI325ZweHA5YLEWJ54Z7vXeuzbwCIAHC3dwp+C8zIXUycajDIug==
  </Signatura>
</IniciPartida>
```

Incrementar dipòsit.

Document XML per l'increment del dipòsit del jugador.

Esquema:

```
<IncrementDiposit>
   <IdentificadorDiposit>
     <Aleatori>       </Aleatori>
     <InstantActual>  </InstantActual>
     <Valor>          </Valor>
     <Targeta>        </Targeta>
   </IdentificadorDiposit>
   <Signatura>      </Signatura>
   <NouDiposit>
     <IdentificadorPartida>
       <IdentificadorJoc>           </IdentificadorJoc>
       <Aleatori>                   </Aleatori>
       <InstantActual>              </InstantActual>
       <NumeroPartida>              </NumeroPartida>
     </IdentificadorPartida>
     <Valor>   </Valor>
   </NouDiposit>
   <Rebut>    </Rebut>
</IncrementDiposit>
```

Exemple:

```
<IncrementDiposit>
  <IdentificadorDiposit>
    <Aleatori>985946074</Aleatori>
    <InstantActual>2005-10-29 19:32:36</InstantActual>
    <Valor>5.0</Valor>
    <Targeta>4444 5555 3333 2222</Targeta>
  </IdentificadorDiposit>
      <Signatura>
           MIIKgAIBATELMAkGBSsOAwIaBQAwCwYJKoZIhvcNAQcBoIIJIjCCBIgwggNwoAMC
           AQICAQIwDQYJKoZIhvcNAQEFBQAwgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlD
           YXRhbG9uaWExEjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMwEQYD
           VQQLEwpDb25zdWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0BCQEW
           EmpjYXN0ZWxsYXJAdW9jLmVkdTAeFw0wNTEwMDQxMTM4MjZaFw0wNjEwMDQxMTM4
           MjZaMIGSMQswCQYDVQQGEwJFUzESMBAGA1UECBMJQ2F0YWx1bnlhMSgwJgYDVQQK
           Ex9Vbml2ZXJzaXRhdCBPYmVydGEgZGUgQ2F0YWx1bnlhMRAwDgYDVQQLEwdBbHVt
           bmVzMRAwDgYDVQQDEwdKdWdhZG9yMSEwHwYJKoZIhvcNAQkBFhJqY2FzdGVsbGFy
           QHVvYy5lZHUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAN3E2Ko7EX0MmxlI
           HlQ1+5BOmUYxccyl7tk2l4vidS35bGEKC+nSM06dXCM8azOQCC9H3eBLyCUetraq
           kliD/xqzdTdMaQ2jIn2eky8Rj1CYRAGuI05GkYZo/kircvg/IgvcdgNFt9uuFxOe
           D/uI5Qb9prgMjfmGXGMo4bdyJFPBAgMBAAGjggFvMIIBazAJBgNVHRMEAjAAMBEG
           CWCGSAGG+EIBAQQEAwIFoDALBgNVHQ8EBAMCBeAwMQYJYIZIAYb4QgENBCQWIlNl
           Z3VyZXRhdCBlbiBYYXJ4ZXMgZGUgQ29tcHV0YWRvcnMwHQYDVR0OBBYEFDJOtz87
           g7Hzq3RwzvWgyIe0Lf4IMIHBBgNVHSMEgbkwgbaAFNJneRhyp6RTrww1H3s294D9
           ha2xoYGSpIGPMIGMMQswCQYDVQQGEwJFUzESMBAGA1UECBMJQ2F0YWxvbmlhMRIw
           EAYDVQQHEwlUYXJyYWdvbmExDDAKBgNVBAoTA1VPQzETMBEGA1UECxMKQ29uc3Vs
           dG9yczEPMA0GA1UEAxMGQ0EgUEZDMSEwHwYJKoZIhvcNAQkBFhJqY2FzdGVsbGFy
           QHVvYy5lZHWCCQCrw7KQLraVODAdBgNVHREEFjAUgRJqY2FzdGVsbGFyQHVvYy5l
           ZHUwCQYDVR0SBAIwADANBgkqhkiG9w0BAQUFAAOCAQEAHm1fA4CCwuICwULPzA4I
           pV25LNu5o/HGqo4cfOBfDsh6WaaPq5fsMrQYO57y+fhn2mqt7qz61cEDYgpUq7aE
           0sX3ChHMH2WHv59Rx3L7oakabkI1e0dOSGrQ4CyUKb75pBLb1ZdOo3ubAtDdm8+m
           J9BozZL1xVckZsiAmNhVGGPQhhAwhlOYrkAbQsHW3tLBRVfCI36IE1eanASgHgvd
           NJiHQkO+b2BPZM/N6k5ZaeF3osfaklkPi52muDConAhZXdasSZg1naUR4E2x9K4a
           ow/ZwGRwJ1W6PsChbRY73bNRJIjnyG8RxSZLJK+R8iytkZC0bwVkII7YB0Zc0rF3
           PTCCBJIwggN6oAMCAQICCQCrw7KQLraVODANBgkqhkiG9w0BAQUFADCBjDELMAkG
```

```
          A1UEBhMCRVMxEjAQBgNVBAgTCUNhdGFsb25pYTESMBAGA1UEBxMJVGFycmFnb25h
          MQwwCgYDVQQKEwNVT0MxEzARBgNVBAsTCkNvbnN1bHRvcnMxDzANBgNVBAMTBkNB
          IFBGQzEhMB8GCSqGSIb3DQEJARYSamNhc3RlbGxhckB1b2MuZWR1MB4XDTA1MTAw
          NDEwNTUxMloXDTA2MTAwNDEwNTUxMlowgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQI
          EwlDYXRhbG9uaWExEjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMw
          EQYDVQQLEwpDb25zdWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0B
          CQEWEmpjYXN0ZWxsYXJAdW9jLmVkdTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
          AQoCggEBALTjkFuSne+TJBFaZL0qDz2889Rx6ErcWLtCK0xz+UPuB9yzd2qHhisR
          jY+EkRnlsXb3p2/1leoTYUGu59bgiIcjMVMNgT/eFRkl9X0oEGZEXHy/4US+w2a4
          PtGmQ7wEyMcSEpkjyfS+GKreynw9VVyWFwAQ9umUVZ28hPrXFt6tbUziYWRB0+Ar
          kGFL8e4zYudtzhh1FMFOvW8WOA2VK5zW596ChXbNQ6+i4OZgYmwWPT9f8x2jk+Pf
          5OGDIyjHzBU4xJ6409JgHDsWtm/5SJd+9wC5GYT5K6oNikR718XsV74svAx8bfA1
          1M3nLT+jdQ7VuFrrCeNhkpTtlqyjcDMCAwEAAaOB9DCB8TAdBgNVHQ4EFgQU0md5
          GHKnpFOvDDUfezb3gP2FrbEwgcEGA1UdIwSBuTCBtoAU0md5GHKnpFOvDDUfezb3
          gP2FrbGhgZKkgY8wgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlDYXRhbG9uaWEx
          EjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMwEQYDVQQLEwpDb25z
          dWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0BCQEWEmpjYXN0ZWxs
          YXJAdW9jLmVkdYIJAKvDspAutpU4MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEF
          BQADggEBAGdbzQcIddybkIqsAhm+vptcjGHv2ae9aBhQc6PQNJF/IBSuYQVh5Q78
          mTROl3cTFfkbl2/LaFrx0Ejdb0s69mbRrHMM+VU49SZiJLV+f/A/Pa0xHPTTfAr5
          rDmOBVNO+GFisAJkmZnu+Wd43w/1fnRIxGsf4GP7s+8Sv8FTX9TiQkJicalKPZKl
          9TyH5BOmrPIH2FURov92wQ2/7vbi/vIYDQeiDfoo6mE0PvOdGJvuQbFOt1xSrIHj
          g1DGgv5d+IEjA++Ry+kw3kuX8t82gsW0QjsnA8dzEv8FWT6apGwoZGivBWbgQJ2+
          F3cRQy5iWMRkOArz/Co++m/3QQ6bZHExggE5MIIBNQIBATCBkjCBjDELMAkGA1UE
          BhMCRVMxEjAQBgNVBAgTCUNhdGFsb25pYTESMBAGA1UEBxMJVGFycmFnb25hMQww
          CgYDVQQKEwNVT0MxEzARBgNVBAsTCkNvbnN1bHRvcnMxDzANBgNVBAMTBkNBIFBG
          QzEhMB8GCSqGSIb3DQEJARYSamNhc3RlbGxhckB1b2MuZWR1AgECMAkGBSsOAwIa
          BQAwDQYJKoZIhvcNAQEBBQAEgYCrZCFBWzzs+dgpgbPN7LDwMbPu1ewKRIxz9ojq
          82fpxq6COyl3r8b9LKNXzv6JLlAjmSf9dGc0nILbPeNZu+TRCjowWSwl3mpheH3L
          FQj2nRgX/1Bb7/8ChonsXiWxnfaAQIa302JUsArYNG7QLHH4Rw5Gi3/3CNoMb0vp
          m3B6mw==
```


```
    </Signatura>
  <NouDiposit>
    <IdentificadorPartida>
      <IdentificadorJoc>BlackJack</IdentificadorJoc>
      <Aleatori>168502483</Aleatori>
      <InstantActual>2005-10-26 22:13:56</InstantActual>
      <NumeroPartida>145</NumeroPartida>
    </IdentificadorPartida>
    <Valor>10.0</Valor>
  </NouDiposit>
     <Rebut>
```


```
         MIIKfQIBATELMAkGBSsOAwIaBQAwCwYJKoZIhvcNAQcBoIIJHzCCBIUwggNtoAMC
         AQICAQEwDQYJKoZIhvcNAQEFBQAwgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlD
         YXRhbG9uaWExEjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMwEQYD
         VQQLEwpDb25zdWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0BCQEW
         EmpjYXN0ZWxsYXJAdW9jLmVkdTAeFw0wNTEwMDQxMTM4MDlaFw0wNjEwMDQxMTM4
         MDlaMIGQMQswCQYDVQQGEwJFUzESMBAGA1UECBMJQ2F0YWx1bnlhMSgwJgYDVQQK
         Ex9Vbml2ZXJzaXRhdCBPYmVydGEgZGUgQ2F0YWx1bnlhMRAwDgYDVQQLEwdBbHVt
         bmVzMQ8wDQYDVQQDEwZHZXN0b3IxIDAeBgkqhkiG9w0BCQEWEWpjYXN0ZWxsYUB1
         b2MuZWR1MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDmtqFKeGB2zGSzQmu5
         m38fZY1Rc8AS8r/QacKxyLNLHxBnPylE+d2BjmnDoSJHlYuV7qkoDaCmHZqRzM22
         kZbdBgpi1akpkStXsDgNqxDBQ5Cz9NvYTqaeUSa/owuHGcsd5VlOwQkGqhQdY9Tv
         gN43fWwR/j8ASF0wQ1nlnF8l+wIDAQABo4IBbjCCAWowCQYDVR0TBAIwADARBglg
         hkgBhvhCAQEEBAMCBaAwCwYDVR0PBAQDAgXgMDEGCWCGSAGG+EIBDQQkFiJTZWd1
         cmV0YXQgZW4gWGFyeGVzIGRlIENvbXB1dGFkb3JzMB0GA1UdDgQWBBQuRbiGe27q
         8EiCxRFYULGz/uVFHTCBwQYDVR0jBIG5MIG2gBTSZ3kYcqekU68MNR97NveA/YWt
         saGBkqSBjzCBjDELMAkGA1UEBhMCRVMxEjAQBgNVBAgTCUNhdGFsb25pYTESMBAG
         A1UEBxMJVGFycmFnb25hMQwwCgYDVQQKEwNVT0MxEzARBgNVBAsTCkNvbnN1bHRv
         cnMxDzANBgNVBAMTBkNBIFBGQzEhMB8GCSqGSIb3DQEJARYSamNhc3RlbGxhckB1
         b2MuZWR1ggkAq8OykC62lTgwHAYDVR0RBBUwE4ERamNhc3RlbGxhQHVvYy5lZHUw
         CQYDVR0SBAIwADANBgkqhkiG9w0BAQUFAAOCAQEAnMZN6KaeEf75VPZtwMbn0dv/
         FKaaHlgbRlIDzbrGGq0aclfNf+3mYv/mR3BcEbn8myJFqDdoU6yzFpYGFr4+ZszC
         kMkyx2GF3gUWqQ2pw/VEqAvj1adoQNR0i9zpdGcFUXO9BOWxprLLgiPP1ME9ulIB
         WgtHii/f9VKitisu0BWGY/4fagfPgGNYyD7AhVNT1AejTPuLCMhSD5XQam4tKvUJ
         6NTWPhcH5uZ6BykeFFOnRew4Y8lCstzJ9He+FQ9U6+lhIt4LkEkhauZcF4o2XtbR
         3EfiU4W2hzGhekGXvxvVgP28gdWXE6pp/hCTY+45b/Fxq7HwoCPPRnkBqMIGkDCC
         BJIwggN6oAMCAQICCQCrw7KQLraVODANBgkqhkiG9w0BAQUFADCBjDELMAkGA1UE
         BhMCRVMxEjAQBgNVBAgTCUNhdGFsb25pYTESMBAGA1UEBxMJVGFycmFnb25hMQww
         CgYDVQQKEwNVT0MxEzARBgNVBAsTCkNvbnN1bHRvcnMxDzANBgNVBAMTBkNBIFBG
         QzEhMB8GCSqGSIb3DQEJARYSamNhc3RlbGxhckB1b2MuZWR1MB4XDTA1MTAwNDEw
```

```
          NTUxMloXDTA2MTAwNDEwNTUxMlowgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlD
          YXRhbG9uaWExEjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMwEQYD
          VQQLEwpDb25zdWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0BCQEW
          EmpjYXN0ZWxsYXJAdW9jLmVkdTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
          ggEBALTjkFuSne+TJBFaZL0qDz2889Rx6ErcWLtCK0xz+UPuB9yzd2qHhisRjY+E
          kRnlsXb3p2/1leoTYUGu59bgiIcjMVMNgT/eFRkl9X0oEGZEXHy/4US+w2a4PtGm
          Q7wEyMcSEpkjyfS+GKreynw9VVyWFwAQ9umUVZ28hPrXFt6tbUziYWRB0+ArkGFL
          8e4zYudtzhh1FMFOvW8WOA2VK5zW596ChXbNQ6+i4OZgYmwWPT9f8x2jk+Pf5OGD
          IyjHzBU4xJ6409JgHDsWtm/5SJd+9wC5GYT5K6oNikR718XsV74svAx8bfA11M3n
          LT+jdQ7VuFrrCeNhkpTtlqyjcDMCAwEAAaOB9DCB8TAdBgNVHQ4EFgQU0md5GHKn
          pFOvDDUfezb3gP2FrbEwgcEGA1UdIwSBuTCBtoAU0md5GHKnpFOvDDUfezb3gP2F
          rbGhgZKkgY8wgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlDYXRhbG9uaWExEjAQ
          BgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMwEQYDVQQLEwpDb25zdWx0
          b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0BCQEWEmpjYXN0ZWxsYXJA
          dW9jLmVkdYIJAKvDspAutpU4MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQAD
          ggEBAGdbzQcIddybkIqsAhm+vptcjGHv2ae9aBhQc6PQNJF/IBSuYQVh5Q78mTRO
          l3cTFfkbl2/LaFrx0Ejdb0s69mbRrHMM+VU49SZiJLV+f/A/Pa0xHPTTfAr5rDmO
          BVNO+GFisAJkmZnu+Wd43w/1fnRIxGsf4GP7s+8Sv8FTX9TiQkJicalKPZKl9TyH
          5BOmrPIH2FURov92wQ2/7vbi/vIYDQeiDfoo6mE0PvOdGJvuQbFOt1xSrIHjg1DG
          gv5d+IEjA++Ry+kw3kuX8t82gsW0QjsnA8dzEv8FWT6apGwoZGivBWbgQJ2+F3cR
          Qy5iWMRkOArz/Co++m/3QQ6bZHExggE5MIIBNQIBATCBkjCBjDELMAkGA1UEBhMC
          RVMxEjAQBgNVBAgTCUNhdGFsb25pYTESMBAGA1UEBxMJVGFycmFnb25hMQwwCgYD
          VQQKEwNVT0MxEzARBgNVBAsTCkNvbnN1bHRvcnMxDzANBgNVBAMTBkNBIFBGQzEh
          MB8GCSqGSIb3DQEJARYSamNhc3RlbGxhckB1b2MuZWR1AgEBMAkGBSsOAwIaBQAw
          DQYJKoZIhvcNAQEBBQAEgYCZCRqJxp2+sC7bvh4/A/8gZ6JSwZoougvw8IfX4ofE
          IN4EG1VTYPoBTMRqMvgtNMhV3ClawTLcs7g0etuor5FKWQLjYe7PMRHb2G+JwT4M
          p1ZBQxfWBSjArVI9IBrBDDJ/grIU1L0Jy0q0bvXBi+MfCDFZDXbdxKvcgSmYBbM7hw==
    </Rebut>
</IncrementDiposit>
```

Fer una aposta.

Document XML per l'intercanvi d'informació que es produeix al fer una aposta.

Esquema:

```
<Aposta>
  <IdentificadorAposta>
    <IdentificadorPartida>
      <IdentificadorJoc>      </IdentificadorJoc>
      <Aleatori>              </Aleatori>
      <InstantActual>         </InstantActual>
      <NumeroPartida>         </NumeroPartida>
    </IdentificadorPartida>
    <Aleatori>                </Aleatori>
    <InstantActual>           </InstantActual>
    <Quantitat>               </Quantitat>
    <Concepte>                </Concepte>
  </IdentificadorAposta>
  <Signatura>                 </Signatura>
  <RebutAposta>               </RebutAposta>
  <CreditDisponible>          </CreditDisponible>
  <RebutCreditDisponible>     </RebutCreditDisponible>
</Aposta>
```

Exemple:

```
<Aposta>
  <IdentificadorAposta>
    <IdentificadorPartida>
      <IdentificadorJoc>BlackJack</IdentificadorJoc>
      <Aleatori>168502483</Aleatori>
      <InstantActual>2005-10-26 22:13:56</InstantActual>
      <NumeroPartida>145</NumeroPartida>
    </IdentificadorPartida>
    <Aleatori>326291767</Aleatori>
```

```
    <InstantActual>2005-10-29 19:40:51</InstantActual>
    <Quantitat>50.0</Quantitat>
    <Concepte>Concepte</Concepte>
  </IdentificadorAposta>
  <Signatura>
        MIIKgAIBATELMAkGBSsOAwIaBQAwCwYJKoZIhvcNAQcBoIIJIjCCBIgwggNwoAMC
        AQICAQIwDQYJKoZIhvcNAQEFBQAwgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlD
        YXRhbG9uaWExEjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMwEQYD
        VQQLEwpDb25zdWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0BCQEW
        EmpjYXN0ZWxsYXJAdW9jLmVkdTAeFw0wNTEwMDQxMTM4MjZaFw0wNjEwMDQxMTM4
        MjZaMIGSMQswCQYDVQQGEwJFUzESMBAGA1UECBMJQ2F0YWx1bnlhMSgwJgYDVQQK
        Ex9Vbml2ZXJzaXRhdCBPYmVydGEgZGUgQ2F0YWx1bnlhMRAwDgYDVQQLEwdBbHVt
        bmVzMRAwDgYDVQQDEwdKdWdhZG9yMSEwHwYJKoZIhvcNAQkBFhJqY2FzdGVsbGFy
        QHVvYy5lZHUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAN3E2Ko7EX0MmxlI
        HlQ1+5BOmUYxccyl7tk2l4vidS35bGEKC+nSM06dXCM8azOQCC9H3eBLyCUetraq
        kliD/xqzdTdMaQ2jIn2eky8Rj1CYRAGuI05GkYZo/kircvg/IgvcdgNFt9uuFxOe
        D/uI5Qb9prgMjfmGXGMo4bdyJFPBAgMBAAGjggFvMIIBazAJBgNVHRMEAjAAMBEG
        CWCGSAGG+EIBAQQEAwIFoDALBgNVHQ8EBAMCBeAwMQYJYIZIAYb4QgENBCQWIlNl
        Z3VyZXRhdCBlbiBYYXJ4ZXMgZGUgQ29tcHV0YWRvcnMwHQYDVR0OBBYEFDJOtz87
        g7Hzq3RwzvWgyIe0Lf4IMIHBBgNVHSMEgbkwgbaAFNJneRhyp6RTrww1H3s294D9
        ha2xoYGSpIGPMIGMMQswCQYDVQQGEwJFUzESMBAGA1UECBMJQ2F0YWxvbmlhMRIw
        EAYDVQQHEwlUYXJyYWdvbmExDDAKBgNVBAoTA1VPQzETMBEGA1UECxMKQ29uc3Vs
        dG9yczEPMA0GA1UEAxMGQ0EgUEZDMSEwHwYJKoZIhvcNAQkBFhJqY2FzdGVsbGFy
        QHVvYy5lZHWCCQCrw7KQLraVODAdBgNVHREEFjAUgRJqY2FzdGVsbGFyQHVvYy5l
        ZHUwCQYDVR0SBAIwADANBgkqhkiG9w0BAQUFAAOCAQEAHm1fA4CCwuICwULPzA4I
        pV25LNu5o/HGqo4cfOBfDsh6WaaPq5fsMrQYO57y+fhn2mqt7qz61cEDYgpUq7aE
        0sX3ChHMH2WHv59Rx3L7oakabkI1e0dOSGrQ4CyUKb75pBLb1ZdOo3ubAtDdm8+m
        J9BozZL1xVckZsiAmNhVGGPQhhAwhlOYrkAbQsHW3tLBRVfCI36IE1eanASgHgvd
        NJiHQkO+b2BPZM/N6k5ZaeF3osfaklkPi52muDConAhZXdasSZg1naUR4E2x9K4a
        ow/ZwGRwJ1W6PsChbRY73bNRJIjnyG8RxSZLJK+R8iytkZC0bwVkII7YB0Zc0rF3
        PTCCBJIwggN6oAMCAQICCQCrw7KQLraVODANBgkqhkiG9w0BAQUFADCBjDELMAkG
        A1UEBhMCRVMxEjAQBgNVBAgTCUNhdGFsb25pYTESMBAGA1UEBxMJVGFycmFnb25h
        MQwwCgYDVQQKEwNVT0MxEzARBgNVBAsTCkNvbnN1bHRvcnMxDzANBgNVBAMTBkNB
        IFBGQzEhMB8GCSqGSIb3DQEJARYSamNhc3RlbGxhckB1b2MuZWR1MB4XDTA1MTAw
        NDEwNTUxMloXDTA2MTAwNDEwNTUxMlowgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQI
        EwlDYXRhbG9uaWExEjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMw
        EQYDVQQLEwpDb25zdWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0B
        CQEWEmpjYXN0ZWxsYXJAdW9jLmVkdTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
        AQoCggEBALTjkFuSne+TJBFaZL0qDz2889Rx6ErcWLtCK0xz+UPuB9yzd2qHhisR
        jY+EkRnlsXb3p2/1leoTYUGu59bgiIcjMVMNgT/eFRkl9X0oEGZEXHy/4US+w2a4
        PtGmQ7wEyMcSEpkjyfS+GKreynw9VVyWFwAQ9umUVZ28hPrXFt6tbUziYWRB0+Ar
        kGFL8e4zYudtzhh1FMFOvW8WOA2VK5zW596ChXbNQ6+i4OZgYmwWPT9f8x2jk+Pf
        5OGDIyjHzBU4xJ6409JgHDsWtm/5SJd+9wC5GYT5K6oNikR718XsV74svAx8bfA1
        1M3nLT+jdQ7VuFrrCeNhkpTtlqyjcDMCAwEAAaOB9DCB8TAdBgNVHQ4EFgQU0md5
        GHKnpFOvDDUfezb3gP2FrbEwgcEGA1UdIwSBuTCBtoAU0md5GHKnpFOvDDUfezb3
        gP2FrbGhgZKkgY8wgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlDYXRhbG9uaWEx
        EjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMwEQYDVQQLEwpDb25z
        dWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0BCQEWEmpjYXN0ZWxs
        YXJAdW9jLmVkdYIJAKvDspAutpU4MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEF
        BQADggEBAGdbzQcIddybkIqsAhm+vptcjGHv2ae9aBhQc6PQNJF/IBSuYQVh5Q78
        mTROl3cTFfkbl2/LaFrx0Ejdb0s69mbRrHMM+VU49SZiJLV+f/A/Pa0xHPTTfAr5
        rDmOBVNO+GFisAJkmZnu+Wd43w/1fnRIxGsf4GP7s+8Sv8FTX9TiQkJicalKPZKl
        9TyH5BOmrPIH2FURov92wQ2/7vbi/vIYDQeiDfoo6mE0PvOdGJvuQbFOt1xSrIHj
        g1DGgv5d+IEjA++Ry+kw3kuX8t82gsW0QjsnA8dzEv8FWT6apGwoZGivBWbgQJ2+
        F3cRQy5iWMRkOArz/Co++m/3QQ6bZHExggE5MIIBNQIBATCBkjCBjDELMAkGA1UE
        BhMCRVMxEjAQBgNVBAgTCUNhdGFsb25pYTESMBAGA1UEBxMJVGFycmFnb25hMQww
        CgYDVQQKEwNVT0MxEzARBgNVBAsTCkNvbnN1bHRvcnMxDzANBgNVBAMTBkNBIFBG
        QzEhMB8GCSqGSIb3DQEJARYSamNhc3RlbGxhckB1b2MuZWR1AgECMAkGBSsOAwIa
        BQAwDQYJKoZIhvcNAQEBBQAEgYBREbLdZeNzpNXQ9SmvYwJtS30jE2TM/uTYf/Sb
        /tA/rUL/h/tOwz7QY+Zj9MHI+9itGJK7dksGhbaoqNayPKcvGCB6qqxrcVNcCq+3
        24ZmaiodSYI0GJt+ajjX8QGdKieTGh4B5NlsOb6Peq/+aHL/ffqP/ONLXhxDh01s
        Szijqw==
  </Signatura>
  <RebutAposta>
        MIIKfQIBATELMAkGBSsOAwIaBQAwCwYJKoZIhvcNAQcBoIIJHzCCBIUwggNtoAMC
        AQICAQEwDQYJKoZIhvcNAQEFBQAwgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlD
        YXRhbG9uaWExEjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMwEQYD
        VQQLEwpDb25zdWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0BCQEW
        EmpjYXN0ZWxsYXJAdW9jLmVkdTAeFw0wNTEwMDQxMTM4MDlaFw0wNjEwMDQxMTM4
        MDlaMIGQMQswCQYDVQQGEwJFUzESMBAGA1UECBMJQ2F0YWx1bnlhMSgwJgYDVQQK
        Ex9Vbml2ZXJzaXRhdCBPYmVydGEgZGUgQ2F0YWx1bnlhMRAwDgYDVQQLEwdBbHVt
```

```
      bmVzMQ8wDQYDVQQDEwZHZXN0b3IxIDAeBgkqhkiG9w0BCQEWEWpjYXN0ZWxsYUB1
      b2MuZWR1MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDmtqFKeGB2zGSzQmu5
      m38fZY1Rc8AS8r/QacKxyLNLHxBnPylE+d2BjmnDoSJHlYuV7qkoDaCmHZqRzM22
      kZbdBgpi1akpkStXsDgNqxDBQ5Cz9NvYTqaeUSa/owuHGcsd5VlOwQkGqhQdY9Tv
      gN43fWwR/j8ASF0wQ1nlnF8l+wIDAQABo4IBbjCCAWowCQYDVR0TBAIwADARBglg
      hkgBhvhCAQEEBAMCBaAwCwYDVR0PBAQDAgXgMDEGCWCGSAGG+EIBDQQkFiJTZWd1
      cmV0YXQgZW4gWGFyeGVzIGRlIENvbXB1dGFkb3JzMB0GA1UdDgQWBBQuRbiGe27q
      8EiCxRFYULGz/uVFHTCBwQYDVR0jBIG5MIG2gBTSZ3kYcqekU68MNR97NveA/YWt
      saGBkqSBjzCBjDELMAkGA1UEBhMCRVMxEjAQBgNVBAgTCUNhdGFsb25pYTESMBAG
      A1UEBxMJVGFycmFnb25hMQwwCgYDVQQKEwNVT0MxEzARBgNVBAsTCkNvbnN1bHRv
      cnMxDzANBgNVBAMTBkNBIFBGQzEhMB8GCSqGSIb3DQEJARYSamNhc3RlbGxhckB1
      b2MuZWR1ggkAq8OykC62lTgwHAYDVR0RBBUwE4ERamNhc3RlbGxhQHVvYy5lZHUw
      CQYDVR0SBAIwADANBgkqhkiG9w0BAQUFAAOCAQEAnMZN6KaeEf75VPZtwMbn0dv/
      FKaaHlgbRlIDzbrGGq0aclfNf+3mYv/mR3BcEbn8myJFqDdoU6yzFpYGFr4+ZszC
      kMkyx2GF3gUWqQ2pw/VEqAvj1adoQNR0i9zpdGcFUXO9BOWxprLLgiPP1ME9ulIB
      WgtHii/f9VKitisu0BWGY/4fagfPgGNYyD7AhVNT1AejTPuLCMhSD5XQam4tKvUJ
      6NTWPhcH5uZ6BykeFFOnRew4Y8lCstzJ9He+FQ9U6+lhIt4LkEkhauZcF4o2XtbR
      3EfiU4W2hzGhekGXvxvVgP28gdWXE6pp/hCTY+45b/Fxq7HwoCPPRnkBqMIGkDCC
      BJIwggN6oAMCAQICCQCrw7KQLraVODANBgkqhkiG9w0BAQUFADCBjDELMAkGA1UE
      BhMCRVMxEjAQBgNVBAgTCUNhdGFsb25pYTESMBAGA1UEBxMJVGFycmFnb25hMQww
      CgYDVQQKEwNVT0MxEzARBgNVBAsTCkNvbnN1bHRvcnMxDzANBgNVBAMTBkNBIFBG
      QzEhMB8GCSqGSIb3DQEJARYSamNhc3RlbGxhckB1b2MuZWR1MB4XDTA1MTAwNDEw
      NTUxMloXDTA2MTAwNDEwNTUxMlowgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlD
      YXRhbG9uaWExEjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMwEQYD
      VQQLEwpDb25zdWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0BCQEW
      EmpjYXN0ZWxsYXJAdW9jLmVkdTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
      ggEBALTjkFuSne+TJBFaZL0qDz2889Rx6ErcWLtCK0xz+UPuB9yzd2qHhisRjY+E
      kRnlsXb3p2/1leoTYUGu59bgiIcjMVMNgT/eFRkl9X0oEGZEXHy/4US+w2a4PtGm
      Q7wEyMcSEpkjyfS+GKreynw9VVyWFwAQ9umUVZ28hPrXFt6tbUziYWRB0+ArkGFL
      8e4zYudtzhh1FMFOvW8WOA2VK5zW596ChXbNQ6+i4OZgYmwWPT9f8x2jk+Pf5OGD
      IyjHzBU4xJ6409JgHDsWtm/5SJd+9wC5GYT5K6oNikR718XsV74svAx8bfA11M3n
      LT+jdQ7VuFrrCeNhkpTtlqyjcDMCAwEAAaOB9DCB8TAdBgNVHQ4EFgQU0md5GHKn
      pFOvDDUfezb3gP2FrbEwgcEGA1UdIwSBuTCBtoAU0md5GHKnpFOvDDUfezb3gP2F
      rbGhgZKkgY8wgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlDYXRhbG9uaWExEjAQ
      BgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMwEQYDVQQLEwpDb25zdWx0
      b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0BCQEWEmpjYXN0ZWxsYXJA
      dW9jLmVkdYIJAKvDspAutpU4MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQAD
      ggEBAGdbzQcIddybkIqsAhm+vptcjGHv2ae9aBhQc6PQNJF/IBSuYQVh5Q78mTRO
      l3cTFfkbl2/LaFrx0Ejdb0s69mbRrHMM+VU49SZiJLV+f/A/Pa0xHPTTfAr5rDmO
      BVNO+GFisAJkmZnu+Wd43w/1fnRIxGsf4GP7s+8Sv8FTX9TiQkJicalKPZKl9TyH
      5BOmrPIH2FURov92wQ2/7vbi/vIYDQeiDfoo6mE0PvOdGJvuQbFOt1xSrIHjg1DG
      gv5d+IEjA++Ry+kw3kuX8t82gsW0QjsnA8dzEv8FWT6apGwoZGivBWbgQJ2+F3cR
      Qy5iWMRkOArz/Co++m/3QQ6bZHExggE5MIIBNQIBATCBkjCBjDELMAkGA1UEBhMC
      RVMxEjAQBgNVBAgTCUNhdGFsb25pYTESMBAGA1UEBxMJVGFycmFnb25hMQwwCgYD
      VQQKEwNVT0MxEzARBgNVBAsTCkNvbnN1bHRvcnMxDzANBgNVBAMTBkNBIFBGQzEh
      MB8GCSqGSIb3DQEJARYSamNhc3RlbGxhckB1b2MuZWR1AgEBMAkGBSsOAwIaBQAw
      DQYJKoZIhvcNAQEBBQAEgYBXm/tLn/dmGaqDesgY1F6lO7TLUFwkb7fG2hrhwH9l
      IwbVeuX+zirVash/XAJhX9+B3k/OFIfwQRiqwIXSMXyaDtMhx92vpju5avjZXpkK
      Q1NectIkTDIR5hG89Rmx+vvKP6ivq1R3wOtHQPqg4H6hEj7NgiGeMgCyv01e+cy/9g==
</RebutAposta>
<CreditDisponible>300.0</CreditDisponible>
<RebutCreditDisponible>
      MIIKfQIBATELMAkGBSsOAwIaBQAwCwYJKoZIhvcNAQcBoIIJHzCCBIUwggNtoAMC
      AQICAQEwDQYJKoZIhvcNAQEFBQAwgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlD
      YXRhbG9uaWExEjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMwEQYD
      VQQLEwpDb25zdWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0BCQEW
      EmpjYXN0ZWxsYXJAdW9jLmVkdTAeFw0wNTEwMDQxMTM4MDlaFw0wNjEwMDQxMTM4
      MDlaMIGQMQswCQYDVQQGEwJFUzESMBAGA1UECBMJQ2F0YWx1bnlhMSgwJgYDVQQK
      Ex9Vbml2ZXJzaXRhdCBPYmVydGEgZGUgQ2F0YWx1bnlhMRAwDgYDVQQLEwdBbHVt
      bmVzMQ8wDQYDVQQDEwZHZXN0b3IxIDAeBgkqhkiG9w0BCQEWEWpjYXN0ZWxsYUB1
      b2MuZWR1MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDmtqFKeGB2zGSzQmu5
      m38fZY1Rc8AS8r/QacKxyLNLHxBnPylE+d2BjmnDoSJHlYuV7qkoDaCmHZqRzM22
      kZbdBgpi1akpkStXsDgNqxDBQ5Cz9NvYTqaeUSa/owuHGcsd5VlOwQkGqhQdY9Tv
      gN43fWwR/j8ASF0wQ1nlnF8l+wIDAQABo4IBbjCCAWowCQYDVR0TBAIwADARBglg
      hkgBhvhCAQEEBAMCBaAwCwYDVR0PBAQDAgXgMDEGCWCGSAGG+EIBDQQkFiJTZWd1
      cmV0YXQgZW4gWGFyeGVzIGRlIENvbXB1dGFkb3JzMB0GA1UdDgQWBBQuRbiGe27q
      8EiCxRFYULGz/uVFHTCBwQYDVR0jBIG5MIG2gBTSZ3kYcqekU68MNR97NveA/YWt
      saGBkqSBjzCBjDELMAkGA1UEBhMCRVMxEjAQBgNVBAgTCUNhdGFsb25pYTESMBAG
      A1UEBxMJVGFycmFnb25hMQwwCgYDVQQKEwNVT0MxEzARBgNVBAsTCkNvbnN1bHRv
      cnMxDzANBgNVBAMTBkNBIFBGQzEhMB8GCSqGSIb3DQEJARYSamNhc3RlbGxhckB1
      b2MuZWR1ggkAq8OykC62lTgwHAYDVR0RBBUwE4ERamNhc3RlbGxhQHVvYy5lZHUw
```

```
        CQYDVR0SBAIwADANBgkqhkiG9w0BAQUFAAOCAQEAnMZN6KaeEf75VPZtwMbn0dv/
        FKaaHlgbRlIDzbrGGq0aclfNf+3mYv/mR3BcEbn8myJFqDdoU6yzFpYGFr4+ZszC
        kMkyx2GF3gUWqQ2pw/VEqAvj1adoQNR0i9zpdGcFUXO9BOWxprLLgiPP1ME9ulIB
        WgtHii/f9VKitisu0BWGY/4fagfPgGNYyD7AhVNT1AejTPuLCMhSD5XQam4tKvUJ
        6NTWPhcH5uZ6BykeFFOnRew4Y8lCstzJ9He+FQ9U6+lhIt4LkEkhauZcF4o2XtbR
        3EfiU4W2hzGhekGXvxvVgP28gdWXE6pp/hCTY+45b/Fxq7HwoCPPRnkBqMIGkDCC
        BJIwggN6oAMCAQICCQCrw7KQLraVODANBgkqhkiG9w0BAQUFADCBjDELMAkGA1UE
        BhMCRVMxEjAQBgNVBAgTCUNhdGFsb25pYTESMBAGA1UEBxMJVGFycmFnb25hMQww
        CgYDVQQKEwNVT0MxEzARBgNVBAsTCkNvbnN1bHRvcnMxDzANBgNVBAMTBkNBIFBG
        QzEhMB8GCSqGSIb3DQEJARYSamNhc3RlbGxhckB1b2MuZWR1MB4XDTA1MTAwNDEw
        NTUxMloXDTA2MTAwNDEwNTUxMlowgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlD
        YXRhbG9uaWExEjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMwEQYD
        VQQLEwpDb25zdWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0BCQEW
        EmpjYXN0ZWxsYXJAdW9jLmVkdTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
        ggEBALTjkFuSne+TJBFaZL0qDz2889Rx6ErcWLtCK0xz+UPuB9yzd2qHhisRjY+E
        kRnlsXb3p2/1leoTYUGu59bgiIcjMVMNgT/eFRkl9X0oEGZEXHy/4US+w2a4PtGm
        Q7wEyMcSEpkjyfS+GKreynw9VVyWFwAQ9umUVZ28hPrXFt6tbUziYWRB0+ArkGFL
        8e4zYudtzhh1FMFOvW8WOA2VK5zW596ChXbNQ6+i4OZgYmwWPT9f8x2jk+Pf5OGD
        IyjHzBU4xJ6409JgHDsWtm/5SJd+9wC5GYT5K6oNikR718XsV74svAx8bfA11M3n
        LT+jdQ7VuFrrCeNhkpTtlqyjcDMCAwEAAaOB9DCB8TAdBgNVHQ4EFgQU0md5GHKn
        pFOvDDUfezb3gP2FrbEwgcEGA1UdIwSBuTCBtoAU0md5GHKnpFOvDDUfezb3gP2F
        rbGhgZKkgY8wgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlDYXRhbG9uaWExEjAQ
        BgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMwEQYDVQQLEwpDb25zdWx0
        b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0BCQEWEmpjYXN0ZWxsYXJA
        dW9jLmVkdYIJAKvDspAutpU4MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQAD
        ggEBAGdbzQcIddybkIqsAhm+vptcjGHv2ae9aBhQc6PQNJF/IBSuYQVh5Q78mTRO
        l3cTFfkbl2/LaFrx0Ejdb0s69mbRrHMM+VU49SZiJLV+f/A/Pa0xHPTTfAr5rDmO
        BVNO+GFisAJkmZnu+Wd43w/1fnRIxGsf4GP7s+8Sv8FTX9TiQkJicalKPZKl9TyH
        5BOmrPIH2FURov92wQ2/7vbi/vIYDQeiDfoo6mE0PvOdGJvuQbFOt1xSrIHjg1DG
        gv5d+IEjA++Ry+kw3kuX8t82gsW0QjsnA8dzEv8FWT6apGwoZGivBWbgQJ2+F3cR
        Qy5iWMRkOArz/Co++m/3QQ6bZHExggE5MIIBNQIBATCBkjCBjDELMAkGA1UEBhMC
        RVMxEjAQBgNVBAgTCUNhdGFsb25pYTESMBAGA1UEBxMJVGFycmFnb25hMQwwCgYD
        VQQKEwNVT0MxEzARBgNVBAsTCkNvbnN1bHRvcnMxDzANBgNVBAMTBkNBIFBGQzEh
        MB8GCSqGSIb3DQEJARYSamNhc3RlbGxhckB1b2MuZWR1AgEBMAkGBSsOAwIaBQAw
        DQYJKoZIhvcNAQEBBQAEgYAxRlnv84YpbJ5APBpeEUuWLPOXrSlcvmWFrjtwKf+8
        aCQWDxWK5O897UGoJVQnevKyrywvci50v4fcUpFBvgrDzssPBICXiufmmTyX5IBy
        BNF6yUD6mWQCXCB4p/xJGjxvFeciQYpTvn5HNVS6/BTapPi97DwUTT9uGjLZaBmmJg==
    </RebutCreditDisponible>
</Aposta>
```

Cobrar una aposta.

Document XML per l'intercanvi d'informació que es produeix en el cobrament d'una aposta.

Esquema:

```
<Cobrament>
  <NouCredit>
    <IdentificadorPartida>
      <IdentificadorJoc>     </IdentificadorJoc>
      <Aleatori>             </Aleatori>
      <InstantActual>        </InstantActual>
      <NumeroPartida>        </NumeroPartida>
    </IdentificadorPartida>
    <Valor>                  </Valor>
  </NouCredit>
  <Rebut>                    </Rebut>
</Cobrament>
```

Exemple:

```
<Cobrament>
  <NouCredit>
    <IdentificadorPartida>
      <IdentificadorJoc>BlackJack</IdentificadorJoc>
```

```
      <Aleatori>168502483</Aleatori>
      <InstantActual>2005-10-26 22:13:56</InstantActual>
      <NumeroPartida>145</NumeroPartida>
    </IdentificadorPartida>
    <Valor>1000.0</Valor>
  </NouCredit>
  <Rebut>
       MIIKgAIBATELMAkGBSsOAwIaBQAwCwYJKoZIhvcNAQcBoIIJIjCCBIgwggNwoAMC
       AQICAQIwDQYJKoZIhvcNAQEFBQAwgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlD
       YXRhbG9uaWExEjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMwEQYD
       VQQLEwpDb25zdWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0BCQEW
       EmpjYXN0ZWxsYXJAdW9jLmVkdTAeFw0wNTEwMDQxMTM4MjZaFw0wNjEwMDQxMTM4
       MjZaMIGSMQswCQYDVQQGEwJFUzESMBAGA1UECBMJQ2F0YWx1bnlhMSgwJgYDVQQK
       Ex9Vbml2ZXJzaXRhdCBPYmVydGEgZGUgQ2F0YWx1bnlhMRAwDgYDVQQLEwdBbHVt
       bmVzMRAwDgYDVQQDEwdKdWdhZG9yMSEwHwYJKoZIhvcNAQkBFhJqY2FzdGVsbGFy
       QHVvYy5lZHUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAN3E2Ko7EX0MmxlI
       HlQ1+5BOmUYxccyl7tk2l4vidS35bGEKC+nSM06dXCM8azOQCC9H3eBLyCUetraq
       kliD/xqzdTdMaQ2jIn2eky8Rj1CYRAGuI05GkYZo/kircvg/IgvcdgNFt9uuFxOe
       D/uI5Qb9prgMjfmGXGMo4bdyJFPBAgMBAAGjggFvMIIBazAJBgNVHRMEAjAAMBEG
       CWCGSAGG+EIBAQQEAwIFoDALBgNVHQ8EBAMCBeAwMQYJYIZIAYb4QgENBCQWIlNl
       Z3VyZXRhdCBlbiBYYXJ4ZXMgZGUgQ29tcHV0YWRvcnMwHQYDVR0OBBYEFDJOtz87
       g7Hzq3RwzvWgyIe0Lf4IMIHBBgNVHSMEgbkwgbaAFNJneRhyp6RTrww1H3s294D9
       ha2xoYGSpIGPMIGMMQswCQYDVQQGEwJFUzESMBAGA1UECBMJQ2F0YWxvbmlhMRIw
       EAYDVQQHEwlUYXJyYWdvbmExDDAKBgNVBAoTA1VPQzETMBEGA1UECxMKQ29uc3Vs
       dG9yczEPMA0GA1UEAxMGQ0EgUEZDMSEwHwYJKoZIhvcNAQkBFhJqY2FzdGVsbGFy
       QHVvYy5lZHWCCQCrw7KQLraVODAdBgNVHREEFjAUgRJqY2FzdGVsbGFyQHVvYy5l
       ZHUwCQYDVR0SBAIwADANBgkqhkiG9w0BAQUFAAOCAQEAHm1fA4CCwuICwULPzA4I
       pV25LNu5o/HGqo4cfOBfDsh6WaaPq5fsMrQYO57y+fhn2mqt7qz61cEDYgpUq7aE
       0sX3ChHMH2WHv59Rx3L7oakabkI1e0dOSGrQ4CyUKb75pBLb1ZdOo3ubAtDdm8+m
       J9BozZL1xVckZsiAmNhVGGPQhhAwhlOYrkAbQsHW3tLBRVfCI36IE1eanASgHgvd
       NJiHQkO+b2BPZM/N6k5ZaeF3osfaklkPi52muDConAhZXdasSZg1naUR4E2x9K4a
       ow/ZwGRwJ1W6PsChbRY73bNRJIjnyG8RxSZLJK+R8iytkZC0bwVkII7YB0Zc0rF3
       PTCCBJIwggN6oAMCAQICCQCrw7KQLraVODANBgkqhkiG9w0BAQUFADCBjDELMAkG
       A1UEBhMCRVMxEjAQBgNVBAgTCUNhdGFsb25pYTESMBAGA1UEBxMJVGFycmFnb25h
       MQwwCgYDVQQKEwNVT0MxEzARBgNVBAsTCkNvbnN1bHRvcnMxDzANBgNVBAMTBkNB
       IFBGQzEhMB8GCSqGSIb3DQEJARYSamNhc3RlbGxhckB1b2MuZWR1MB4XDTA1MTAw
       NDEwNTUxMloXDTA2MTAwNDEwNTUxMlowgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQI
       EwlDYXRhbG9uaWExEjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMw
       EQYDVQQLEwpDb25zdWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0B
       CQEWEmpjYXN0ZWxsYXJAdW9jLmVkdTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
       AQoCggEBALTjkFuSne+TJBFaZL0qDz2889Rx6ErcWLtCK0xz+UPuB9yzd2qHhisR
       jY+EkRnlsXb3p2/1leoTYUGu59bgiIcjMVMNgT/eFRkl9X0oEGZEXHy/4US+w2a4
       PtGmQ7wEyMcSEpkjyfS+GKreynw9VVyWFwAQ9umUVZ28hPrXFt6tbUziYWRB0+Ar
       kGFL8e4zYudtzhh1FMFOvW8WOA2VK5zW596ChXbNQ6+i4OZgYmwWPT9f8x2jk+Pf
       5OGDIyjHzBU4xJ6409JgHDsWtm/5SJd+9wC5GYT5K6oNikR718XsV74svAx8bfA1
       1M3nLT+jdQ7VuFrrCeNhkpTtlqyjcDMCAwEAAaOB9DCB8TAdBgNVHQ4EFgQU0md5
       GHKnpFOvDDUfezb3gP2FrbEwgcEGA1UdIwSBuTCBtoAU0md5GHKnpFOvDDUfezb3
       gP2FrbGhgZKkgY8wgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlDYXRhbG9uaWEx
       EjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMwEQYDVQQLEwpDb25z
       dWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0BCQEWEmpjYXN0ZWxs
       YXJAdW9jLmVkdYIJAKvDspAutpU4MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEF
       BQADggEBAGdbzQcIddybkIqsAhm+vptcjGHv2ae9aBhQc6PQNJF/IBSuYQVh5Q78
       mTROl3cTFfkbl2/LaFrx0Ejdb0s69mbRrHMM+VU49SZiJLV+f/A/Pa0xHPTTfAr5
       rDmOBVNO+GFisAJkmZnu+Wd43w/1fnRIxGsf4GP7s+8Sv8FTX9TiQkJicalKPZKl
       9TyH5BOmrPIH2FURov92wQ2/7vbi/vIYDQeiDfoo6mE0PvOdGJvuQbFOt1xSrIHj
       g1DGgv5d+IEjA++Ry+kw3kuX8t82gsW0QjsnA8dzEv8FWT6apGwoZGivBWbgQJ2+
       F3cRQy5iWMRkOArz/Co++m/3QQ6bZHExggE5MIIBNQIBATCBkjCBjDELMAkGA1UE
       BhMCRVMxEjAQBgNVBAgTCUNhdGFsb25pYTESMBAGA1UEBxMJVGFycmFnb25hMQww
       CgYDVQQKEwNVT0MxEzARBgNVBAsTCkNvbnN1bHRvcnMxDzANBgNVBAMTBkNBIFBG
       QzEhMB8GCSqGSIb3DQEJARYSamNhc3RlbGxhckB1b2MuZWR1AgECMAkGBSsOAwIa
       BQAwDQYJKoZIhvcNAQEBBQAEgYCgznxud13ACbj3X09ZMyGY96Wo4GFEcTbX103Q
       XI+BSvvL5CeyW2jsTcViI/OMH+D4g4w8rJ7pOpEv0LI4chjGkKsCCDlN70/UljX7
       fCZZcQl/rMr6lKFNDoHbIsj/SXfc6KW/kzvaTuFBLMz49pRBnO2lQLkdT73A7ZsN
       ac2LNQ==
   </Rebut>
</Cobrament>
```

Demanar carta descoberta i tapada.

Al demanar carta cal executar el protocol de compromís, i per tant és necessari un document XML per a dur-lo a terme.

Esquema:

```
<Compromis>
  <Lliurament>
    <IdentificadorPartida>
      <IdentificadorJoc>            </IdentificadorJoc>
      <Aleatori>                    </Aleatori>
      <InstantActual>               </InstantActual>
      <NumeroPartida>               </NumeroPartida>
    </IdentificadorPartida>
    <HashAleatori>                  </HashAleatori>
  </Lliurament>
  <SignaturaHash>                   </SignaturaHash>
  <Obertura>
    <IdentificadorPartida>
      <IdentificadorJoc>            </IdentificadorJoc>
      <Aleatori>                    </Aleatori>
      <InstantActual>               </InstantActual>
      <NumeroPartida>               </NumeroPartida>
    </IdentificadorPartida>
    <Aleatori>                      </Aleatori>
  </Obertura>
  <SignaturaAleatori>               </SignaturaAleatori>
  <Carta />
</Compromis>
```

Exemple:

```
<Compromis>
  <Lliurament>
    <IdentificadorPartida>
      <IdentificadorJoc>BlackJack</IdentificadorJoc>
      <Aleatori>168502483</Aleatori>
      <InstantActual>2005-10-26 22:13:56</InstantActual>
      <NumeroPartida>145</NumeroPartida>
    </IdentificadorPartida>
    <HashAleatori>zBNjjXaCf6LvfQwyBQxdnW6weuQ=</HashAleatori>
  </Lliurament>
  <SignaturaHash>
       MIIKgAIBATELMAkGBSsOAwIaBQAwCwYJKoZIhvcNAQcBoIIJIjCCBIgwggNwoAMC
       AQICAQIwDQYJKoZIhvcNAQEFBQAwgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlD
       YXRhbG9uaWExEjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMwEQYD
       VQQLEwpDb25zdWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0BCQEW
       EmpjYXN0ZWxsYXJAdW9jLmVkdTAeFw0wNTEwMDQxMTM4MjZaFw0wNjEwMDQxMTM4
       MjZaMIGSMQswCQYDVQQGEwJFUzESMBAGA1UECBMJQ2F0YWx1bnlhMSgwJgYDVQQK
       Ex9Vbml2ZXJzaXRhdCBPYmVydGEgZGUgQ2F0YWx1bnlhMRAwDgYDVQQLEwdBbHVt
       bmVzMRAwDgYDVQQDEwdKdWdhZG9yMSEwHwYJKoZIhvcNAQkBFhJqY2FzdGVsbGFy
       QHVvYy5lZHUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAN3E2Ko7EX0MmxlI
       HlQ1+5BOmUYxccyl7tk2l4vidS35bGEKC+nSM06dXCM8azOQCC9H3eBLyCUetraq
       kliD/xqzdTdMaQ2jIn2eky8Rj1CYRAGuI05GkYZo/kircvg/IgvcdgNFt9uuFxOe
       D/uI5Qb9prgMjfmGXGMo4bdyJFPBAgMBAAGjggFvMIIBazAJBgNVHRMEAjAAMBEG
       CWCGSAGG+EIBAQQEAwIFoDALBgNVHQ8EBAMCBeAwMQYJYIZIAYb4QgENBCQWIlNl
       Z3VyZXRhdCBlbiBYYXJ4ZXMgZGUgQ29tcHV0YWRvcnMwHQYDVR0OBBYEFDJOtz87
       g7Hzq3RwzvWgyIe0Lf4IMIHBBgNVHSMEgbkwgbaAFNJneRhyp6RTrww1H3s294D9
       ha2xoYGSpIGPMIGMMQswCQYDVQQGEwJFUzESMBAGA1UECBMJQ2F0YWxvbmlhMRIw
       EAYDVQQHEwlUYXJyYWdvbmExDDAKBgNVBAoTA1VPQzETMBEGA1UECxMKQ29uc3Vs
       dG9yczEPMA0GA1UEAxMGQ0EgUEZDMSEwHwYJKoZIhvcNAQkBFhJqY2FzdGVsbGFy
       QHVvYy5lZHWCCQCrw7KQLraVODAdBgNVHREEFjAUgRJqY2FzdGVsbGFyQHVvYy5l
       ZHUwCQYDVR0SBAIwADANBgkqhkiG9w0BAQUFAAOCAQEAHm1fA4CCwuICwULPzA4I
       pV25LNu5o/HGqo4cfOBfDsh6WaaPq5fsMrQYO57y+fhn2mqt7qz61cEDYgpUq7aE
       0sX3ChHMH2WHv59Rx3L7oakabkI1e0dOSGrQ4CyUKb75pBLb1ZdOo3ubAtDdm8+m
```

```
      J9BozZL1xVckZsiAmNhVGGPQhhAwhlOYrkAbQsHW3tLBRVfCI36IE1eanASgHgvd
      NJiHQkO+b2BPZM/N6k5ZaeF3osfaklkPi52muDConAhZXdasSZg1naUR4E2x9K4a
      ow/ZwGRwJ1W6PsChbRY73bNRJIjnyG8RxSZLJK+R8iytkZC0bwVkII7YB0Zc0rF3
      PTCCBJIwggN6oAMCAQICCQCrw7KQLraVODANBgkqhkiG9w0BAQUFADCBjDELMAkG
      A1UEBhMCRVMxEjAQBgNVBAgTCUNhdGFsb25pYTESMBAGA1UEBxMJVGFycmFnb25h
      MQwwCgYDVQQKEwNVT0MxEzARBgNVBAsTCkNvbnN1bHRvcnMxDzANBgNVBAMTBkNB
      IFBGQzEhMB8GCSqGSIb3DQEJARYSamNhc3RlbGxhckB1b2MuZWR1MB4XDTA1MTAw
      NDEwNTUxMloXDTA2MTAwNDEwNTUxMlowgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQI
      EwlDYXRhbG9uaWExEjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMw
      EQYDVQQLEwpDb25zdWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0B
      CQEWEmpjYXN0ZWxsYXJAdW9jLmVkdTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
      AQoCggEBALTjkFuSne+TJBFaZL0qDz2889Rx6ErcWLtCK0xz+UPuB9yzd2qHhisR
      jY+EkRnlsXb3p2/1leoTYUGu59bgiIcjMVMNgT/eFRkl9X0oEGZEXHy/4US+w2a4
      PtGmQ7wEyMcSEpkjyfS+GKreynw9VVyWFwAQ9umUVZ28hPrXFt6tbUziYWRB0+Ar
      kGFL8e4zYudtzhh1FMFOvW8WOA2VK5zW596ChXbNQ6+i4OZgYmwWPT9f8x2jk+Pf
      5OGDIyjHzBU4xJ6409JgHDsWtm/5SJd+9wC5GYT5K6oNikR718XsV74svAx8bfA1
      1M3nLT+jdQ7VuFrrCeNhkpTtlqyjcDMCAwEAAaOB9DCB8TAdBgNVHQ4EFgQU0md5
      GHKnpFOvDDUfezb3gP2FrbEwgcEGA1UdIwSBuTCBtoAU0md5GHKnpFOvDDUfezb3
      gP2FrbGhgZKkgY8wgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlDYXRhbG9uaWEx
      EjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMwEQYDVQQLEwpDb25z
      dWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0BCQEWEmpjYXN0ZWxs
      YXJAdW9jLmVkdYIJAKvDspAutpU4MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEF
      BQADggEBAGdbzQcIddybkIqsAhm+vptcjGHv2ae9aBhQc6PQNJF/IBSuYQVh5Q78
      mTROl3cTFfkbl2/LaFrx0Ejdb0s69mbRrHMM+VU49SZiJLV+f/A/Pa0xHPTTfAr5
      rDmOBVNO+GFisAJkmZnu+Wd43w/1fnRIxGsf4GP7s+8Sv8FTX9TiQkJicalKPZKl
      9TyH5BOmrPIH2FURov92wQ2/7vbi/vIYDQeiDfoo6mE0PvOdGJvuQbFOt1xSrIHj
      g1DGgv5d+IEjA++Ry+kw3kuX8t82gsW0QjsnA8dzEv8FWT6apGwoZGivBWbgQJ2+
      F3cRQy5iWMRkOArz/Co++m/3QQ6bZHExggE5MIIBNQIBATCBkjCBjDELMAkGA1UE
      BhMCRVMxEjAQBgNVBAgTCUNhdGFsb25pYTESMBAGA1UEBxMJVGFycmFnb25hMQww
      CgYDVQQKEwNVT0MxEzARBgNVBAsTCkNvbnN1bHRvcnMxDzANBgNVBAMTBkNBIFBG
      QzEhMB8GCSqGSIb3DQEJARYSamNhc3RlbGxhckB1b2MuZWR1AgECMAkGBSsOAwIa
      BQAwDQYJKoZIhvcNAQEBBQAEgYB6o+dkjrXUTp/muxodEq4GFLXhcXKd7Xayivfr
      gt6l1XekrlMYhpoD+iHwPFL2iBa/i/u7rLxN3iw3DY1iIGczIHs3CjCZAMBotkcY
      3GkamRoqk2prq8WcxRadHIAlNJfaaZ6zFX/VGw4oBWZPg9zpBj/Qv6Mz30IToq5a
      Y6mfJA==
</SignaturaHash>
<Obertura>
  <IdentificadorPartida>
    <IdentificadorJoc>BlackJack</IdentificadorJoc>
    <Aleatori>168502483</Aleatori>
    <InstantActual>2005-10-26 22:13:56</InstantActual>
    <NumeroPartida>145</NumeroPartida>
  </IdentificadorPartida>
  <Aleatori>697114854</Aleatori>
</Obertura>
<SignaturaAleatori>
      MIIKgAIBATELMAkGBSsOAwIaBQAwCwYJKoZIhvcNAQcBoIIJIjCCBIgwggNwoAMC
      AQICAQIwDQYJKoZIhvcNAQEFBQAwgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlD
      YXRhbG9uaWExEjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMwEQYD
      VQQLEwpDb25zdWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0BCQEW
      EmpjYXN0ZWxsYXJAdW9jLmVkdTAeFw0wNTEwMDQxMTM4MjZaFw0wNjEwMDQxMTM4
      MjZaMIGSMQswCQYDVQQGEwJFUzESMBAGA1UECBMJQ2F0YWx1bnlhMSgwJgYDVQQK
      Ex9Vbml2ZXJzaXRhdCBPYmVydGEgZGUgQ2F0YWx1bnlhMRAwDgYDVQQLEwdBbHVt
      bmVzMRAwDgYDVQQDEwdKdWdhZG9yMSEwHwYJKoZIhvcNAQkBFhJqY2FzdGVsbGFy
      QHVvYy5lZHUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAN3E2Ko7EX0MmxlI
      HlQ1+5BOmUYxccyl7tk2l4vidS35bGEKC+nSM06dXCM8azOQCC9H3eBLyCUetraq
      kliD/xqzdTdMaQ2jIn2eky8Rj1CYRAGuI05GkYZo/kircvg/IgvcdgNFt9uuFxOe
      D/uI5Qb9prgMjfmGXGMo4bdyJFPBAgMBAAGjggFvMIIBazAJBgNVHRMEAjAAMBEG
      CWCGSAGG+EIBAQQEAwIFoDALBgNVHQ8EBAMCBeAwMQYJYIZIAYb4QgENBCQWIlNl
      Z3VyZXRhdCBlbiBYYXJ4ZXMgZGUgQ29tcHV0YWRvcnMwHQYDVR0OBBYEFDJOtz87
      g7Hzq3RwzvWgyIe0Lf4IMIHBBgNVHSMEgbkwgbaAFNJneRhyp6RTrww1H3s294D9
      ha2xoYGSpIGPMIGMMQswCQYDVQQGEwJFUzESMBAGA1UECBMJQ2F0YWxvbmlhMRIw
      EAYDVQQHEwlUYXJyYWdvbmExDDAKBgNVBAoTA1VPQzETMBEGA1UECxMKQ29uc3Vs
      dG9yczEPMA0GA1UEAxMGQ0EgUEZDMSEwHwYJKoZIhvcNAQkBFhJqY2FzdGVsbGFy
      QHVvYy5lZHWCCQCrw7KQLraVODAdBgNVHREEFjAUgRJqY2FzdGVsbGFyQHVvYy5l
      ZHUwCQYDVR0SBAIwADANBgkqhkiG9w0BAQUFAAOCAQEAHm1fA4CCwuICwULPzA4I
      pV25LNu5o/HGqo4cfOBfDsh6WaaPq5fsMrQYO57y+fhn2mqt7qz61cEDYgpUq7aE
      0sX3ChHMH2WHv59Rx3L7oakabkI1e0dOSGrQ4CyUKb75pBLb1ZdOo3ubAtDdm8+m
      J9BozZL1xVckZsiAmNhVGGPQhhAwhlOYrkAbQsHW3tLBRVfCI36IE1eanASgHgvd
      NJiHQkO+b2BPZM/N6k5ZaeF3osfaklkPi52muDConAhZXdasSZg1naUR4E2x9K4a
      ow/ZwGRwJ1W6PsChbRY73bNRJIjnyG8RxSZLJK+R8iytkZC0bwVkII7YB0Zc0rF3
```

```
        PTCCBJIwggN6oAMCAQICCQCrw7KQLraVODANBgkqhkiG9w0BAQUFADCBjDELMAkG
        A1UEBhMCRVMxEjAQBgNVBAgTCUNhdGFsb25pYTESMBAGA1UEBxMJVGFycmFnb25h
        MQwwCgYDVQQKEwNVT0MxEzARBgNVBAsTCkNvbnN1bHRvcnMxDzANBgNVBAMTBkNB
        IFBGQzEhMB8GCSqGSIb3DQEJARYSamNhc3RlbGxhckB1b2MuZWR1MB4XDTA1MTAw
        NDEwNTUxMloXDTA2MTAwNDEwNTUxMlowgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQI
        EwlDYXRhbG9uaWExEjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMw
        EQYDVQQLEwpDb25zdWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0B
        CQEWEmpjYXN0ZWxsYXJAdW9jLmVkdTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
        AQoCggEBALTjkFuSne+TJBFaZL0qDz2889Rx6ErcWLtCK0xz+UPuB9yzd2qHhisR
        jY+EkRnlsXb3p2/1leoTYUGu59bgiIcjMVMNgT/eFRkl9X0oEGZEXHy/4US+w2a4
        PtGmQ7wEyMcSEpkjyfS+GKreynw9VVyWFwAQ9umUVZ28hPrXFt6tbUziYWRB0+Ar
        kGFL8e4zYudtzhh1FMFOvW8WOA2VK5zW596ChXbNQ6+i4OZgYmwWPT9f8x2jk+Pf
        5OGDIyjHzBU4xJ6409JgHDsWtm/5SJd+9wC5GYT5K6oNikR718XsV74svAx8bfA1
        1M3nLT+jdQ7VuFrrCeNhkpTtlqyjcDMCAwEAAaOB9DCB8TAdBgNVHQ4EFgQU0md5
        GHKnpFOvDDUfezb3gP2FrbEwgcEGA1UdIwSBuTCBtoAU0md5GHKnpFOvDDUfezb3
        gP2FrbGhgZKkgY8wgYwxCzAJBgNVBAYTAkVTMRIwEAYDVQQIEwlDYXRhbG9uaWEx
        EjAQBgNVBAcTCVRhcnJhZ29uYTEMMAoGA1UEChMDVU9DMRMwEQYDVQQLEwpDb25z
        dWx0b3JzMQ8wDQYDVQQDEwZDQSBQRkMxITAfBgkqhkiG9w0BCQEWEmpjYXN0ZWxs
        YXJAdW9jLmVkdYIJAKvDspAutpU4MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEF
        BQADggEBAGdbzQcIddybkIqsAhm+vptcjGHv2ae9aBhQc6PQNJF/IBSuYQVh5Q78
        mTROl3cTFfkbl2/LaFrx0Ejdb0s69mbRrHMM+VU49SZiJLV+f/A/Pa0xHPTTfAr5
        rDmOBVNO+GFisAJkmZnu+Wd43w/1fnRIxGsf4GP7s+8Sv8FTX9TiQkJicalKPZKl
        9TyH5BOmrPIH2FURov92wQ2/7vbi/vIYDQeiDfoo6mE0PvOdGJvuQbFOt1xSrIHj
        g1DGgv5d+IEjA++Ry+kw3kuX8t82gsW0QjsnA8dzEv8FWT6apGwoZGivBWbgQJ2+
        F3cRQy5iWMRkOArz/Co++m/3QQ6bZHExggE5MIIBNQIBATCBkjCBjDELMAkGA1UE
        BhMCRVMxEjAQBgNVBAgTCUNhdGFsb25pYTESMBAGA1UEBxMJVGFycmFnb25hMQww
        CgYDVQQKEwNVT0MxEzARBgNVBAsTCkNvbnN1bHRvcnMxDzANBgNVBAMTBkNBIFBG
        QzEhMB8GCSqGSIb3DQEJARYSamNhc3RlbGxhckB1b2MuZWR1AgECMAkGBSsOAwIa
        BQAwDQYJKoZIhvcNAQEBBQAEgYBGpCJcMVLWuGoi4UTLKoHUzlwsm0UoMYQUBDh4
        ZWcAywXcHw0IDxOmCfoNI7bSbCGPB0yfmz8IiIkvsrqpapbhw0cJmXLPicFqYVas
        drJxDfQGtC1OdtGPq760rtg2Tt4maWas5EW2cQvyNcETMgX8p67vcjQd/U6lGVAV
        TCOLCw==
  </SignaturaAleatori>
  <Carta />
</Compromis>
```

Capítol 6. RMI.

Definició de RMI.

El sistema d'Invocació Remota de Mètodes (RMI) de Java permet a un objecte que s'executa en una màquina virtual de Java cridar a mètodes d'objectes que estan en màquines virtuals diferents, ja sigui en el mateix ordinador o en un de remot.

Les aplicacions RMI normalment comprenen dos programes separats, un servidor i un client. Una aplicació servidor típica crea un munt d'objectes remots, fa accessibles unes referències a aquests objectes, i espera a que els clients cridin a aquests mètodes o objectes remots. Una aplicació client típica obté una referència d'un o més objectes remots en el servidor i en crida els seus mètodes.

RMI proporciona el mecanisme per el que es comuniquen i passen informació el client i el servidor. A aquest tipus d'aplicacions se'ls anomena aplicacions d'objectes distribuïts.

Interfície del servidor.

Els mètodes i objectes als que es pot accedir en un servidor RMI es defineixen en una interfície.

En el cas del nostre gestor la interfície és la següent:

```
package pfc;

import java.rmi.Remote;
import java.rmi.RemoteException;

public interface IGestorServer extends Remote {
        String PeticioAutenticacio(String XML) throws RemoteException;
        boolean ComprovacioAutenticacio(String XML) throws RemoteException;
        String IniciPartida(String XML) throws RemoteException;
        String Aposta(String XML) throws RemoteException;
        String Compromis(String XML) throws RemoteException;
        int LliuramentCompromis(String XML) throws RemoteException;
        String CobramentAposta(String XML) throws RemoteException;
        String IncrementarDiposit(String XML) throws RemoteException;
}
```

Diagrama de classes RMI.

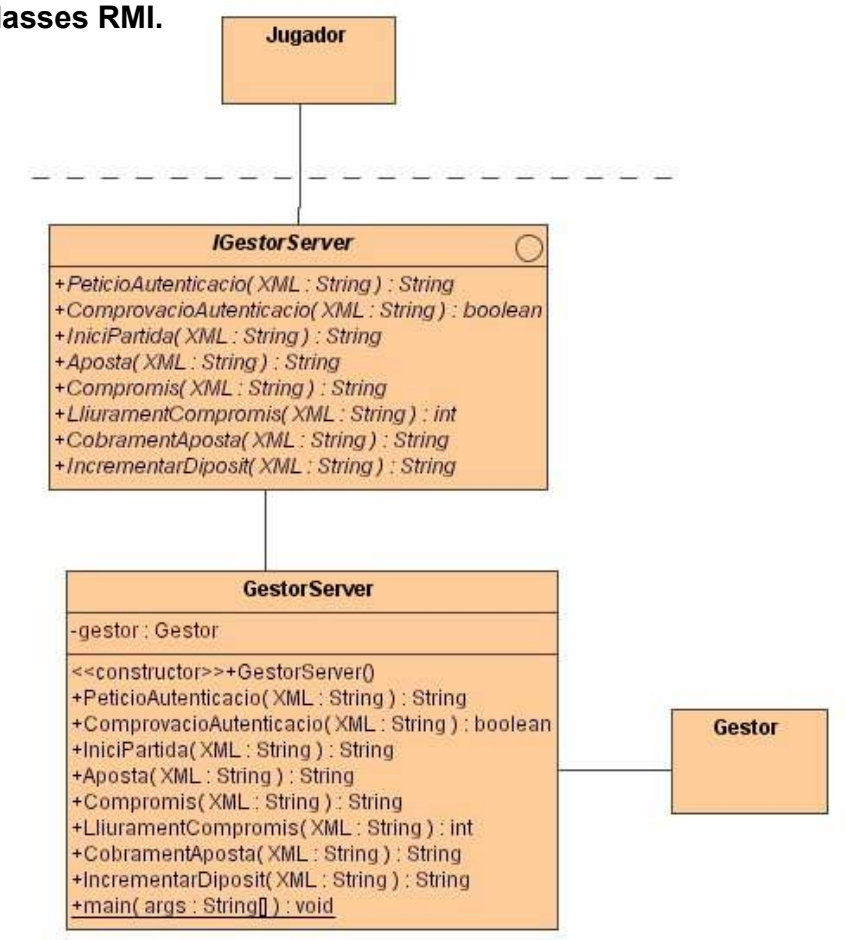
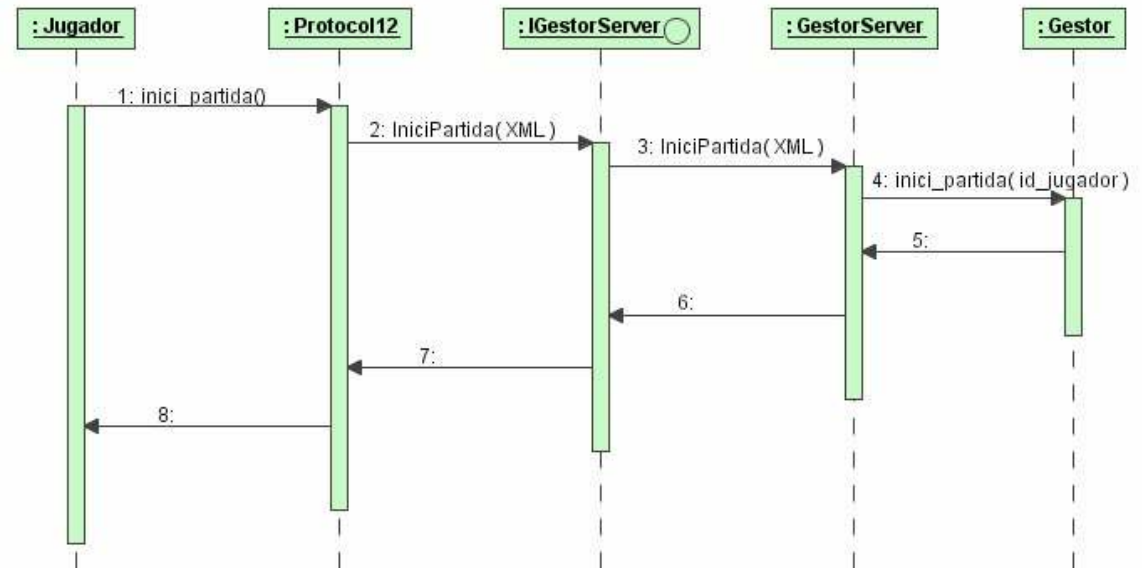


Diagrama de seqüència RMI (cas inici partida).



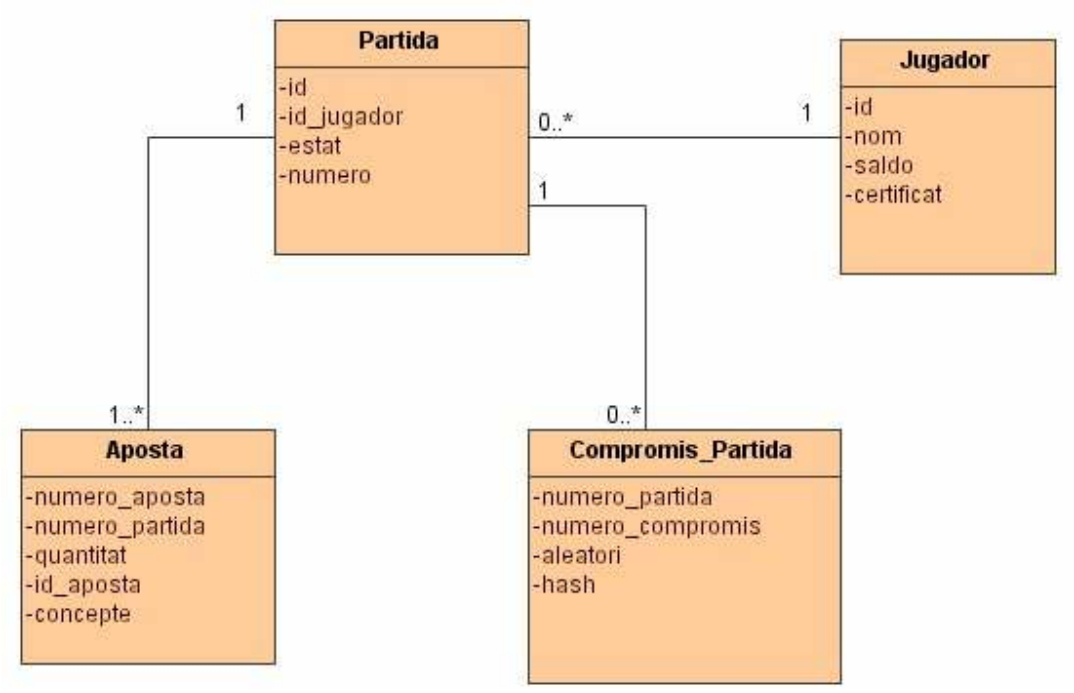
Capítol 7. Base de dades.

La utilització d'una base de dades ens permetrà emmagatzemar les dades de les partides.

Per a fer-ho utilitzarem el gestor MySQL. Es tracta d'un sistema de base de dades relacionals SQL de codi obert, desenvolupat, distribuït i suportat per l'empresa MySQL AB.

Podem disposar d'una versió complerta i gratuïta de MySQL, si és per a fins acadèmics.

Diagrama relacional de la base de dades



Descripció del diagrama.

1.- Taula PARTIDA.

Aquí es guarden les dades de les partides que es juguen.

Camps:

Id	- Identificador de partida.
Id_jugador	- Identificador del jugador que participa en la partida.
Estat	- Estat de la partida (0: activa, 1: finalitzada).

Número - Número de partida.

2.- Taula JUGADOR.

Dades dels jugadors.

Camps:

Id - Identificador del jugador.
Nom - Nom del jugador.
Saldo - Saldo del jugador.
Certificat - Ruta on s'ubica l'arxiu del certificat del jugador.

3.- Taula APOSTA.

Apostes realitzades en una partida.

Camps:

Número partida - Número de la partida en la que s'ha realitzat l'aposta.
Número aposta - Número d'aposta dins de la partida.
Quantitat - Quantitat apostada.
Id_aposta - Identificador de l'aposta.
Concepte - Concepte de l'aposta.

4.- Taula COMPROMIS_PARTIDA.

Taula per gestionar les dades que cal guardar durant el protocol de compromís.

Camps:

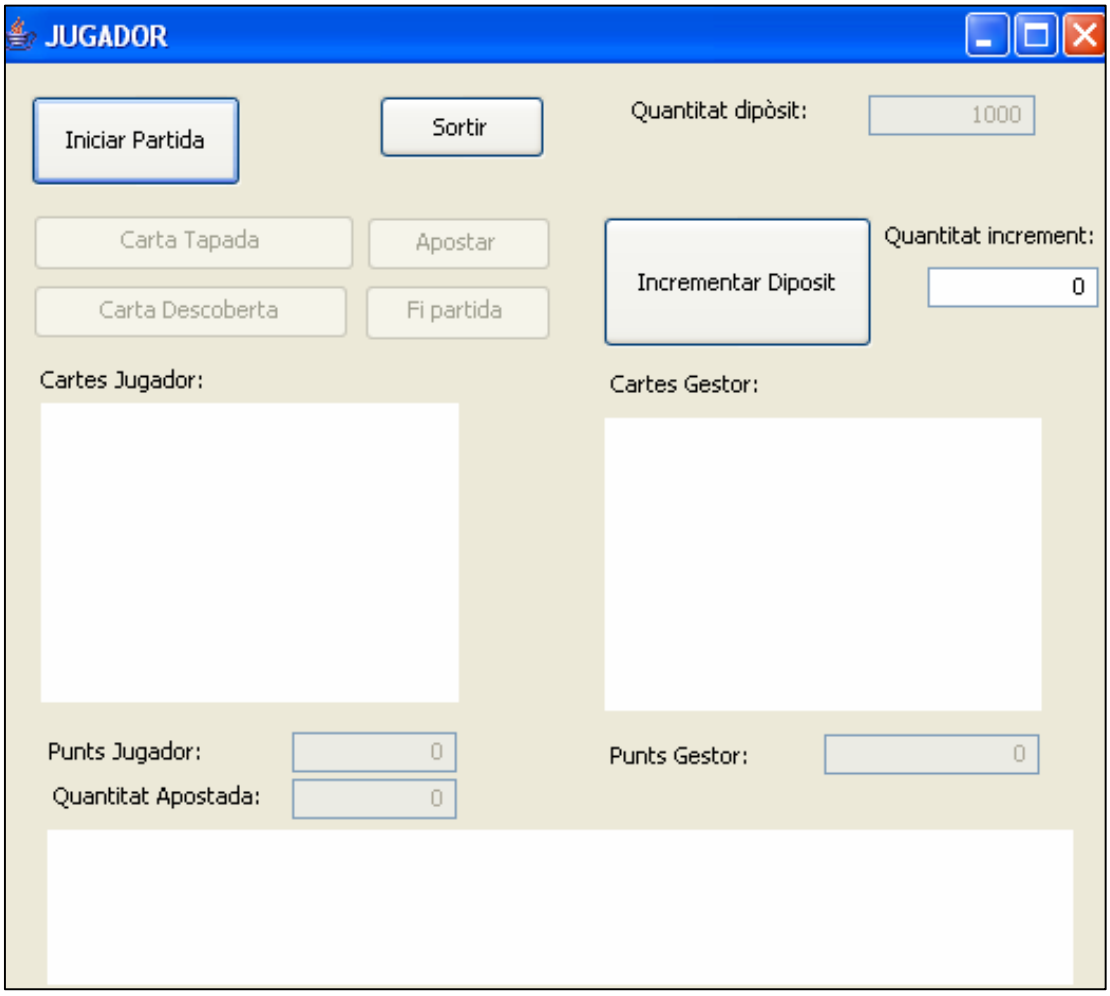
Número partida - Número de la partida.
Número compromís - Número de compromís dins una partida.
Aleatori - Aleatori del gestor en la primera fase del compromís.
Hash - Hash enviat inicialment per el jugador.

Capítol 8. Interfície Jugador.

La interfície d'usuari permet als jugadors realitzar les següents funcionalitats:

- Autenticar-se contra el gestor del joc (integrat dins l'inici de partida).
- Iniciar una partida.
- Realitzar una aposta.
- Incrementar el dipòsit de diners.
- Seguir l'operativa del joc.
- Pagar/cobrar una aposta.
- Abandonar la partida.

Aspecte de la interfície del jugador



Execució del programari del jugador.

Per executar el programa cal introduir la següent instrucció a l'intèrpret de comandes:

```
java  -Djava.rmi.server.codebase=file:/c:\pfc\classes/
      -Djava.security.policy=java.policy
      pfc.JugadorFrame
```

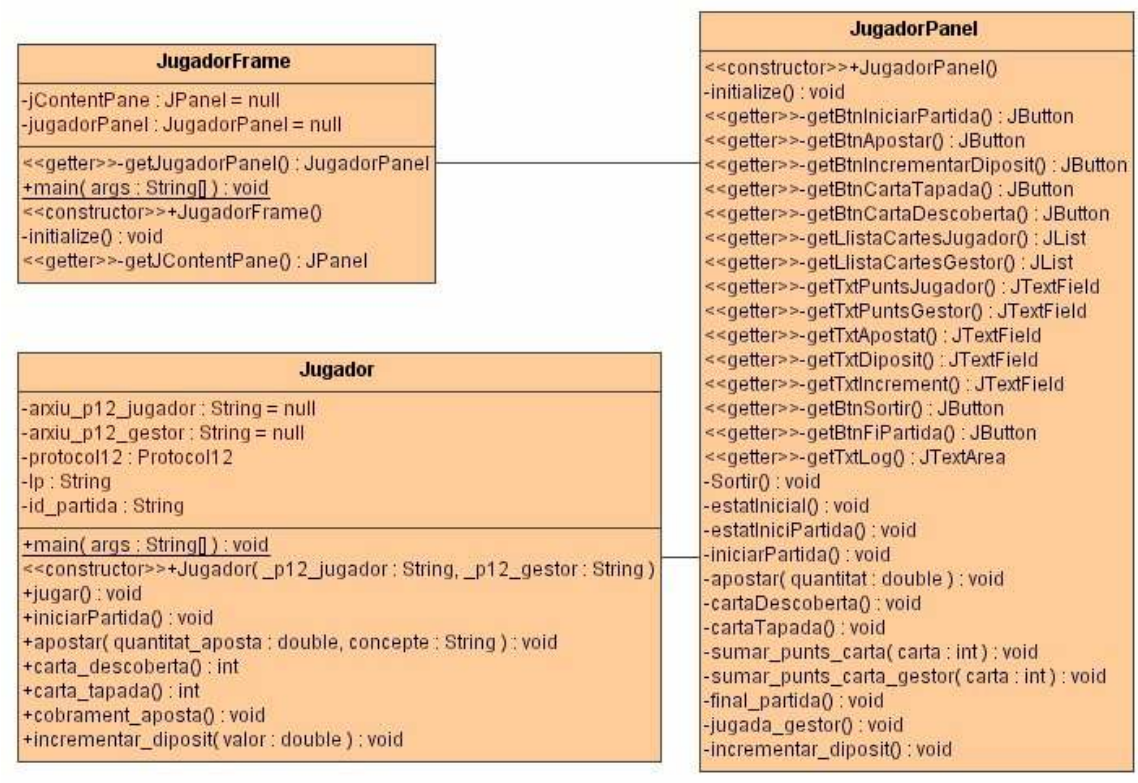
S'ha deixa preparat per entorn Windows un arxiu .bat que executa l'anterior instrucció.

Configuració programari jugador.

El programa llegeix l'arxiu ConfiguracioJugador.xml per a carregar diferents paràmetres que necessita:

```
<?xml version="1.0"?>
<ConfiguracioJugador>
      <ArxiuP12Gestor>C:\PKI\gestor.p12</ArxiuP12Gestor>
      <ArxiuP12Jugador>C:\PKI\jugador.p12</ArxiuP12Jugador>
</ConfiguracioJugador>
```

Diagrama de classes interfície jugador.

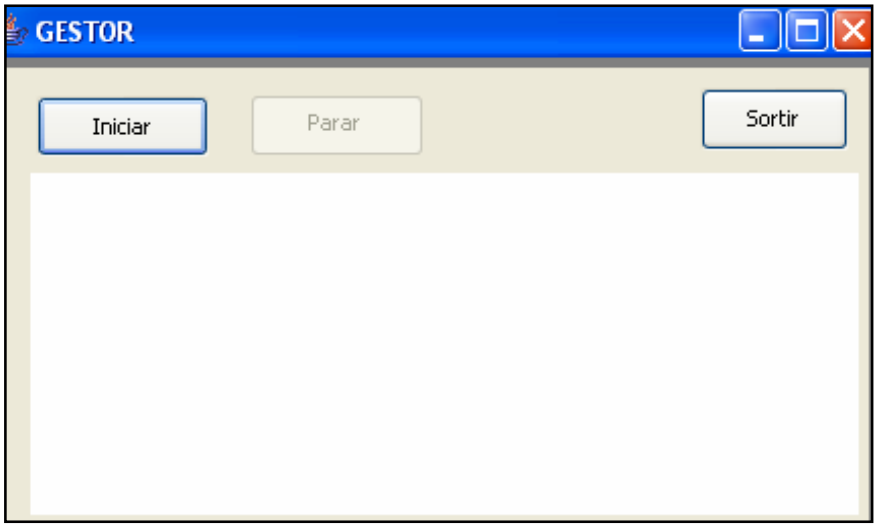


Capítol 9. Interfície Gestor.

La interfície del gestor del joc permet a un usuari realitzar les següents funcions:

- Iniciar el servidor RMI del gestor.
- Parar el servidor RMI del gestor.

Aspecte de la interfície del gestor.



Execució del programari del gestor.

Per executar el programa cal introduir la següent instrucció a l'intèrpret de comandes:

```
java -Djava.rmi.server.codebase=file:/c:\pfc\classes/
     -Djava.rmi.server.hostname=localhost
     -Djava.security.policy=java.policy
     pfc.GestorFrame
```

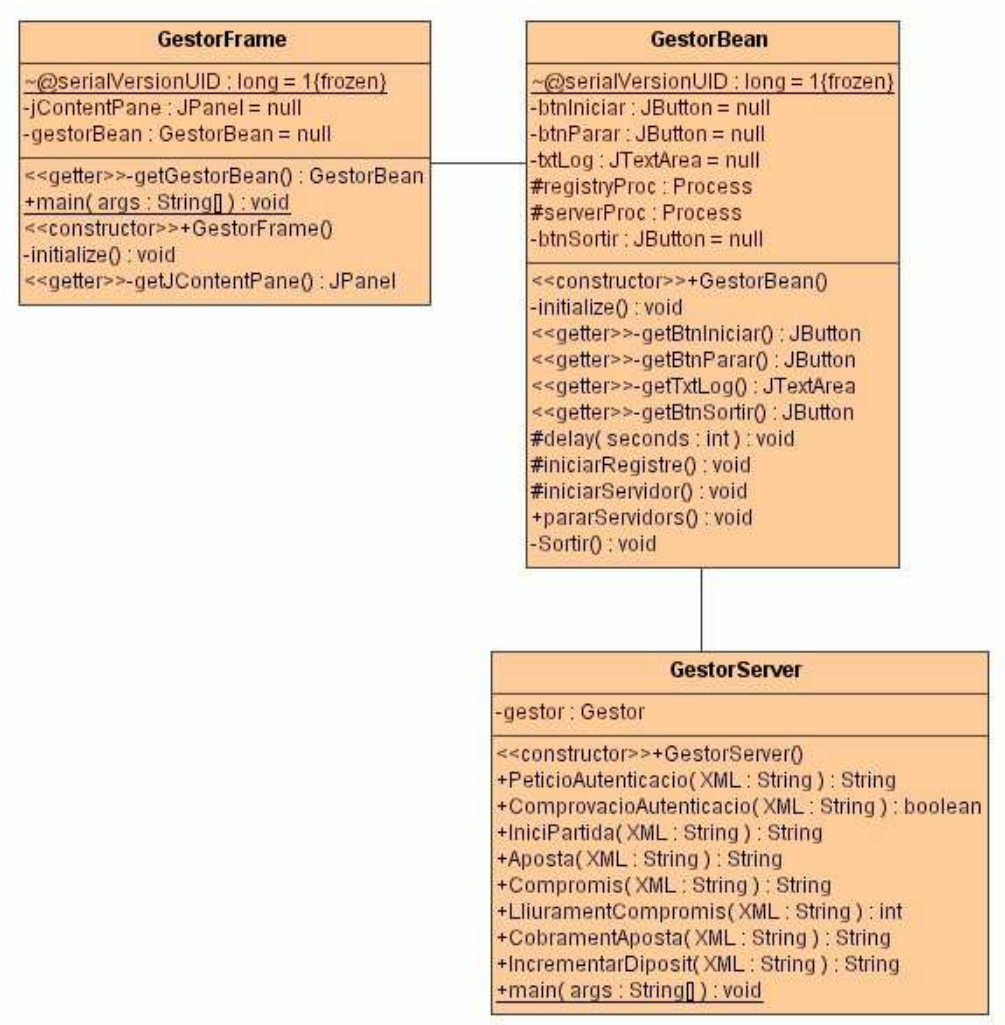
S'ha deixa preparat per entorn Windows un arxiu .bat que executa l'anterior instrucció.

Configuració programari jugador.

El programa llegeix l'arxiu ConfiguracioGestor.xml per a carregar diferents paràmetres que necessita:

```
<?xml version="1.0"?>
<ConfiguracioGestor>
      <ServidorBD>localhost</ServidorBD>
      <BaseDades>pfc</BaseDades>
      <UsuariBD>uoc</UsuariBD>
      <PasswordBD>uoc</PasswordBD>
      <Classes>/c:\pfc\classes/</Classes>
      <Politiques>c:\pfc\java.policy</Politiques>
      <ServidorRMI>localhost</ServidorRMI>
      <ArxiuP12Gestor>C:\PKI\gestor.p12</ArxiuP12Gestor>
      <PasswordP12>uoc2001</PasswordP12>
</ConfiguracioGestor>
```

Diagrama de classes interfície gestor.



Capítol 10. Valoració econòmica.

Suposant un preu de 40 € per hora, i tenint en compte que s'han invertit unes 350 hores en el projecte, ens surt un cost de desenvolupament de:

14.000 €

Capítol 11. Conclusions.

Generals

S'ha dissenyat, i implementat, un sistema de joc electrònic de BlackJack remot, que ofereix als jugadors un nivell de seguretat similar al que es pot tenir quan juguem en un casino tradicional.

S'han complert tots els objectius en quant a seguretat, desenvolupant el sistema amb els protocols i eines que especificades en el PFC.

Personals

Per a desenvolupar les aplicacions que composen el projecte he hagut d'aprendre el funcionament de tot el procés de joc del BlackJack, així com provar diferents programaris que hi ha en el mercat per aquest fi.

Per a poder dur a terme el projecte he necessitat aprendre a utilitzar en profunditat certes eines informàtiques, que m'han aportat els següents coneixements:

- Consolidar els coneixements adquirits en l'assignatura de Criptografia.
- Aprofundir en el coneixement de la metodologia UML, utilitzant l'eina MagicDraw.
- Aprofundir en el llenguatge de programació Java i aprendre a fer servir components de tractament de gràfics amb el Visual Editor de l' Eclipse.
- Aprendre a treballar amb el sistema de bases de dades MySQL.
- Augmentar la pràctica en l'ús del IAIK, per utilitzar criptografia en Java.
- Augmentar la pràctica en l'ús del JDOM, per manipular XML en Java.
- Consolidar els coneixements sobre OpenSSL.
- Aprendre a fer servidors RMI.
- Aprendre a fer interfícies de Java.

En definitiva, crec que el projecte ha servit per consolidar molts dels coneixements que he adquirit en els estudis i formar-me un bona idea del que és desenvolupar una aplicació criptogràfica real, amb totes les seves dificultats i problemes, preparant-me així per poder utilitzar-ho en la meu àmbit laboral, si cal.

Glossari.

BlackJack: joc de cartes de casino.

CA: autoritat certificadora (que emet certificats digitals).

Eclipse: editor de Java.

IAIK: biblioteca de classes criptogràfiques per Java.

Java: llenguatge de programació de SUN Microsystems.

JDOM: biblioteca de classes per manipular XML amb Java.

MagicDraw: Eina de disseny UML.

MySQL: gestor de bases de dades relacionals SQL.

OpenSSL: programari per gestionar certificats criptogràfics.

PKI: infraestructura criptogràfica de clau pública.

RMI: Invocació remota de mètodes de Java.

SQL: llenguatge de consulta de bases de dades.

UML: metodologia de disseny d'aplicacions informàtiques.

XML: llenguatge de representació de dades.

Bibliografia.

Enginyeria del programari
Benet Campderich Falgueras. UOC. 2004.

Java™ 2 Platform Standard Edition 5.0 API Specification
http://java.sun.com/j2se/1.5.0/docs/api/index.html

JDOC Documentation
http://www.jdom.org/downloads/docs.html

MySQL 4.1 Reference Manual
http://dev.mysql.com/doc/refman/4.1/en/index.html

OpenSSL.
http://personales.ya.com/reque/apuntes/memoria/paginas/openssl.html#4

The Java™ Tutorial: RMI
http://java.sun.com/docs/books/tutorial/rmi/index.html

UML 2 For Dummies
Michael Jesse Chonoles i James A. Schard. Ed. Hungry Minds. 2003.

Visual Editor: building a customed bean.
http://www.eclipse.org/vep/WebContent/docs/demos/custom_field/FieldBean.html

Wikipedia
http://www.wikipedia.org

Annexos.

I. Relació d'arxius font.

B64Manager.java – Gestió de codificació en base 64.
CipherManager.java – Gestió de xifrats.
Criptografia.java – Gestió de funcions criptogràfiques.
DataManager.java – Gestió de la base de dades.
DocumentAposta.java – Gestió XML aposta.
DocumentAutenticacio.java – Gestió XML autenticació.
DocumentCobrament.java – Gestió XML cobrament.
DocumentCompromis.java – Gestió XML compromís.
DocumentIncrementDiposit.java – Gestió XML increment dipòsit.
DocumentIniciPartida.java – Gestió XML inici partida.
Gestor.java – Programa que encapsula les funcions del gestor.
GestorBean.java – Interfície del gestor.
GestorFrame.java – Marc per la interfície del gestor.
GestorServer.java – Servidor RMI pel gestor.
IGestorServer.java – Interfície RMI del gestor.
Jugador.java – Encapsulat de la funcionalitat del jugador.
JugadorFrame.java – Marc per la interfície del jugador.
JugadorPanel.java – Interfície del jugador.
MessageImprint.java – Gestió de signatures criptogràfiques.
P12.java – Gestió de certificats criptogràfics.
Protocol1.java – Encapsulat les funcions del protocol 1.
Protocol12.java – Encapsulat de les funcions del protocol 12.
Protocol13.java – Encapsulat les funcions del protocol 13.
Protocol14.java – Encapsulat les funcions del protocol 14.
Protocol2.java – Encapsulat les funcions del protocol 2.
Protocol3.java – Encapsulat les funcions del protocol 3.
Protocol4.java – Encapsulat les funcions del protocol 4.
Protocol5.java – Encapsulat les funcions del protocol 5.
Protocol6.java – Encapsulat les funcions del protocol 6.
Protocol7.java – Encapsulat les funcions del protocol 7.
SignerManager.java – Gestió de signatures criptogràfiques.

II. Instruccions per crear la base de dades.

```
CREATE DATABASE /*!32312 IF NOT EXISTS*/ pfc;
USE pfc;

--
-- Table structure for table `pfc`.`aposta`
--

DROP TABLE IF EXISTS `aposta`;
CREATE TABLE `aposta` (
  `numero_partida` decimal(7,0) NOT NULL default '0',
  `numero_aposta` decimal(7,0) NOT NULL default '0',
  `quantitat` decimal(9,2) NOT NULL default '0.00',
  `id_aposta` text NOT NULL,
  `concepte` varchar(255) default NULL,
  PRIMARY KEY  (`numero_partida`,`numero_aposta`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

DROP TABLE IF EXISTS `compromis_partida`;
CREATE TABLE `compromis_partida` (
  `numero_partida` int(10) unsigned NOT NULL default '0',
  `numero_compromis` int(10) unsigned NOT NULL default '0',
  `aleatori` int(10) unsigned NOT NULL default '0',
  `hash` varchar(255) NOT NULL default '',
  PRIMARY KEY  (`numero_partida`,`numero_compromis`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

DROP TABLE IF EXISTS `jugador`;
CREATE TABLE `jugador` (
  `id` decimal(7,0) NOT NULL default '0',
  `nom` varchar(60) default NULL,
  `saldo` decimal(9,2) default NULL,
  `certificat` varchar(255) default NULL,
  PRIMARY KEY  (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

/*!40000 ALTER TABLE `jugador` DISABLE KEYS */;
INSERT INTO `jugador` (`id`,`nom`,`saldo`,`certificat`) VALUES
 ('1','Pere Pi Comas','2600.00','C:\\PKI\\jugador.p12');
/*!40000 ALTER TABLE `jugador` ENABLE KEYS */;

DROP TABLE IF EXISTS `partida`;
CREATE TABLE `partida` (
  `id` varchar(255) NOT NULL default '',
  `id_jugador` decimal(7,0) NOT NULL default '0',
  `estat` char(1) NOT NULL default '',
  `numero` decimal(7,0) default NULL,
  PRIMARY KEY  (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

/*!40000 ALTER TABLE `partida` ENABLE KEYS */;

/*!40101 SET SQL_MODE=@OLD_SQL_MODE */;
/*!40014 SET FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS */;
/*!40014 SET UNIQUE_CHECKS=@OLD_UNIQUE_CHECKS */;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
```

III. Joc de proves.

Servidor (gestor).

- Instal·lar el MysQL 4.1.

- Crear la base de dades amb l'script \src\sql\bd.sql.

- Editar l'arxiu ConfiguracioGestor.xml per configurar:
  * El servidor de MySQL.
  * El nom de la base de dades ("pfc" per defecte).
  * L'usuari de la base de dades ("uoc" per defecte).
  * El password de la base de dades ("uoc" per defecte).
  * La ruta sencera de la carpeta "classes" que hi ha a \bin.
  * La ruta sencera de l'arxiu de politiques que hi ha a \bin.
  * El nom del servidor RMI.
  * La ruta sencera de l'arxiu p12 del gestor.
  * El password de l'arxiu p12.

- Executar Gestor.bat (per a Windows). En cas de Linux cal adaptar el fitxer, tot i que es possible que funcioni tal qual.

- Prémer el botó "Iniciar".

- Per finalitzar prémer el botó "parar" o directament el de "sortir".

Jugador.

- Editar l'arxiu ConfiguracioJugador.xml per configurar:
  * La ruta sencera de l'arxiu p12 del jugador.
  * La ruta sencera de l'arxiu p12 del gestor.

- Executar Jugador.bat (per a windows). En cas de Linux cal adaptar el fitxer, tot i que es possible que funcioni tal qual.

- Prémer el botó "Iniciar partida".

- Demanar cartes fins finalitzar la partida o prémer "fi partida".

- Per sortir prémer el botó "sortir".