UNIVERSITAT OBERTA DE CATALUNYA

ENGINYERIA TÈCNICA EN INFORMÀTICA DE SISTEMES

TREBALL FINAL DE CARRERA

SISTEMES DE PAGAMENT

Micropagaments amb monedes Payword

MEMÒRIA

Nom Estudiant

CARLOS GARCÍA BUENO

Nom Consultor

ANTONI MARTÍNEZ BALLESTÉ

CURS 2003-2004 QUADRIMESTRE DE PRIMAVERA

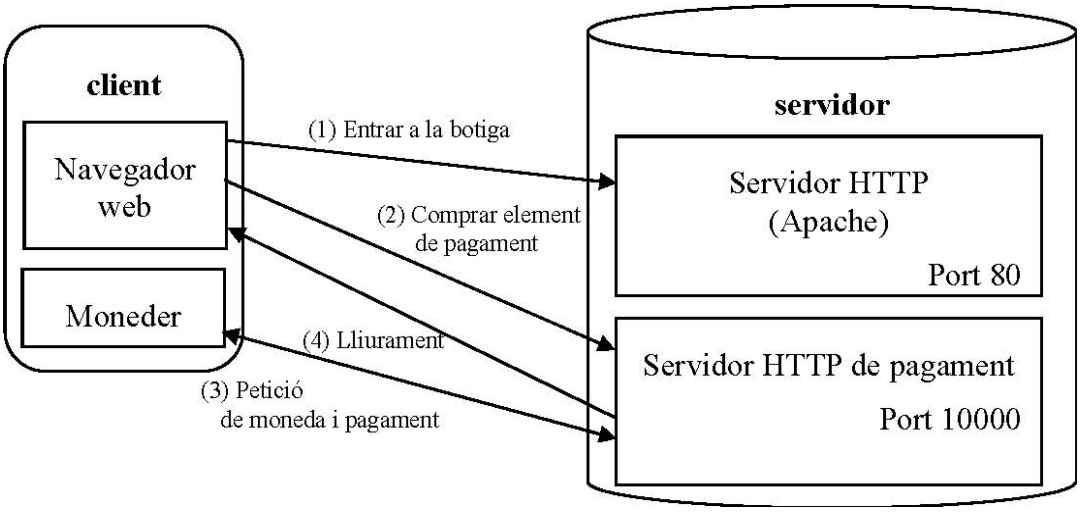
Resumen

Aquesta memòria presenta un projecte per a crear un prototipus on es pugui veure el funcionament dels micropagaments amb monedes payword.

Es realitzarà un sistema de venda d'elements multimèdia (cançons MP3) que es pagui usant el sistema de micropagaments PayWord. Consta de les següents parts:

Un servidor web que, abans de lliurar un element, demanarà al moneder del client un pagament vàlid. Un cop rebut i verificat el pagament, s'enviarà el contingut demanat dins una resposta HTTP.

Un programa moneder, executat al client, que generarà monedes PayWord i farà els tractes amb el servidor HTTP de pagament.



Índex

1. Introducció i estat de l'art.

Aquest projecte tracta el tema del comerç electrònic amb micropagaments per Internet. Per il·lustrar-lo s'ha implementat un prototipus de botiga web que ven fitxers de música per Internet. Els pagaments es realitzen amb monedes PayWord.

No hi ha cap dubte de que Internet està introduint una sèrie de canvis importants en molts aspectes de les nostres vides. No obstant, les tecnologies relacionades amb Internet encara guarden un potencial més gran si cap que el que ja coneixem.

En els darrers anys una sèrie d'aplicacions d'Internet s'han obert camí en els mitjans de comunicació abans de estar disponibles, com pot ser el "comerç electrònic". Poques aplicacions son tan pobres, tecnològicament parlant, com les que actualment s'anuncien com "sol·lucions per a comerç electrònic" i la cosa pot empitjorar si afegim la paraula "segur".

Vol dir això que el comerç electrònic en Internet del que tant es parla i s'escriu no es real?, que no es factible tecnològicament donar una resposta a tant important demanda?. Desgraciadament, la resposta és (pel moment) afirmativa en ambos casos, encara que això no impedeix que la xarxa generi molts diners. Els continus avanços en tecnologia fan preveure que en un futur no molt llunyà estarem en condicions d'afrontar el problema amb millors expectatives que les actuals. El esforç investigador que s'està dedicant és molt important i, més prompte o més tard, produirà els seus fruits.

Però entrem una mica més a fons en les causes de tan fosc panorama. Perquè no es possible realitzar aplicacions de comerç electrònic amb micropagaments per Internet si existeixen altres aplicacions com el correu electrònic, amb complexitat similar?
La raó hi ha que cercar-la en la naturalesa d'aquesta aplicació: els diners. La falta de seguretat de les aplicacions existents té escasa repercussió en el seu ús (o més concretament en la reticència a usar-les). No succeeix el mateix en cas de que hi hagi interessos econòmics pel mig.

Encara que tots tenim una idea sobre en què consisteix l'anomenat "comerç electrònic", ningú sap a ciència certa com es materialitzarà ni fins que punt arribaran els seus potencials, però al menys ja podem fer-nos una idea clara del que pot ser i del que serà mai. Per exemple, no serà el substitut del comerç com avui el coneixem, però si revolucionarà la forma en que les empreses es comuniquen. No serà una sol·lució total, però segur que introduirà noves formes e inclús nous objectes de comerç.

Encara ens falten una sèrie de temes per a aconseguir que el comerç electrònic acabi arrencant:

- Els mitjans de pagament adequats. Aquest TFC tracta una forma possible de realitzar micropagaments.

- La identificació i responsabilitat dels usuaris. És necessari proporcionar mecanismes d'identificació dels usuaris (tan clients com proveïdors) i establir confiança entre els mateixos.

- Mecanismes de protecció dels elements privats. S'han de definir mecanismes fiables per a controlar l'accés a aquests recursos, evitar el seu ús inadequat, protegir els drets d'autor, etc.

- Anominat. Les sol·lucions aportades han de respectar la privacitat o l'anonimat quan sigui necessari.

En aquest moment, l'estat de l'art sobre els pagaments per Internet ens ofereix uns sistemes que permeten realitzar pagaments segurs, no obstant, aquest sistemes estan limitats a transaccions amb un import mínim i estan basades en els sistemes de targetes de crèdit, pel que el seu ús no es suficient per a cobrir totes les necessitats de pagament que es poden produir en el entorn del comerç en Internet. Alguns sistemes de pagament que existeixen són: Millicent, MicroMint, Payword, and Wenbo Mao's, Paypal. En aquest TFC veurem el sistema PayWord.

1.1 Punt de partida i aportació del TFC. El sistema Payword

La publicació tècnica "PayWord and MicroMint – Two simple micropayment schemes" dels autors Ronald L. Rivest i Adi Shamir amb data 7 de maig de 1996 serveix com a punt de partida per a aquest treball.

En aquest informe es detalla el sistema de funcionament del sistema Payword de la següent manera: (s'ha traduït una part del document original anglès)

"El client estableix un compte amb el servidor de pagament, el qual li entrega un certificat digital que conté el nom del servidor, el nom de l'usuari, l'adreça IP de l'usuari, la clau pública de l'usuari, la data d'expiració i altres informacions. El certificat s'ha de renovar amb el servidor (per exemple cada mes), per tal de que el compte de l'usuari sigui vàlid. El certificat autoritza a l'usuari per a crear monedes PayWord, i assegura als venedors que les monedes PayWord del client son acceptades pel servidor de pagament. Assumim que cada moneda val exactament 1 euro (podria ser un altre valor).

En una aplicació típica, quan el client fa clic en un enllaç del venedor en una pàgina no gratuïta, el seu navegador determina si és la primera petició del client per a aquest dia. La primera vegada, el client calcula i signa amb la seva clau privada un "contracte" per a una nova cadena de PayWords específica del client i el venedor:

$w_1, w_2, ..., w_n$. El client crea la cadena payword en ordre invers agafant la darrera PayWord w_n aleatòriament, i després calcula $w_i = hash(w_{i+1})$ per a i=n-1, n-2,…,0. Aquí w_0 es l'arrel de la cadena payword, i no és una payword en sí mateixa. El contracte conté l'arrel w0, però cap payword w_i per a i>0. Llavors, el client presenta aquest contracte i la seva clau pública al venedor, el qual verifica les signatures.

El iéssim pagament (per a i=1,2,…) del client al venedor consisteix en el parell (w_i, i), el qual pot verificar el venedor utilitzant w_{i-1}. Cada pagament no requereix càlculs del client, i només una simple operació de hash pel venedor.

Al final de cada dia, el venedor presenta al servidor l'últim pagament (w_l, l) (l'índex més gran) rebut per cada client aquest dia, juntament amb el seu corresponent contracte. El servidor carrega als comptes dels clients els cèntims i els paga al venedor (el servidor també podria cobrar comissions , però aquí són ignorades)."

En aquest treball construirem un model semblant amb algunes variacions respecte al document de Ronald L. Rivest i Adi Shamir..

1.2 Objectius del TFC. El prototipus del projecte

Aquest treball implementa un prototipus d'aplicació realitzada en Java per a implementar les entitats que apareixen en el esquema PayWord.

En el prototipus implementat intervenen:

- El client que vol adquirir un fitxer de música i que disposa de:
    - Un moneder per generar i pagar amb monedes PayWord
    - Un navegador d'Internet compatible amb Java.
- Una botiga web que disposa de:
    - Un servidor web (Apache, Internet Information Server, etc)
    - Un servidor de pagament que emmagatzema que gestiona els pagaments.
    - Un servidor de fitxers amb protocol HTTP per tal de lliurar els fitxers de música demanats pel client, previ el pagament d'una certa quantitat de monedes payword.

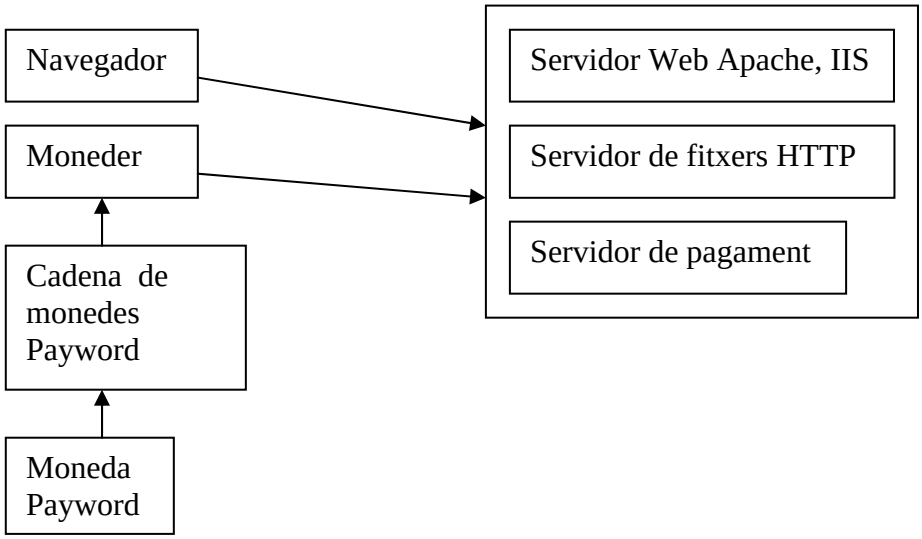
1.3 Aspectes del sistema Payword que no s'han considerat

Hi ha una sèrie de funcions de l'esquema PayWord que no es realitzen per raons de senzillesa del prototipus, segons especificació del professor responsable del treball. Aquest treball pretén mostrar només com utilitzar les monedes Payword sense entrar en l'apartat d'autentificació dels moneders que es connecten a la botiga. Per tant, no es considera el següent:

- Creació d'un certificat digital per a la botiga.
- Sol·licitud a la botiga d'un certificat digital per al client
- Generació per part de la botiga del certificat digital del client
- Incorporació del certificat digital del client en el moneder.
- Signatura de la moneda inicial (contracte) del moneder amb el certificat digital del client.
- Quan el moneder envia la moneda inicial a la botiga, no s'adjunta la seva clau pública RSA
- Verificació per part de la botiga de la signatura de la moneda inicial rebuda del moneder.

Assumim doncs, que les monedes rebudes són autèntiques i legals per a utilitzar en la botiga.

2. Els elements del prototipus



2.1 Les monedes payword

Les monedes payword que utilitzarem en aquest projecte seran creades pel moneder del client i seguiran la estructura del model de Rivest especificat abans.

2.2 Les cadenes de monedes payword

Anomenarem "cadena payword" al cada conjunt de n monedes generat pel moneder, més la moneda inicial W0. Si es realitza un pagament de 3 monedes, el servidor de pagament emmagatzemarà la moneda inicial w0, la darrera moneda i el número de monedes rebudes de la cadena. Si el client utilitza el moneder per a fer un segon pagament, com que la moneda inicial serà la mateixa, el servidor afegirà més monedes a la mateixa cadena payword. Si el client esborra les monedes i crea de noves, llavors tindrem una nova cadena payword formada per una nova moneda inicial i per la resta de monedes. El servidor guardarà les noves monedes rebudes, apart, en una nova cadena de pagament. Si el moneder perd una moneda en la transmissió, el servidor ja no pot acceptar cap moneda més de la cadena. Per tant, el client haurà de esborrar les monedes sobrants, tornar a crear més monedes en el moneder i el servidor ho detectarà com una cadena nova vàlida de pagament.

2.3 El moneder del client

És una aplicació JAVA que permet connectar-se al servidor de pagament, crear i enviar les monedes. Aquest disposa de les opcions: connectar-se al servidor, desconnectar-se del servidor, activar moneder, enviar monedes, desactivar moneder, crear monedes, esborrar monedes i sortir, a tal efecte. Esborrar les monedes no comporta cap pèrdua econòmica, ja que només és important el nombre de monedes que el servidor de pagament hagi rebut correctament de cada cadena payword. La moneda inicial W0 es guarda en el fitxer de text "monederw0.dat" i la resta de monedes en el fitxer de text "moneder.dat". Aquests fitxers són generats automàticament pel moneder.

2.4 El servidor de pagament

Al servidor de pagaments es poden connectar diversos moneders a l'hora i un servidor de fitxers HTTP. El servidor de pagament emmagatzemarà les cadenes payword rebudes de cada moneder i les exportarà a un fitxer de text. Aquest fitxer de text, pot ser utilitzat per a sol·licitar al banc el reemborsament dels diners.

2.5 El servidor de fitxers HTTP

Aquesta aplicació JAVA és l'encarregada de servir les peticions HTTP que arriben des dels navegadors d'Internet dels clients. Normalment la petició arribarà d'aquesta manera:

http://localhost:10001/nomFitxer.zip&id=1&quantitat=3

El servidor HTTP extraurà de la URL la informació sobre el fitxer a descarregar, l'identificador del moneder i la quantitat de monedes a pagar. Posteriorment, notificarà al servidor de pagament que el moneder amb identificador id, ha de realitzar un pagament, i s'esperarà fins que es realitzi o fins que s'exhaureixi un interval de temps. Si el pagament s'ha realitzat, es podrà descarregar el fitxer. En cas contrari, es descarregarà una pàgina web "nomoneder.html" indicant que el pagament no s'ha realitzat en el temps requerit.

2.6 La web de la botiga

Consisteix en una sèrie de pàgines web en html i javascript que permeten navegar per la botiga i escollir els fitxers a descarregar. La pàgina inicial es "index.html". Només s'ha implementat la descàrrega en el primer fitxer de musica (Àlbum Gaia, Intèrpret Mago de Oz), per raons de senzillesa del prototipus.

Per a indicar el fitxer a descarregar i el seu preu disposarem d'un applet JAVA que podem insertar en la pàgina web. Aquest applet construirà la URL de la petició HTTP amb el format descrit abans quan es premi el botó "COMPRAR".

```
<APPLET height=200  width=350 align=baseline code=Apcontrol.class>
 <PARAM NAME="an" VALUE="350">
 <PARAM NAME="al" VALUE="200">
 <PARAM NAME="bgcolor" VALUE="E8DF90">
 <PARAM NAME="fgcolor" VALUE="2020F0">
 <PARAM NAME="title" VALUE="Album Gaia - Intérpret Mago de Oz">
 <PARAM NAME="servidor" VALUE="http://127.0.0.1">
 <PARAM NAME="fitxer" VALUE="musica01.zip">
 <PARAM NAME="preu" VALUE="3">
</APPLET>
```

3 El procediment de pagament

El client entra en la pàgina web de la botiga i escolleix el fitxer a descarregar. En el prototipus només es pot descarregar el fitxer "GAIA". La resta no estan activats.

El client connecta el moneder amb el servidor de pagament i activa el moneder.

En la pàgina del fitxer ha descarregar hi ha un applet en el que ha d'introduir l'identificador del moneder. Al prémer el botó "COMPRAR" comença el procés de pagament.

El servidor HTTP:

El servidor HTTP entra en un bucle infinit en espera de peticions de descàrrega de fitxers.

Quan li arriba una petició, es crea un procés independent per tractar-la i torna al bucle infinit.

El servidor HTTP analitza quin fitxer s'ha demanat, quin identificador de moneder li correspon i quina quantitat ha de pagar.

El servidor HTTP comunica al Servidor de pagament que el moneder amb identificador id ha de pagar n monedes.

El servidor HTTP esperarà durant 90 segons a que el servidor de pagament li notifiqui que ha rebut el pagament. En aquest cas, entregarà el fitxer al client. Si no es rep el pagament, entregarà una pàgina html indicant l'error.

El servidor de pagament:

Al iniciar-se espera la connexió del servidor de fitxers HTTP.

Després entra en un bucle infinit en espera de connexions de moneders.

Quan un moneder es connecta, s'obri un procés independent per tractar-lo i continua el bucle infinit.

Quan el servidor de fitxers HTTP li notifica un pagament a realitzar, si el client ha connectat i activat el seu moneder, el servidor de pagament resta a la espera de que li enviïn les n monedes. En cas contrari avisa al servidor HTTP.

El servidor de pagament emmagatzema cada moneda que rep del moneder fins arribar al total de monedes pendents de rebre. Per cada moneda correcta rebuda, s'envia un missatge al moneder per a que l'esborri. Si es rep una moneda incorrecta, s'avisa al moneder i la moneda s'ignora. En aquest cas, el moneder haurà de tornar a crear una cadena de monedes bones. Si les monedes s'han verificat correctament, s'enviarà la conformitat al servidor HTTP.

4 Utilització del prototipus

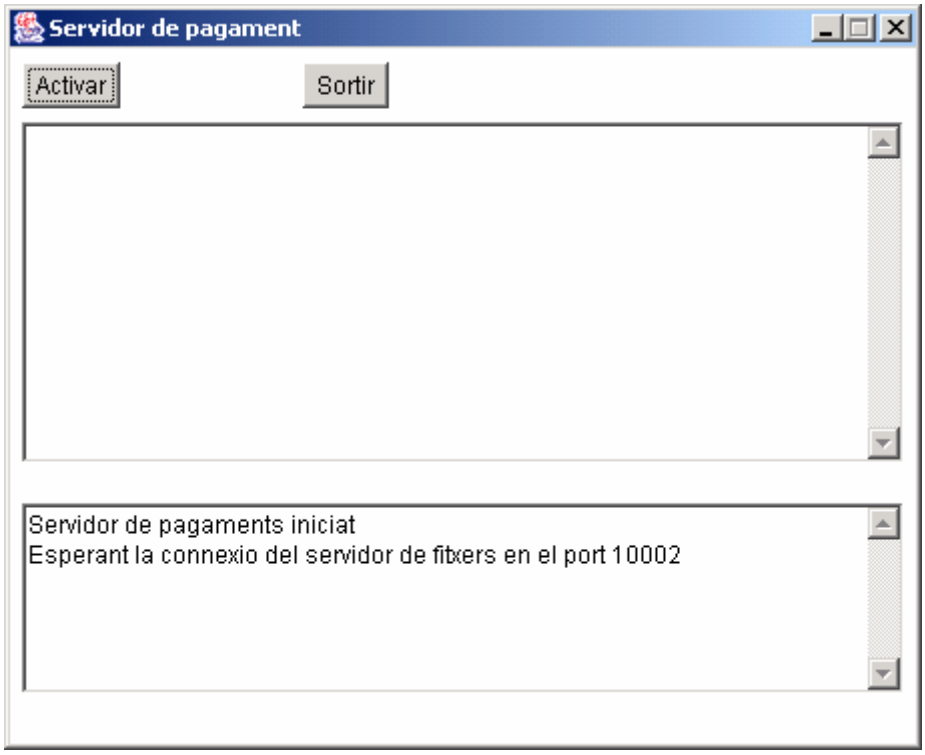
4.1 Exemple de pagament per un fitxer de música

Totes les interfícies disposen d'un quadre de text on podem veure els diferents missatges de control que s'envien en resposta a les accions. Això ens serveix per veure com està funcionant el prototipus i així podem estudiar el seu comportament i aprendre el mecanisme dels pagaments amb monedes payword.

a) Primer hem d'executar el servidor de pagament. Per això obrim una finestra MS-DOS en la carpeta on hem posat els fitxers i executem la instrucció:

java PServPagos

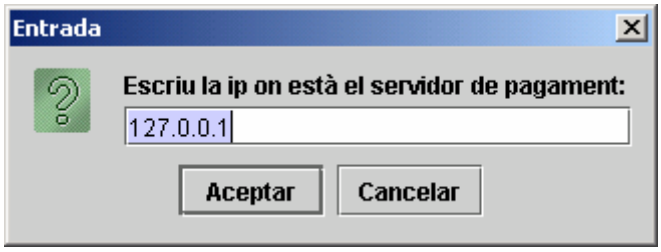
Quan aparegui la interfície gràfica farem clic en el botó ACTIVAR



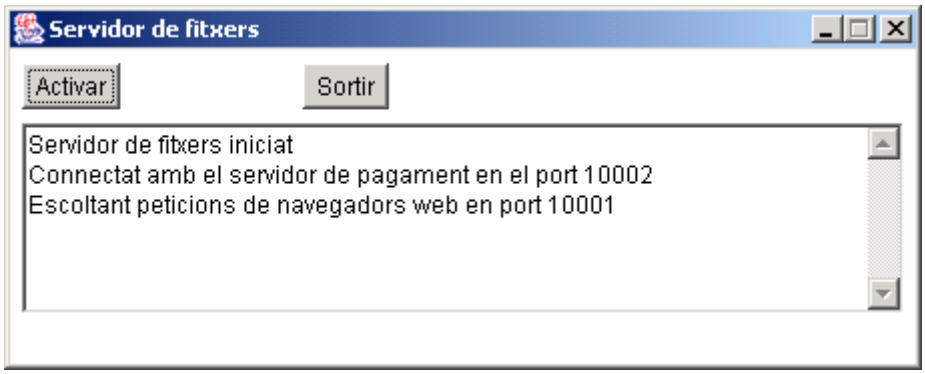
b) Ara executarem el servidor de fitxers de la mateixa manera amb la instrucció:

java FServFitxers

Sortirà un quadre de diàleg on ens pregunta la IP on es troba en execució el servidor de pagament. Podem contestar 127.0.0.1



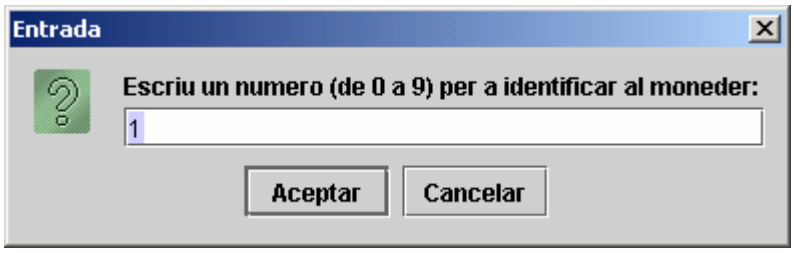
Quan aparegui la interfície gràfica farem clic en el botó ACTIVAR

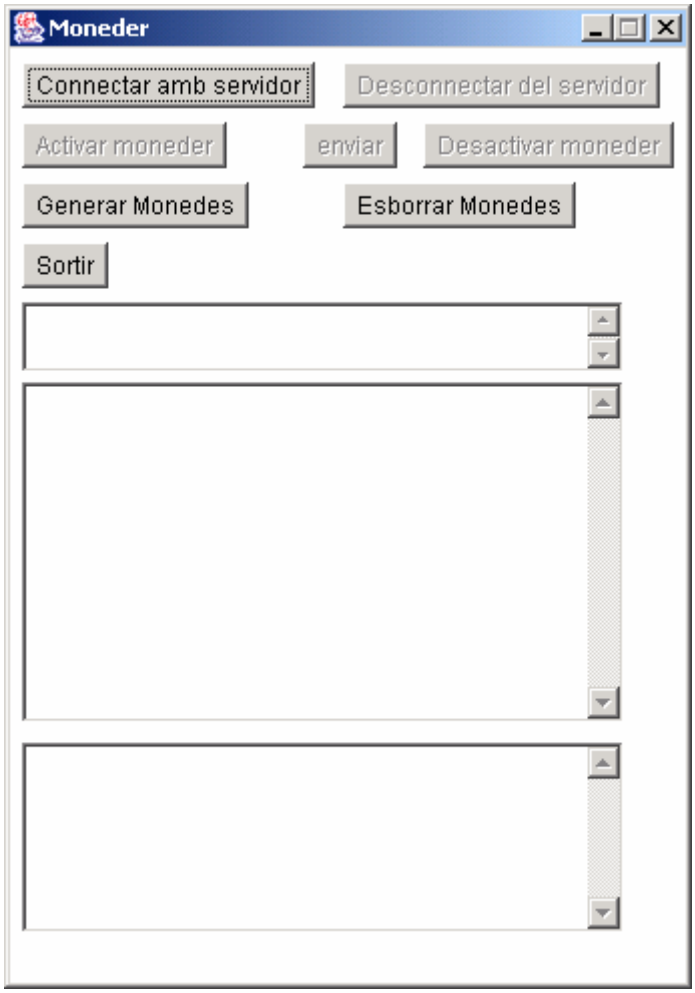


c) Posem en marxa el moneder del client de la mateixa manera amb:

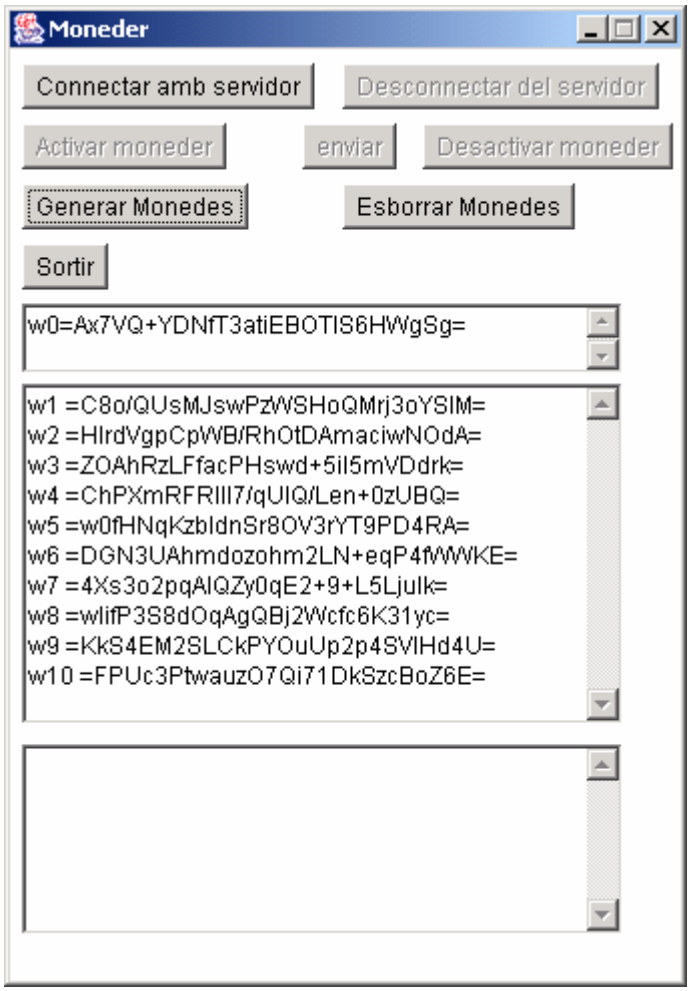
java UClientMoneder

Sortirà un quadre de diàleg on ens pregunta el identificador que volem donar al moneder. Podem contestar amb el numero 1.

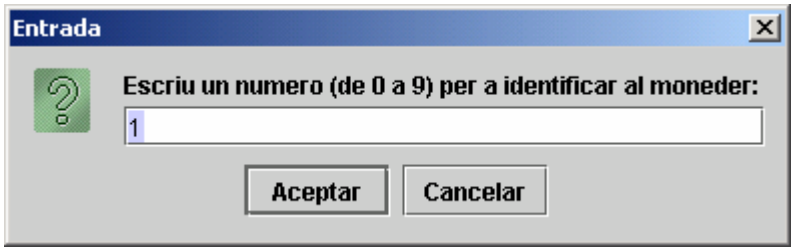


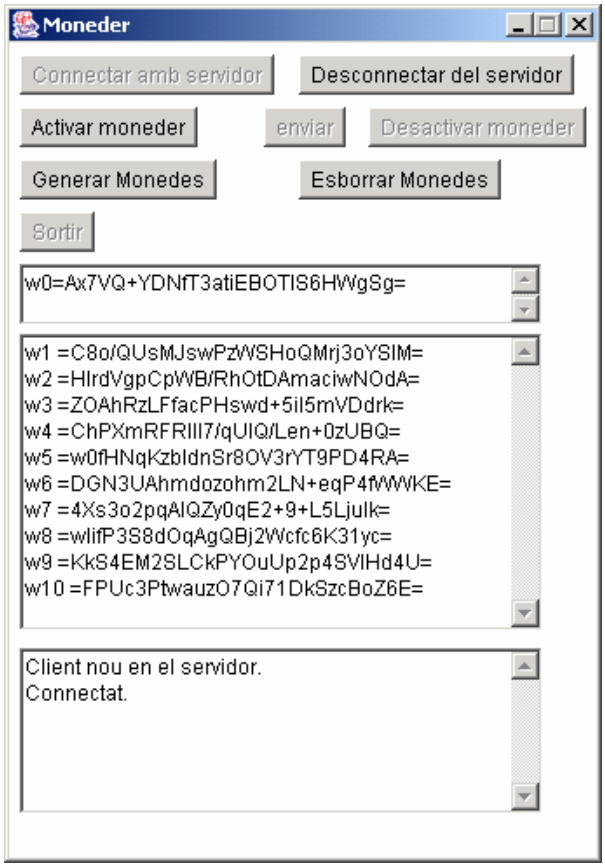


Si no tenim monedes o per a assegurar-nos que tenim una cadena de monedes correcta per a començar, es pot tornar a generar el fitxer de monedes amb el botó "GENERAR MONEDES". Podrem observar la moneda inicial w0 i les monedes generades en el quadre de visualització del moneder. En principi el número total de monedes a generar en una cadena payword és de 10. Es pot canviar en les fonts Java i tornar a compilar-ho.



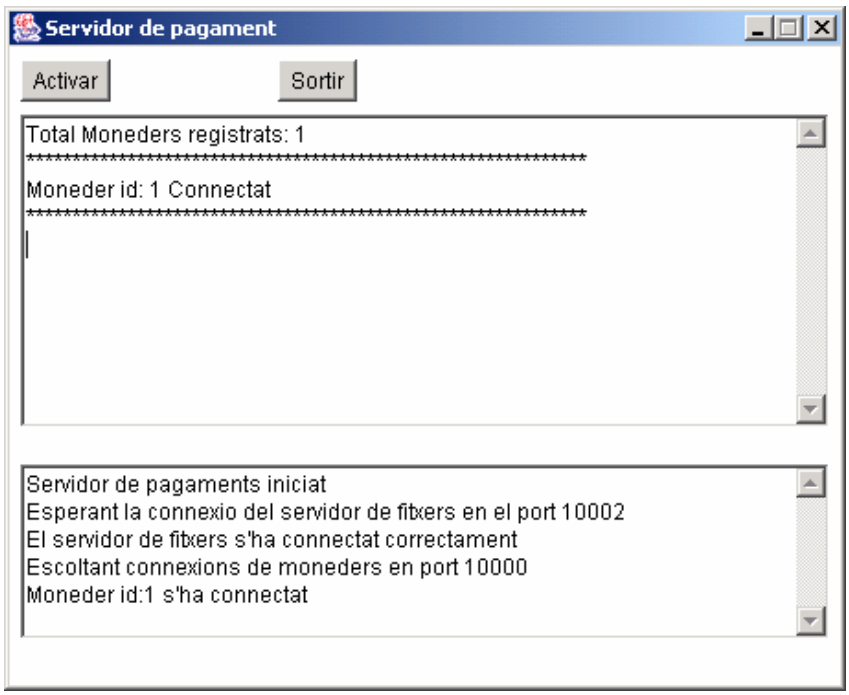
Ara farem clic en el botó CONNECTAR per a registrar el moneder en el servidor de pagament. Si estem connectats, vol dir que, s'ha obert un socket de comunicació del moneder amb el servidor i aquest ha creat un procés independent per al tractament del moneder.



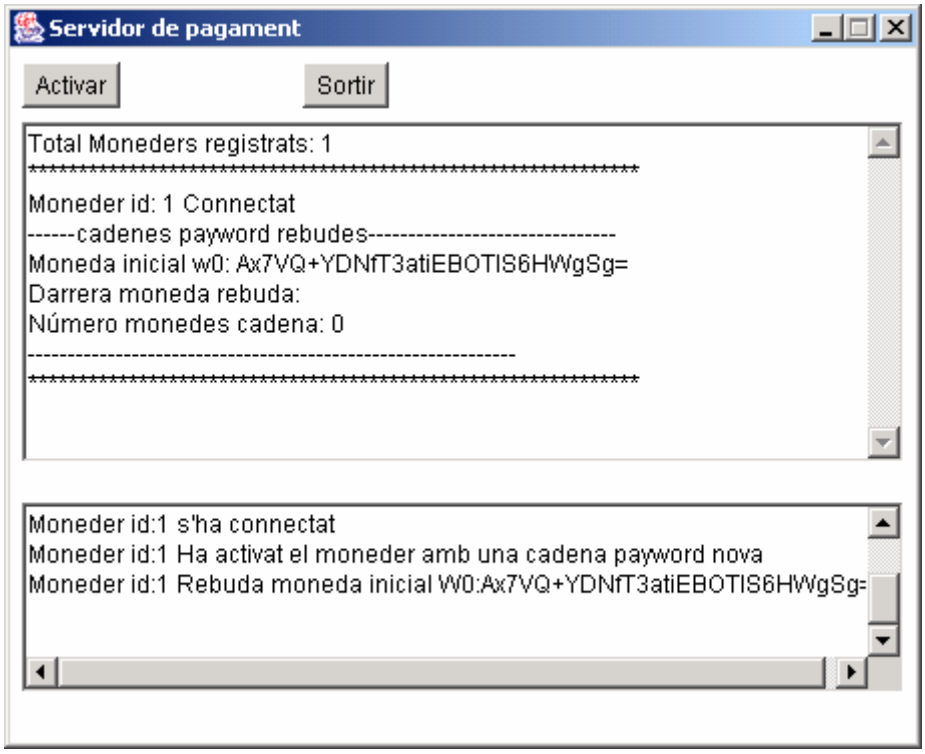


Podem observar els missatges de funcionament en el quadre de text inferior.

El servidor de pagament ha registrat el moneder i ho mostra de la següent manera:

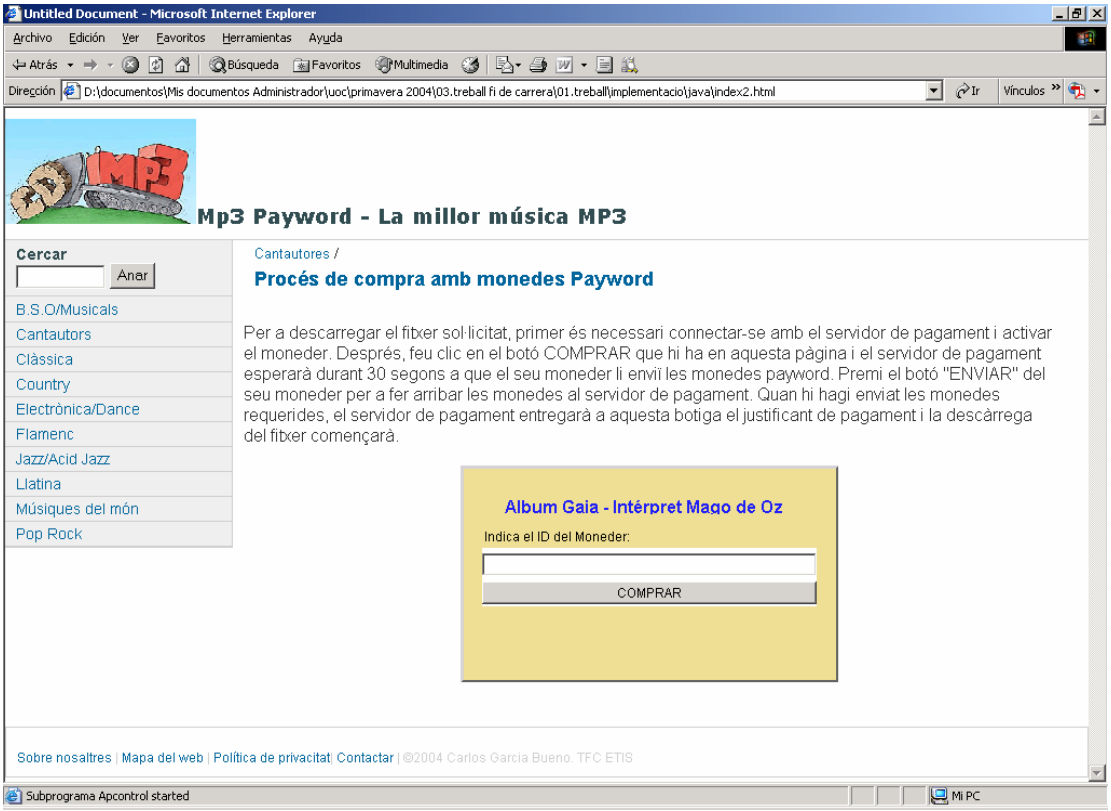


Ens queda ara activar el moneder enviant la moneda inicial W0 (contracte). Això es fa amb el botó ACTIVAR. Veiem com el servidor de pagament mostra que el moneder s'ha connectat i com té una cadena payword oberta amb 0 monedes bones rebudes.



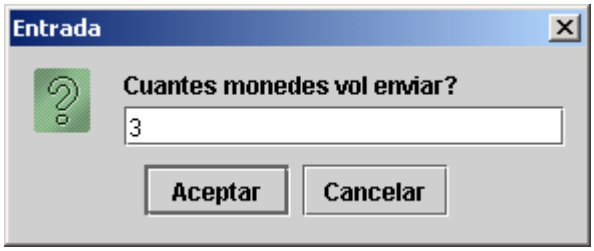
d) Entrarem en la botiga web obrint el fitxer index.html amb el navegador d'Internet.

No tots els fitxers de música es poden descarregar. Només hi ha un enllaç activat. Farem clic en l'enllaç GAIA per a comprar el fitxer de música.

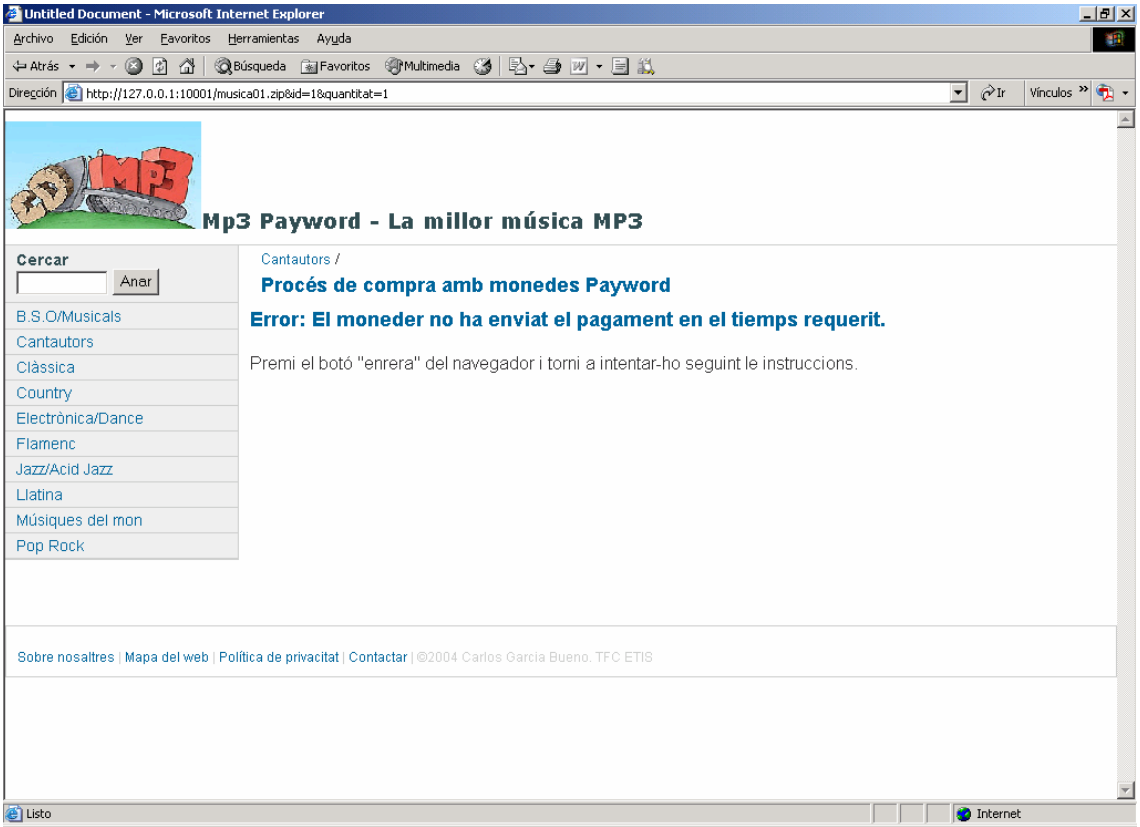


Introduirem l'identificador del moneder (número 1) i farem clic en el botó comprar.

Anem al moneder que tenim activat i fem clic en el botó ENVIAR per a transmetre les 3 monedes.

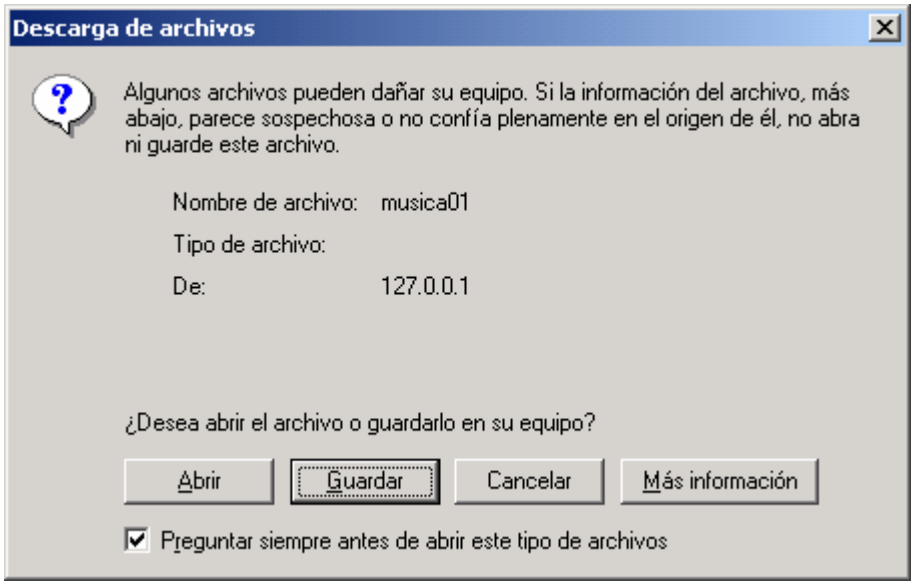


Si no hem enviat les 3 monedes en el temps esperat veurem aquesta pàgina.

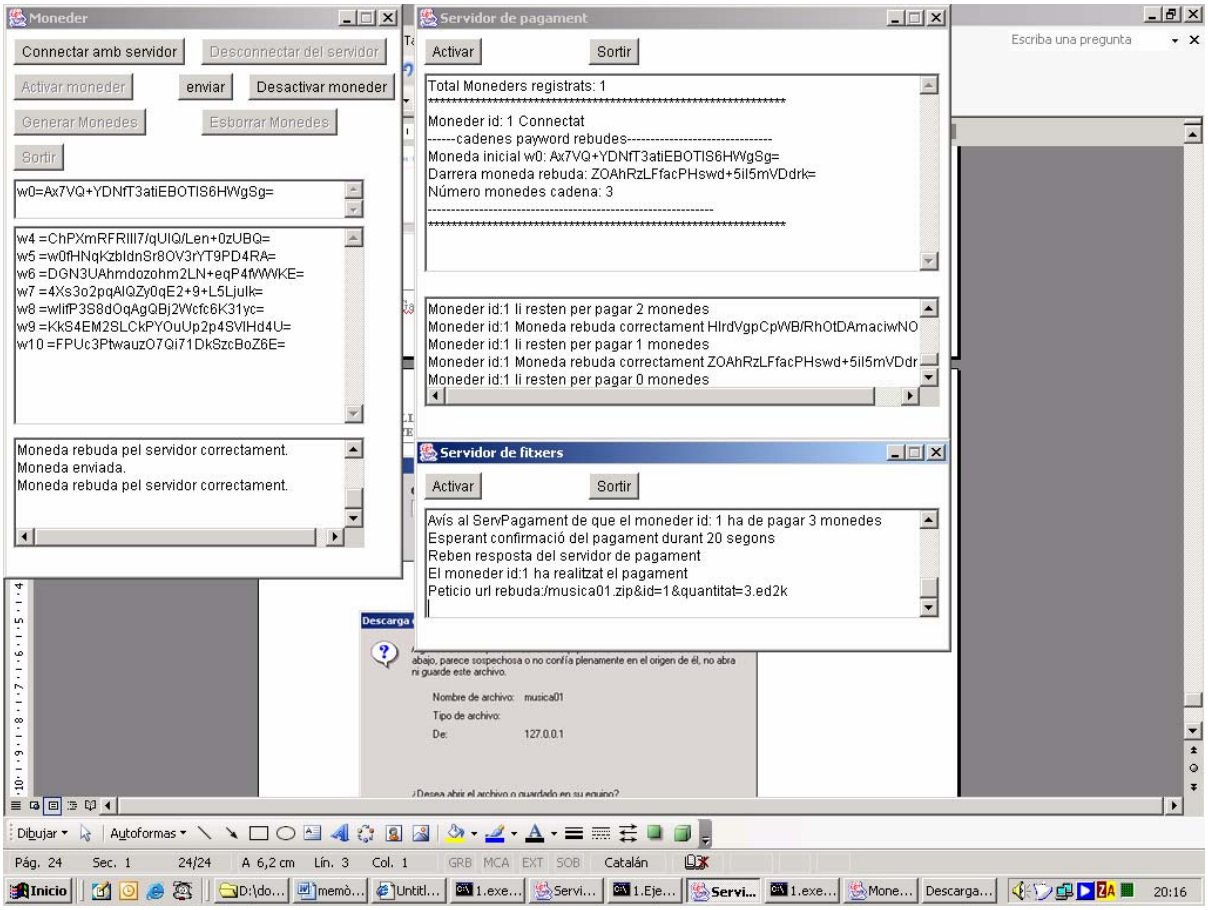


Hem de tenir en compte que una petició http per obtenir una pàgina pot estar composta de varies peticions http independents. Això és perquè hi ha fotos, fitxers d'estil, fitxers flash, etc en una pàgina web. Les peticions de fitxers .zip seran servides previ pagament, totes les altres peticions, son servides gratuïtament per servidor de fitxers HTTP.

En el cas de que li enviem correctament, s'inicia la descàrrega del fitxer sol·licitat.



Observem una mica els missatges de control que s'han enviat els processos:



El moneder rep missatges de confirmació de les monedes que ha enviat al servidor de pagament. El servidor de pagament mostra la cadena payword que ha emmagatzemat amb el pagament fet pel moneder: Té una moneda inicial, la darrera moneda rebuda i ens diu que la cadena és de 3 monedes. El servidor de fitxers HTTP ha rebut la confirmació per enviar el fitxer al client.

Una vegada tanquem el servidor de pagament, poden recuperar el fitxer "pagaments.dat" que ha creat. En aquest fitxer es guarden els pagaments rebuts per tal de presentar-los on calgui:

Fitxer pagaments.dat

Total Moneders registrats: 1
****
Moneder id: 1 Connectat
------cadenes payword rebudes----------
Moneda inicial w0: Ax7VQ+YDNfT3atiEBOTlS6HWgSg=
Darrera moneda rebuda: ZOAhRzLFfacPHswd+5iI5mVDdrk=
Número monedes cadena: 3

****

4.2 Altres Consideracions d'ús

1) Si el servidor de pagament s'atura i es torna a posar en marxa no es carreguen en memòria els pagaments anteriors. Això en un servidor real s'hauria de completar, però per a l'estudi dels pagaments amb payword en aquest prototipus no és necessari.

2) Es poden fer proves amb dos moneders en una mateixa màquina.

3) Els botons del moneder s'activen i desactiven en funció de les accions vàlides en cada moment.

4) Totes les possibles combinacions d'accions entre moneders, servidor de pagament i servidor de fitxers no han estat provades. Per aquest motiu és possible que en algun moment el prototipus no es comporti com esperem. En aquest cas, haurem de reiniciar tots els processos i tornar a generar les monedes.

5) Degut a la cache del navegador si es torna a repetir la operació de compra és possible que es descarregui el fitxer sol·licitat sense enviar més monedes.

4.3 Problemes que ens hem trobat

- Dificultat en trobar documentació en espanyol sobre el sistema payword.

- En ocasions enlloc d'iniciar-se la descàrrega del fitxer .zip, el navegador interpreta el fitxer com a un text i el visualitza.

5 Conclusions

Amb aquest projecte hem pogut veure com funcionen les monedes payword per a realitzar micropagaments per Internet. Aquest projecte és susceptible de ser ampliat, per exemple incorporant els algoritmes RSA per a verificació de signatures digitals, etc.

El sistema payword amb tres entitats: botiga, banc i client té problemes de seguretat.

El sistema permet l'engany tant per part del client com del banc, per la qual cosa és necessari afegir més controls si es vol fer que sigui operatiu.

Un client maliciós pot danyar al banc comprant per més quantitat que el total de crèdit que el banc ha garantit pel l'ús del certificat. En general, hi ha dos possibilitats del banc respecte al certificat. Primera: el banc agafa la responsabilitat completa del certificat i compensa tots els pagaments creats per les compres del client, i segona, el banc no redimeix els pagaments que excedeixen el límit del client i no comparteix la pèrdua amb la botiga si hi ha problemes. En l'esquema payword, el banc pot reduir el seu risc adoptant la possibilitat segona enlloc de la primera. Però, aquest paper implica que el banc pot danyar la botiga en la possibilitat segona, ja que pot personificar un client imaginari i fent que la botiga comparteixi la pèrdua amb el banc.

Si bé el desenvolupament del comerç electrònic encara no acaba de despegar, la realitat és que en els propers anys anirà millorant la situació i es desenvoluparan sol·lucions de micropagaments que aconseguiran els objectius proposats

Glossari

Cadena Payword	conjunt de monedes payword rebudes pel venedor
Certificat	Identificació expedida per una autoritat de certificació que identifica a un usuari.
Contracte	Moneda inicial w0 d'una cadena de monedes payword.
Hash	Funció que s'aplica a un contingut per a obtenir un resum
Micropagament	pagament d'una quantitat més petita del que és habitual
Moneda Payword	moneda definida per Rivest i Shamir per a realitzar pagaments per Internet
Moneder	aplicació que permet generar i enviar monedes payword
Socket	canal per a comunicar dos processos amb TCP/IP

Bibliografia i recursos

- Mòduls Assignatura Criptografia. Estudis d'Enginyeria Tècnica Informàtica de Sistemes. UOC
- Mòduls Assignatura Xarxes II Estudis d'Enginyeria Tècnica Informàtica de Sistemes. Universitat Oberta de Catalunya
- Mòduls Assignatura Enginyeria del Programari. Estudis d'Enginyeria Tècnica Informàtica de Sistemes. UOC
- Reference API Specifications Java Sun SDK http://java.sun.com/reference/api/index.html
- Java network programming / Elliotte Rusty Harold Cambridge [etc.] : O'Reilly, 1997 . Catàleg de la UOC
- Programación en Java / Pedro Manuel Cuenca Jiménez Madrid : Anaya Multimedia, 1997
- Electronic Payment Systems (PayWord) Donal O'Mahony, Michael Peirce, Hitesh Tewari; 1997
- "PayWord and MicroMint – Two simple micropayment schemes", Ronald L. Rivest i Adi Shamir, 7 de maig de 1996 http://theory.lcs.mit.edu/~rivest/RivestShamir-mpay.ps
- CHI, E. Evaluation of Micropayment Schemes. Hewlett-Packard Labs.Tech Rep. HPL-97-http://www.hpl.hp.com/techreports/97/HPL-97-14.html
- Comisión Europea. OII Guide to Electronic Payment. http://www2.echo.lu/oii/en/e-pay.html
- SET. Secure Electronic Transaction. http://www.setco.org/

Annexos

Annex A Planificació del projecte

Per tal de realitzar el projecte es van seguir les següents tasques de planificació:
El projecte va ser descompost en una tasca de cerca d'informació (T1), de preparació de l'entorn de treball (T2), de disseny (T3), d'implementació (T4) i de redacció de memòria (T5). Tot seguit es descriuen les tasques i llurs subtasques:

CERCA D'INFORMACIÓ	
T1.1	Cerca d'informació sobre el sistema de micropagaments PayWord.
T1.2	Repàs conceptes sobre els mecanismes d'enviament d'informació en HTTP estudiats a Xarxes II. Recerca de nova informació.
T1.3	Repàs sobre conceptes de comunicació de processos a través de sockets estudiats a Xarxes II. Recerca de nova informació.
T1.4	Repàs de conceptes sobre encriptació d'informació amb funcions de hash SHA1. Recerca de nova informació.

PREPARACIÓ DE L'ENTORN DE TREBALL	
T2.1	Instal·lació i configuració del software de desenvolupament i proves: servidor web IIS, SDK de SUN, Real Java, Microsoft Visió per fer els dissenys de diagrames UML, Macromedia Dreamweaver, etc
T2.2	Còpia en el disc dur de la documentació, pacs i pràctiques de les assignatures relacionades: Criptografia, Enginyeria del Programari, Xarxes, etc., que serviran d'exemples

DISSENY	
T3.1	Dissenyar el programa, a nivell de processos, comunicació i interacció moneder--->servidor pagament Usuari ---------->web botiga
T3.2	Dissenyar el client moneder i decidir-ne les funcionalitats bàsiques (generació de cupons, enviament de cupons, etc)
T3.3	Desenvolupar el programari a alt nivell, amb comentaris i de forma descriptiva. Realitzant aquesta tasca ens poden adonar d'errors de disseny o millores, havent de modificar els resultats de tasques anteriors.

IMPLEMENTACIÓ	
T4.1	Implementació del client moneder i del servidor de pagament. No s'enviaran monedes PayWord en aquesta fase sinó missatges que s'entendran com a pagaments vàlids.
T4.2	Afegiment del mòdul PayWord en el client per a fabricació de monedes i en el servidor per a verificar-les.
lT4.3	Disseny de la web de la botiga

MEMÒRIA	
T5.1	Elaboració de la memòria: objectiu del projecte, estat de l'art i eines de programació utilitzades
T5.2	Elaboració de la memòria: disseny del programa amb diagrames i descripció a alt nivell
T5.3	Elaboració de la memòria: proves, incidències i conclusions
T5.4	Elaboració de la memòria: apèndix amb codi font, degudament comentat
T5.5	Fer presentació del projecte amb PowerPoint o altres aplicacions

La planificació temporal es va endarrerir una mica en alguns apartats però al final es van complir tots els plaços d'entrega:

Setmana		**Dates**	**Activitat**	**Esdeveniment**
1	OK	26 febrer – 29 febrer	Definir els objectius del projecte i l'abast	
2	OK	1 –7 març	Definir les diferents tasques. Realitzar la planificació	
3	OK	8-14 març	Realitzar les tasques de Cerca, preparació de l'entorn de treball i de Disseny	9/03/04 PAC 1 Lliurament planificació
4	OK	15-21 març		
5	OK	22-28 març		
6	OK	29 març – 4 abril	Redactar els capítols provisionals corresponents de la memòria	
	OK	5-11 abril	Realitzar les tasques d'implementació Redactar els capítols provisionals corresponents de la memòria	
8	OK	12-18 abril		13/04/04 PAC2 Lliurament informe Estat del treball
9	OK	19-25 abril		
10	OK	26 abril – 2 maig		
11	OK	3-9 maig		
12	OK	10-16 maig		
13	OK	17-23 maig	Elaborar la presentació Completar la memòria definitiva	17/05/04 PAC3 Lliurament informe Estat del treball
14	OK	24-30 maig		
15	OK	31 maig – 6 juny		
16	OK	7-13 juny		10/06/04 Lliurament provisional
17	OK	14-20 juny	Revisions	18/06/04 Lliurament Final Complert Presentació

Annex B Instal·lació del prototipus

És necessari instal·lar prèviament el SDK Java de Sun. Pot funcionar en Windows i Linux.

El projecte s'entrega complert en un fitxer .zip que hi ha que descomprimir. Una vegada descomprimit, tenim la següent estructura de carpetes:

TFC_Sistemes_Pagament_cgarciabu
- Implementacio
- Javadoc
- Memoria
- Presentacio
- UML

Els fitxers del servidor i del client es poden instal·lar en una mateixa màquina per tal de fer funcionar el simulador que hem creat. Per provar el prototipus cal situar-se en la carpeta implementació i executar:

- Java PServpagos
- Java FServFitxers
- Java UClientMoneder
- Index.html (amb el navegador d'Internet)

Si instal·lem el prototipus en una altra màquina sense incorpora tota la informació del projecte hem de copiar aquests fitxers:

servidor HTTP:

FGestioServFitxers.class
FInterficie$1.class
FInterficie.class
FServFitxers.class
FTractarPeticioWeb.class
FTractarServPagos.class
MiLayout.class
Missatges.class
Semafors.class

Servidor de pagament:

PCadena.class
PDadesMoneders.class
PGestioServPagos.class
PInterficie$1.class
PInterficie.class
PMoneder.class
PServPagos.class
PTractarMoneder.class
PTractarServFitxers.class

La botiga web:

Apcontrol.class
Apform.class
Tapiz.class
index.html
index2.html
nomoneder.html
notrobat.html
alejandrosanz75.jpg
alexubago75.jpg
cantodelloco75.jpg
magodeoz75.jpg
mp3.jpg
redhot75.jpg
1.gif
pixelrojo.gif
musica01.zip
musica01.mp3
2col_leftNav.css
main2.css

En el client s'ha d'instal·lar el moneder. Es pot fer en la mateixa màquina.

UClientMoneder.class
UGestioMoneder.class
UInterficie$1.class
UInterficie.class
MiLayout.class
Missatges.class

Annex C Diagrames UML

En aquest treball s'adjunten en fitxers externs els diagrames UML del disseny, els quals podem obrir amb els enllaços que hi ha a continuació amb "Control+clic del ratolí" en Word 2003 o amb "clic del ratolí" en Word 2000:

DIAGRAMES UML EN FORMAT MICROSOFT VISIO

UML.VSD

DIAGRAMES UML EN FORMAT JPG

CASOS D'ÚS:

UML_casos_us.jpg

MONEDER:

UML-Moneder.jpg
UML_Moneder-UClientMoneder.jpg
UML_Moneder-UGestioMoneder.jpg
UML_Moneder-UInterficie.jpg

SERVIDOR DE FITXER HTTP:

UML_ServFitxersHTTP.jpg
UML_ServFitxersHTTP-FGestioServFitxers.jpg
UML_ServFitxersHTTP-FInterficie.jpg
UML_ServFitxersHTTP-FServFitxers.jpg
UML_ServFitxersHTTP-FTractarPeticioWeb.jpg
UML_ServFitxersHTTP-FTractarServPagos.jpg
UML_ServFitxersHTTP-Semafors.jpg

SERVIDOR DE PAGAMENT:

UML_servpagos.jpg
UML_ServPagos-PCadena.jpg
UML_Servpagos-PDadesMoneders.jpg
UML_ServPagos-PGestioServPagos.jpg
UML_ServPagos-PInterficie.jpg
UML_ServPagos-PMoneder.jpg
UML_Servpagos-PServPagos.jpg
UML_Servpagos-PTractarMoneder.jpg
UML_ServPagos-PTractarServFitxers.jpg

ALTRES:
UML_Applet.jpg
UML_MiLayout.jpg
UML_Missatges.jpg

Annex D Documentació JAVADOC

En aquest treball s'adjunten en fitxers externs els fitxers javadoc de la implementació, els quals podem obrir amb els enllaços que hi ha a continuació amb "Control+clic del ratolí" en Word 2003 o amb "clic del ratolí" en Word 2000:

FITXERS JAVADOC EN FORMAT HTML:

Index.html
Apcontrol.html
FGestioServFitxers.html
FInterficie.html
FServFitxers.html
FTractarPeticioWeb.html
FTractarServPagos.html
MiLayoult.html
Missatges.html
PCadena.html
PDadesMoneders.html
PGestioServPagos.html
PInterficie.html
PMoneder.html
PServPagos.html
PTractarMoneder.html
PTractarServFitxers.html
Semafors.html
UClientMoneder.html
UGestioMoneder.html
UInterficie.html

Annex E Codi Font en Java

En aquest treball s'adjunten en fitxers externs els fitxers amb el codi font en JAVA, els quals podem obrir amb els enllaços que hi ha a continuació amb "Control+clic del ratolí" en Word 2003 o amb "clic del ratolí" en Word 2000:

FITXERS AMB CODI FONT EN JAVA:

Apcontrol.java
FGestioServFitxers.java
FInterficie.java
FServFitxers.java
FTractarPeticioWeb.java
FTractarServPagos.java
MiLayout.java
Missatges.java
PCadena.java
PDadesMoneders.java
PGestioServPagos.java
PInterficie.java
PMoneder.java
PServPagos.java
PTractarMoneder.java
PTractarServFitxers.java
Semafors.java
UClientMoneder.java
UGestioMoneder.java
UInterficie.java

Annex F Altres fitxers adjunts al treball

En aquest treball s'adjunten en fitxers externs altres fitxers interessants, els quals podem obrir amb els enllaços que hi ha a continuació amb "Control+clic del ratolí" en Word 2003 o amb "clic del ratolí" en Word 2000:

PayWord and MicroMint - Two simple micropayment schemes (en format PDF)
Ronald L. Rivest i Adi Shamir