Departament de Ciències Matemàtiques i Informàtica

UNIVERSITAT DE LES ILLES BALEARS

PROTOCOLS DE SEGURETAT AMB TERCERES PARTS: EL PROBLEMA DE LA CONFIANÇA I LA PROPIETAT DE VERIFICABILITAT

TESI DOCTORAL

Macià Mut Puigserver
Director: Josep Lluís Ferrer Gomila

Departament de Ciències Matemàtiques i Informàtica

UNIVERSITAT DE LES ILLES BALEARS

PROTOCOLS DE SEGURETAT AMB TERCERES PARTS: EL PROBLEMA DE LA CONFIANÇA I LA PROPIETAT DE VERIFICABILITAT

Tesi Doctoral presentada per optar al grau de Doctor
en Informàtica per la Universitat de les Illes Balears

Autor: Macià Mut Puigserver
Director: Dr. Josep Lluís Ferrer Gomila

2006

El sotasignant, Dr Josep Lluís Ferrer Gomila, Doctor en Informàtica per la Universitat de les Illes Balears i professor titular d'universitat del Departament de Ciències Matemàtiques i Informàtica de la Universitat de les Illes Balears,

FAIG CONSTAR:

Que la present tesi titulada *Protocols de Seguretat amb Terceres Parts: El Problema de la Confiança i la Propietat de Verificabilitat*, ha estat realitzada sota la meva direcció per en Macià Mut Puigserver per optar al grau de Doctor en Informàtica per la Universitat de les Illes Balears.

I perquè consti, signo la present

Palma, 27 de juny de 2006

Dr. Josep Lluís Ferrer Gomila
Director de la Tesi

A na Francina i en Mateu

TAULA DE CONTINGUTS

Capítol 1

Introducció

Les comunicacions electròniques van adquirint una gran importància i ofereixen noves possibilitats en els intercanvis d'informació, sobretot en el camp de les transaccions comercials i en l'anomenada administració electrònica. En el món "no electrònic" aquestes transaccions dutes a terme mitjançant amb mitjans més convencionals presenten problemes de seguretat i desconfiança (l'arbitratge de terceres parts com, per exemple, jutges, policies, notaris, agents postals entre d'altres, ha donat tradicionalment seguretat en aquests intercanvis). En els transaccions electròniques, dutes a terme mitjançant protocols de comunicació, la seguretat també té un paper cada cop més rellevant perquè dóna una protecció contra possibles amenaces, com són les manipulacions desautoritzades de les dades o les falsificacions. Així doncs, alguns aspectes de la seguretat en les transaccions electròniques són l'eix d'aquesta tesi.

Diverses institucions, tant públiques com privades, han desenvolupat sobre Internet serveis de seguretat com l'autenticació, el control d'accés, la confidencialitat de dades, la integritat de dades o les evidències de no rebuig d'origen i/o recepció, en aplicacions com transaccions electròniques en la web, comerç electrònic, correu electrònic, servei de directori (DNS, X.500, LDAP), EDI o diners electrònics. Aquests protocols pretenen ésser la versió electrònica dels procediments que s'han estat utilitzant en el món convencional on les transaccions s'han fet normalment entre persones reunides en una sala i el suport emprat per als documents ha estat el paper. En canvi, en aquests nous procediments, les transaccions es faran entre entitats remotes i el suport emprat per als documents és l'electrònic. La seguretat, com en el cas dels procediments convencionals, ha de tenir, doncs, una funció cabdal.

Les solucions proposades en els articles científics sobre els intercanvis d'informació electrònics entre dues parts no sempre tenen una implementació senzilla i pràctica. És per això que sovint s'involucren en l'intercanvi terceres parts que actuen com a entitats que

ajuden a resoldre i simplificar el problema, però, a canvi, els usuaris han de dipositar una certa *confiança* en les seves accions. D'aquí ve que es pugui definir *confiança* [C04] com el mètode subjectiu per reduir la complexitat, tot assumint, en base a un coneixement subjectiu limitat, les accions beneficioses d'entitats independents. D'aquesta manera la confiança es converteix en un mitjà per tractar amb la complexitat i dur-la a nivells manejables. És a dir, mitjançant la introducció de terceres parts en el protocol, es pretén trobar solucions més pràctiques per als protocols de comunicació amb problemes de seguretat.

En conseqüència, podem trobar nombroses propostes que incorporen Terceres Parts de Confiança (TTP, per l'acrònim en anglès *Trusted Third Party*) amb la intenció de ser procediments electrònics pràctics, simples de cara a l'usuari. A més a més, les característiques de seguretat d'aquests procediments són un factor clau. Ara bé, si ens fixam en definicions de confiança com la que trobam a [JL04], que es refereixen al terme com l'extrem pel qual una part vol dependre d'algú, o d'alguna cosa, en una situació donada i amb un sentiment de relativa seguretat, encara que hi pugui haver conseqüències negatives, llavors podem deduir que la seguretat de l'intercanvi queda en mans de la conducta de la TTP. Ens sembla, per tant, que la fiabilitat i la seguretat de les TTPs, així com la confiança que s'hi ha de dipositar és un tema que ha de ser tractat, especialment dins l'entorn on actuen, que són els protocols de seguretat, ja que en podem rebre "conseqüències negatives", tal com enuncia la definició anterior.

Aquestes possibles conseqüències fan pensar que en situacions pràctiques no podem suposar que una TTP actuarà com una entitat que proporciona serveis accessibles al públic i que només emetrà evidències vàlides sempre d'acord amb les especificacions del protocol. És a dir, no podem dir que la confiança és garantia per si mateixa del compliment dels requisits de seguretat d'un intercanvi. Per això molts d'usuaris són reticents a l'hora de dipositar confiança en entitats de seguretat remotes i virtuals, cosa que dificulta la implantació i l'extensió de l'ús de procediments electrònics anàlegs als procediments convencionals d'ús freqüent com són l'acció de compra-venda d'un determinat bé, l'emissió d'un correu electrònic certificat, l'ús de diners electrònics per fer les compres a través d'Internet, la utilització d'un procediment de vot electrònic, etc.

Els processos convencionals tenen terceres parts de confiança establertes des de fa molts d'anys. Encara que en alguns casos, fins i tot, poguessin presentar menys garanties objectives de seguretat que les seves homòlogues en versió electrònica, detectam dos factors importants que en faciliten l'ús:

- tradició després d'anys d'implantació
- presència a un lloc físic concret i atenció als usuaris per part de persones físiques

En canvi, la dificultat dels usuaris a posar confiança en una entitat remota dins del context d'una transacció electrònica s'entén pel fet que en el món virtual no comptam amb els factors del món convencional que abans hem esmentat i això és un fre a l'expansió d'aquests procediments electrònics. En publicacions on es proposen nous protocols de seguretat que freqüentment involucren TTPs (per exemple, intercanvi equitatiu de valors, comerç electrònic o l'administració digital) s'han desenvolupat bàsicament dos tipus de solucions a l'hora de resoldre el problema del dipòsit de confiança:

- El primer enfocament consisteix a dissenyar protocols que prescindeixen de l'ús de la TTP, amb la qual cosa eludeixen el problema però, a canvi, el cost de la no inclusió de la TTP és tan elevat que a la pràctica aquests protocols han estat catalogats d'inviables per múltiples autors [AMG01, BGM90, FPH00, GJM99, SM02]. Alguns protocols de seguretat que tenen aquest plantejament els podem trobar a [AT94, B83, D93, E82, EGL85, G84, MR99, TEDIS94].
- El segon enfocament proposa la inclusió de múltiples TTPs en el sistema i, d'aquesta manera, no s'ha de dipositar tota la confiança en una TTP sinó que s'ha de distribuir entre el conjunt de TTPs de forma que el sistema garanteixi la seguretat, encara que una minoria d'aquestes sigui corrupta. Freqüentment, les solucions que s'han aportat amb aquest enfocament empren esquemes criptogràfics llindar (podem trobar referències a aquest tipus d'esquemes a [S96]), cosa que comporta un increment de càlcul molt gran i un augment notable en les comunicacions respecte als protocols que utilitzen esquemes de criptografia simètrica i de clau pública com els formulats a [ASW97, S96]. Aquest inconvenient fa que aquests tipus de propostes [FR95, G93, S96] siguin qualificades d'inviables a la pràctica, com també passa amb les solucions del primer enfocament.

Tenint en compte que, per donar resposta al problema plantejat, qualsevol tipus d'enfocament podria ser vàlid, sempre i quan aconseguís superar les crítiques abans esmentades, hem estudiat les solucions proposades per altres autors pel que fa a protocols d'intercanvi equitatiu de valors. Aquest és un cas paradigmàtic de la implicació de TTPs en protocols de seguretat i encara no té solucions definitives per als casos particulars que responen en aquest model (per exemple: signatura electrònica de contractes, correu electrònic certificat, pagament per rebut, etc.). Després d'això, hem proposat aquí una solució per al correu electrònic certificat, que és un cas particular d'intercanvi equitatiu de valors, on dissenyam un procediment d'enviament d'un missatge certificat amb les característiques de seguretat que requereixen aquests tipus d'intercanvis i que aborda el problema que hem plantejat; és a dir, facilita el dipòsit de confiança en les TTPs per part dels usuaris minimitzant els inconvenients que això pugui plantejar. En concret, aquesta proposta és un protocol de correu electrònic certificat amb múltiples parts de confiança on

una minoria corrupta de TTPs no romp cap de les propietats de seguretat del protocol. És a dir, plantejam el problema des de l'òptica del segon enfocament esmentat anteriorment, però introduïm alguns canvis significatius que ens permeten evitar les principals crítiques que reben aquests tipus de solucions i que hem esmentat anteriorment.

Amb l'ús de la criptografia simètrica i de clau pública hem cercat superar els punts crítics d'aquestes propostes. La nostra principal innovació és l'ús exclusiu d'aquests esquemes criptogràfics més convencionals, per després reduir la necessitat de dipositar confiança en una tercera part perquè s'hi veu involucrada una organització de TTPs que assegura l'equitat de l'intercanvi encara que una minoria d'aquestes no actuï correctament. Per tant, el grup de TTPs garanteix la seguretat sense necessitat d'esquemes criptogràfics llindar, cosa que significa una solució millor que les aportades anteriorment per altres autors, amb una reducció significativa del càlcul i també de la quantitat d'intercanvis. La reducció en la sobrecàrrega en les comunicacions del protocol és més remarcada encara pel fet de tenir un enfocament optimista; això vol dir que no sempre les TTPs es veuran involucrades en protocols, sinó que només serà necessari posar-s'hi en contacte en cas que hi hagi algun problema durant l'execució del protocol bàsic. El fet d'involucrar múltiples TTPs en el protocol de correu electrònic certificat significa que l'usuari no necessitarà posar un alt grau de confiança en una TTP, ja que un error o una conducta malintencionada d'una TTP puntual no malmet la seguretat del sistema. Com és natural, perquè això sigui així, se suposa que ha de ser més fàcil corrompre una TTP que no un grup d'elles.

No obstant això, es fa necessari un estudi de l'actuació dels serveis que donen les TTPs als usuaris davant la dificultat de trobar una solució genèrica al problema; per això explorarem les característiques de la implantació d'aquestes entitats en protocols de seguretat. Volem conèixer la intervenció de les TTPs des de punts de vista diferents per saber quines dificultats pot comportar a un usuari l'ús dels seus serveis. Així, la nostra proposta consisteix en classificar els serveis de les TTPs des de distints punt de vista. Aquestes classificació ens permetrà fer-nos una idea del que suposa la intervenció d'una TTP en els protocols de seguretat. En aquest punt ens podrem fixar que el conjunt de valors resultant d'aquesta classificació recau sobre dos eixos fonamentals: el grau de confiança que els usuaris del protocol han de dipositar en aquestes i el cost addicional en comunicació que comporta la inclusió de la TTP en el protocol. L'anàlisi realitzada ens ha permès obtenir un coneixement més precís de l'actuació de les TTPs en els protocols criptogràfics i les implicacions que això pot tenir. D'aquesta manera hem pogut avançar en la recerca de mecanismes que puguin donar seguretat a un usuari quan ha de dipositar confiança en una tercera part.

Concretament, el primer paràmetre de classificació que presentarem proposa classificar la intervenció de la TTP com a *verificable* o *no verificable* (depenent si l'usuari pot o no pot demostrar un possible incompliment de servei per part de la TTP). La propietat de

verificabilitat fou inicialment definida a [ASW98, FPH00]. La inclusió d'aquesta característica en un protocol determinat ens servirà per poder disminuir d'una forma directa i objectiva la quantitat de confiança que l'usuari ha de dipositar en la TTP i així, millorar l'efectivitat del protocol respecte a altres possibles solucions que utilitzin el mateix enfocament de la primera proposta feta en aquesta tesi (incorporació de múltiples terceres parts en el protocol per tal de disminuir el grau de confiança que un usuari hauria de dipositar en aquestes entitats). En aquesta primera proposta reduïm efectivament la confiança que els usuaris han de dipositar en l'actuació de les terceres parts. Ara bé, hem comprovat que amb la introducció de la verificabilitat en els protocols de seguretat podem minimitzar també el grau de confiança en una tercera part i, a més, no és necessari involucrar en el protocol múltiples terceres parts i d'aquesta manera es poden obtenir protocols més eficients.

La *verificabilitat* és un exemple més de la terminologia que la comunitat virtual ha definit amb relació al problema que estam tractant, és a dir, amb la confiança que els usuaris puguin tenir sobre els nous procediments electrònics. Però hi ha encara alguns conceptes més d'aquesta terminologia relativa al tema, com són els termes *Trust Developement* i *Trust Management* que podem trobar definits a llibres com [TM03, TM04]. *Trust Developement* fa referència a la manera com les distintes entitats virtuals obtenen confiança i també n'incrementen el nivell dins de la comunitat. *Trust Management* determina com la confiança podrà assignar-se, modificar-se o revocar-se. Hom coincideix que les mesures de seguretat són crucials per al *Trust Developement* i que la solució ha de venir del fet que els usuaris han de poder identificar fàcilment entorns virtuals de confiança [IM04]. La *verificabilitat*, en aquest context, pot ser una de les mesures de seguretat que ajudi a donar confiança a l'usuari. Si una tercera part és verificable però no actua correctament i, en conseqüència, es perden les propietats de seguretat del protocol, aleshores els usuaris afectats per aquesta mala actuació podran provar aquest fet davant d'un àrbitre independent. D'aquesta manera, es pot construir aquest entorn virtual de confiança que pot ajudar a vèncer les reticències d'alguns usuaris sobre l'ús d'aquests protocols.

A més del protocol de correu electrònic certificat resistent a una minoria de terceres parts corruptes que ja hem esmentat, les propostes que fem en aquesta tesi van encaminades a aplicar i desenvolupar la propietat de verificabilitat dins dels protocols de seguretat. En el capítol 4 d'aquesta tesi analitzam les característiques de l'actuació de les TTPs en alguns protocols de seguretat i en el capítol 5 comentam les conseqüències que pot tenir la no verificabilitat de la TTP que intervé a coneguts protocols que han estat formulats per altres autors. A partir d'aquí, en els capítols següents, analitzarem les característiques de les operacions de les terceres parts quan donen servei als usuaris de distints tipus de protocols de seguretat i després formularem nous intercanvis en base als protocols originals on demostrarem que aquestes noves propostes compten amb l'actuació d'una TTP

verificable. Per això hem escollit tres casos típics de protocols criptogràfics en què normalment intervenen terceres parts: l'especificació d'un protocol de diners electrònics, d'un protocol de votació electrònica i d'un protocol de correu electrònic certificat. Les distintes solucions proposades per a aquests tres casos en els articles científics solen involucrar TTPs i en cap dels tres casos no s'ha arribat a solucions definitives i satisfactòries. La nostra proposta, com ja hem explicat, consisteix a afegir la propietat de verificabilitat a un protocol ben conegut de cada un d'aquests casos. Llavors direm que la tercera part de confiança involucrada en el protocol és verificable. Això significarà que l'usuari disposarà en tot moment d'evidències que demostraran com la TTP ha gestionat la seva petició i, en cas de discrepància, tendrà al seu abast elements suficients per corregir la situació.

Les propostes anteriors mostren com a partir d'un determinat protocol de seguretat podem aconseguir que la TTP involucrada sigui verificable. Es tracta de construir aquest entorn de confiança dins del protocol per mitjà del subministrament d'evidències sobre cada una de les operacions de la TTP a l'usuari. Hem aconseguit això gràcies a la detecció, l'anàlisi i la posterior classificació de cada una de les accions de la tercera part de confiança. Un cop superada aquesta fase, podem procedir a modificar cada una d'aquestes accions de manera que pugui ser classificada com a verificable. Aquest sistema ens ha permès introduir la verificabilitat dins dels protocols sense que això comporti la renúncia a cap altra característica de seguretat, tan sols amb un augment pràcticament negligible de la quantitat d'intercanvis del protocol i de la capacitat de càlcul necessària per executar-lo. Aquest sistema s'ha traduït en propostes concretes que detallarem més endavant en aquest document.

El treball d'introduir la verificabilitat dins de protocols de seguretat tan diversos ens ha permès definir amb més detall tot l'entorn d'aquesta propietat. Els primers apartats del capítol 5 estan dedicats a aquesta aportació de la tesi: proposam noves definicions i distingim nous conceptes (sempre d'acord amb la terminologia emprada oficialment en els documents estàndards [X.400, X.500, X.800, ISO7498] promoguts pels organismes internacionals reconeguts) per poder aplicar la verificabilitat dins dels protocols de seguretat, definint els elements de seguretat que la TTP utilitza per donar servei a les peticions dels usuaris i distingint per primera vegada dos tipus de verificabilitat: *on-line* i *off-line*. Consideram *on-line* la *verificabilitat* quan l'usuari d'un servei rep evidències sobre l'operació de la TTP que està proporcionant el servei sol·licitat; aquestes evidències demostren de forma immediata si la TTP ha actuat correctament o no. La *verificabilitat* serà *off-line* si les evidències rebudes per un usuari no serveixen per demostrar si la TTP ha proporcionat de forma correcta el servei sol·licitat; en canvi, si posteriorment sorgeix una disputa entre les parts involucrades en el protocol, llavors la comprovació de totes evidències rebudes per les diferents parts demostrarà la bona o mala actuació de la TTP. Aquesta distinció ens permet ser més acurats i estrictes alhora d'analitzar les operacions

de les TTPs i, per tant, podem ser més precisos quan introduïm la propietat en un protocol; per exemple, nosaltres consideram que la tercera part és verificable només si la verificabilitat que ofereix en els seus serveis és *on-line*. Aquest conjunt de definicions també ens ajudaran a demostrar d'una forma més categòrica si una TTP és verificable o no.

Una conseqüència d'aquest treball d'anàlisi de la intervenció d'una TTP en un protocol, ha estat la catalogació de les tasques fonamentals que realitza una TTP en tres grans conjunts: *recepció* de les peticions dels usuaris (inclou el fet comprovar la correcció de la petició), *generació i emissió* d'ítems d'informació a l'usuari (com per exemple la confirmació o la cancel·lació d'una determinada transacció) i la *comprovació* de l'estat d'una transacció (cosa que també inclou l'actualització d'aquest estat en funció dels esdeveniments). A partir d'aquí hem pogut aportar unes orientacions de disseny de protocols que faciliten la introducció de terceres parts verificables dins dels protocols de seguretat. Aquestes orientacions es poden resumir de la manera següent: per operacions del tipus *recepció* s'ha de tenir en compte que és necessari que l'usuari sempre obtengui una resposta de la TTP a la seva petició (encara que la seva petició sigui errònia). La resposta ha de servir d'evidència de no rebuig de recepció. Per operacions del tipus *generació i emissió* de missatges emesos per una TTP com a resposta a la petició de servei d'un usuari, s'ha de tenir present que aquest missatge tengui la propietat de no rebuig d'origen i han d'estar lligats a la petició de l'usuari a través d'un mateix identificador. Per operacions del tipus *comprovació* i actualització de l'estat d'una determinada transacció és necessari que siguin operacions públiques si les volem verificables. Pensam, per això, que és una bona pràctica que les terceres parts de confiança expressin els estats de les transaccions a través de missatges publicats a directoris públics mantenguts per la mateixa entitat.

Cada una d'aquestes orientacions està pensada perquè, quan sigui aplicada en el disseny d'un protocol, els usuaris obtenguin evidències de no rebuig de cada una de les operacions que fa la TTP per donar servei a l'usuari i, d'aquesta manera, els serveis de la TTP tenguin *verificabilitat on-line*. Per mostrar això i tenint com a punt de partida les orientacions de disseny abans esmentades, aportam un nou protocol de seguretat que té com a característica una TTP verificable. Aquesta nova aportació no és la introducció de la verificabilitat dins d'un protocol ja definit sinó l'especificació d'un nou protocol on les directives de disseny ens han assegurat el compliment d'aquesta nova propietat tal i com demostrarem en el capítol 9 d'aquesta tesi.

Per a aquesta nova proposta hem tengut en compte que el tipus de protocols on més s'ha ressenyat el concepte de verificabilitat és en els protocols d'intercanvi equitatiu de valors. Per això hem escollit aquesta classe d'intercanvis per aplicar les nostres orientacions en el nou disseny d'un protocol per al correu electrònic certificat, que és un cas particular de

d'intercanvi equitatiu i que, com ja hem esmentat abans, encara no disposa d'una solució plenament satisfactòria i que s'hagi adoptat com a definitiva i estàndard. És per això que en el capítol 9 hem dissenyat un nou protocol on hem adoptat com a punt de partida la verificabilitat i les seves orientacions de disseny. El resultat és un protocol de correu electrònic certificat que no tan sols compleix la fita de verificabilitat sinó també les principals exigències i propietats que ha de tenir un protocol d'intercanvi equitatiu [KMZ02]. Així l'usuari té una seguretat i unes garanties afegides (la *verificabilitat forta* de les accions de la TTP) que faciliten i milloren la confiança de l'usuari sobre l'èxit de la transacció, quan fa servir aquest protocol.

D'acord amb tot això que hem exposat, pensam que és necessari donar més seguretat als usuaris pel que fa a les accions de terceres parts si volem expandir i facilitar l'ús dels nous procediments electrònics. Com podrem veure, les solucions donades en aquesta tesi van en aquest sentit. La primera solució aportada proposa donar aquestes garanties de seguretat als usuaris incorporant múltiples terceres parts de confiança i aconseguint que el protocol preservi la seguretat de l'intercanvi fins i tot si una minoria de les terceres parts involucrades és corrupta. En aquesta proposta, com ja veurem, també aconseguim minimitzar les crítiques que es fan a aquest tipus d'enfocament tot i que per la seva naturalesa és necessari incloure múltiples TTPs, cosa que suposa un cost superior en comunicacions que si tenim només una tercera part de confiança. No obstant això, hem cercat noves solucions involucrant una única TTP i introduint la propietat de verificabilitat en els protocols de seguretat. Aquesta ha estat una manera de crear, d'una forma directa i senzilla, un entorn virtual de confiança. L'objectiu és donar més seguretat als serveis que proporciona una TTP dins d'un protocol de seguretat pel fet de subministrar a l'usuari evidències sobre com s'està gestionant la seva petició. Per això hem orientat les nostres propostes en dos sentits: primerament, hem mostrat com podem introduir la verificabilitat dins d'un protocol ja definit i, en segon lloc, hem dissenyat un nou protocol d'acord amb unes orientacions que ens permeten introduir i demostrar que la tercera part involucrada en el protocol és verificable. També és important la ressenya que fem de la propietat de verificabilitat i la distinció que aportam entre la verificabilitat forta i la dèbil. Tal i com demostram, la verificabilitat aconseguida a les nostres propostes és forta, cosa que dóna unes garanties més immediates i evidents sobre la seguretat de l'intercanvi.

Cada una de les aportacions que hem esmentat en aquesta introducció està desenvolupada en els capítols d'aquesta tesi. El següent capítol revisa com pot ser la intervenció d'una tercera part en un protocol i el problema associat al dipòsit de confiança. En el tercer capítol detallam la nostra proposta de protocol de correu electrònic certificat resistent a una minoria de TTPs corruptes. En el quart capítol proposam una classificació dels serveis de seguretat proporcionats per TTPs i introduïm els nous conceptes relatius a la propietat de verificabilitat d'una tercera part. En el capítol cinc revisam la verificabilitat en els protocols de seguretat i definim els conceptes que hem associat en aquesta propietat. En

els capítols sis, set i vuit explicarem les nostres propostes per fer una anàlisi dels serveis que proporciona una tercera part de confiança en un protocol de diners electrònics, de vot electrònic i d'intercanvi equitatiu, respectivament. Després d'aquesta anàlisi, en cada un d'aquests capítols, veurem com podem convertir la tercera part involucrada en els protocols anteriors en una TTP verificable. Posteriorment en el capítol novè proposam una sèrie de recomanacions per dissenyar protocols amb TTP verificables. En el mateix capítol dissenyarem un nou protocol de correu electrònic certificat, seguint les recomanacions anteriors, i demostrarem que la TTP involucrada té verificabilitat forta. Finalment en el capítol desè exposarem les conclusions de la tesi.

Per acabar aquesta introducció vull donar les gràcies a aquelles persones que, d'una manera o d'una altra, m'han ajudat a dur aquest projecte endavant.

En primer lloc, vull expressar el meu agraïment més sincer al Dr. Josep Lluís Ferrer, per la seva disposició a dirigir la meva recerca. He d'agrair-li l'empenta, la iniciativa, la dedicació, els suggeriments i les crítiques que han fet que aquesta tesi pugui veure la llum. La seva qualitat científica i humana ha fet molt agradable aquest treball.

Al Dr. Llorenç Huguet, de qui he après molt, la persona que em va donar la confiança i el suport per començar a investigar. La seva humanitat i capacitat de treball han aconseguit fer fàcil allò que semblava difícil.

A la companya de recerca Dra. Magdalena Payeras pel que m'ha sabut transmetre d'il·lusió i rigor professional.

Faig extensiu el meu agraïment als companys de feina i als amics que sempre sent al meu costat i amb els quals compartesc inquietuds.

Un record molt especial es mereixen els meus pares, pel suport i l'exemple que tota la vida m'han donat. La il·lusió que ells han dipositat en mi ha estat la força que m'ha permès dur a terme aquesta tesi.

Finalment vull agrair de tot cor a na Maria no només el seu inestimable ajut i consell, sinó també, i per sobre de tot, el seu desig de compartir un viatge i no dubtar mai que arribarà a bon port.

Capítol 2

Protocols de seguretat i terceres parts de confiança

2.1 Introducció

Els requeriments de seguretat dins d'una organització han experimentat canvis notables després de la introducció i l'ús de les tecnologies de la informació, especialment després d'expansió de l'ús de les xarxes telemàtiques. La dispersió geogràfica dels equips multiplica les possibilitats d'atacs i d'operacions no autoritzades. D'aquí que cobrin valor totes aquelles mesures que van encaminades a augmentar la seguretat en les comunicacions. *Seguretat de Xarxes* o *Internetwork Security* són termes que designen els entorns i les mesures que es poden prendre per introduir la seguretat en les comunicacions. A [CG04, S95, S96] podem trobar definits aquests termes així com moltes de les tècniques que s'utilitzen per minimitzar la vulnerabilitat dels sistemes. Encara que, com queda palesa en aquestes referències, la protecció total o el que també s'anomena seguretat total no és possible, ja que quan es construeix un escut de protecció contra un determinat atac, sempre serà possible concebre un atac més fort que rompi aquest escut.

Per regular la seguretat, els organismes internacionals (principalment l'ITU-T i l'ISO, d'una banda, i els comitès de la Internet Society, de l'altra) han elaborat una sèrie de normes que serveixen de referència per al desenvolupament de la seguretat en les xarxes telemàtiques. El Model de Referència per a la Interconnexió de Sistemes Oberts [ISO7498] és la norma matriu de les arquitectures telemàtiques jerarquitzades en nivells. La formulació de seguretat d'aquesta norma ve especificada a [ISO7498-2]. D'acord amb aquestes normes hem de considerar tres aspectes importants en la seguretat de xarxes:

- Atac de Seguretat: qualsevol acció que compromet la seguretat de la informació propietat d'una organització.
- Mecanisme de Seguretat: mecanisme emprat per detectar, prevenir o recuperar-se d'un atac de seguretat.

- Servei de Seguretat: protegeix les comunicacions dels usuaris davant de determinats atacs. Per proporcionar el servei s'utilitzen un o més mecanismes de seguretat.

Ara podem introduir el concepte de *Protocol de Seguretat* que consisteix en un conjunt de regles i formats que determinen l'intercanvi de peces d'informació, en el que intervenen dues o més entitats (de nivell N) i que està dissenyat per donar determinats serveis de seguretat a entitats d'un nivell superior (de nivell N+1). Generalment els mecanismes de seguretat utilitzats per donar aquest serveis estan basats en tècniques criptogràfiques. Tot i que la seguretat de xarxes va més enllà de la criptografia, és indubtable la importància d'aquesta en la provisió de serveis de seguretat. Podem trobar bones explicacions de les principals tècniques criptogràfiques a [MOV97, S02, S95, S96, RH91].

La provisió d'alguns serveis de seguretat requereix el concurs de Terceres Parts de Confiança, TTP (*Trusted Third Party*). Les TTPs són agents telemàtics especialitzats que intervenen en els intercanvis d'informació per donar serveis de seguretat. Per establir comunicacions segures, en alguns casos, és convenient i fins i tot necessari el concurs d'una o vàries TTPs que proporcionen els serveis de seguretat que demanen les entitats involucrades en la comunicació.

Les TTPs representen, doncs, un paper molt importat per a la seguretat en els procediments telemàtics i poden fer funcions similars com les que duen a terme les terceres parts en els procediments tradicionals, això és, notaris, agents de correu, etc. Així el model de comunicació general de seguretat que tendrem serà el representat a la figura 2.1.

En aquest capítol volem revisar les característiques principals de la involucració de les TTPs en els protocols de seguretat. Per això veurem els punts essencials de les normes i recomanacions sobre TTPs que han fet els organismes internacionals reguladors. En concret, d'una banda, descriurem com pot ser la intervenció de les TTPs en els protocols de seguretat, com és la interacció entre usuaris i TTPs i quins són els principals serveis que proporcionen les TTPs. D'altra banda, volem revisar el concepte de confiança i quins són els problemes que pot tenir un usuari quan confia la seguretat del protocol a l'actuació d'una TTP. També revisarem quins tipus de solucions han estat proposades en els articles científics per minimitzar els problemes derivats del dipòsit de confiança dels usuaris en les TTPs.

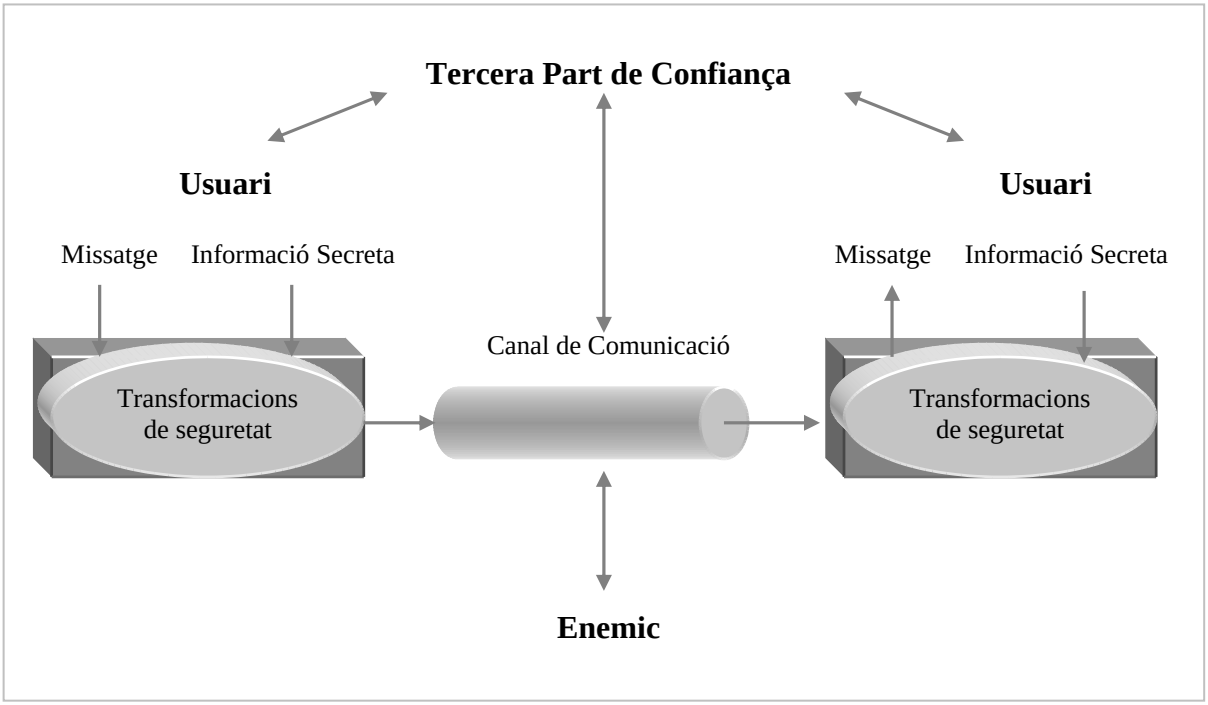

Figura 2.1. Model general de comunicació

2.2 Terceres Parts de Confiança en els protocols de seguretat

Podem entendre que per la situació remota dels actors, un intercanvi d'informació entre dues entitats a través d'una xarxa telemàtica comporta un element de confiança; és a dir, per exemple, el receptor podria haver d'assumir que la identitat de l'emissor dels missatges que rep provenen realment d'aquest emissor i, a canvi, l'emissor també hauria d'assumir que el receptor que rep els missatges té realment la identitat del receptor pel qual la informació fou emesa. El fet d'involucrar d'elements de confiança en tota comunicació telemàtica podria no ser suficient, sempre en funció dels requeriments de seguretat que tengui la comunicació, i podria ser necessari o convenient l'ús de TTPs que facilitin un intercanvi segur d'informació.

El paper que representen les TTPs inclou la provisió de seguretat en qualsevol tipus de transaccions i altres intercanvis d'informació formals, i donen seguretat sobre certs aspectes com són ara la identitat de les parts involucrades en la comunicació, la recepció dels missatges en un determinat moment i forma i, per qualsevol disputa que pugui sorgir sobre l'intercanvi, l'ús de mètodes apropiats per a la creació i lliurament de les evidències requerides que permetran demostrar el que ha passat durant la transacció. Els serveis

proporcionats per les TTPs poden incloure tots aquells serveis necessaris per a l'administració de claus, l'administració de certificats, suport en la identificació i l'autenticació, serveis d'atributs de privilegis, de no rebuig, serveis de segellat en el temps, serveis de notaria pública electrònica i servei de directori. Una TTP pot proporcionar alguns o tots aquests serveis.

Una TTP ha de ser dissenyada, implementada i administrada per proporcionar garanties dels serveis de seguretat que proporciona i satisfer els requeriments legals i reguladors. El tipus i nivells de protecció adoptats o requerits variaran en funció del servei concret proporcionat per la TTP i del context dins del qual es realitza l'intercanvi d'informació.

Associats amb la provisió i amb l'operació d'una TTP existeixen un cert nombre de temes relatius a la seguretat sobre els quals és necessària una orientació general que doni ajuda a les entitats involucrades en una comunicació, els programadors, els proveïdors de sistemes i serveis, etc. Això inclou orientacions sobre temes que tenen relació amb els rols, posicions i relacions de les TTPs i les entitats que utilitzen els seus serveis, els requeriments de seguretat genèrics, qui hauria de ser el proveïdor de cada tipus de servei, quines possibles solucions de seguretat hi ha, i l'ús operatiu i administració de la seguretat del servei de la TTP. Per tot això, els organismes internacionals han publicat una sèrie de recomanacions i informes tècnics [X.509, X.800, X.810, X.813]. En especial s'ha de destacar el document ITU-T *Recommendation* X.842 (2000), *Information technology – Security techniques – Guideliness for the use and management of Trusted Third Party services* [X.842]. Aquest document proporciona una orientació per a l'ús i l'administració de TTPs, una definició de les obligacions bàsiques i els serveis proporcionats, la seva descripció i el seu propòsit, i els papers i les responsabilitats de les TTPs i de les entitats que utilitzen els seus serveis.

També s'indica que una TTP hauria d'utilitzar les recomanacions generals per a la protecció dels seus serveis. Les recomanacions generals per a l'administració de la seguretat en les tecnologies de la informació es poden trobar a ISO/IEC 13335 [ISO13335-1, ISO13335-3, ISO13335-4, ISO13335-5]. Llavors, el compromís d'una TTP per proporcionar serveis de seguretat hauria d'estar descrit en un document formal sobre la seva política de seguretat. Podem trobar un exemple d'aquest tipus de document formal sobre la política de seguretat que tracta sobre els certificats de clau pública al RFC 2527, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* [RFC2527].

2.2.1 Intervenció de les TTPs en els protocols de seguretat

Una TTP és una organització que proporciona un o més serveis de seguretat, i és de confiança per altres entitats respecte a les activitats relacionades amb aquests serveis de

seguretat. Una TTP és utilitzada en els protocols de seguretat per oferir un valor afegit en els serveis que reben les entitats connectades a una xarxa telemàtica per tal de facilitar que les comunicacions siguin segures. Aquestes entitats han de poder escollir quina és la TTP que utilitzaran per proveir-se dels serveis requerits, en funció de les característiques d'aquesta TTP.

Tal com s'identifica a [X.842], des d'un punt de vista de comunicacions, les TTPs i les entitats involucrades en un protocol de seguretat poden tenir diferents configuracions: *in-line*, *on-line* i *off-line*. La configuració adoptada influirà lògicament en la prestació del servei, en el cost del mateix i en la càrrega de comunicacions del protocol. Tot seguit, veurem un exemple de cada configuració on suposarem un escenari de comunicació en el qual una *Entitat A* envia dades o missatges a una *Entitat B*. En aquest escenari hi ha present una TTP que coopera amb aquestes dues entitats amb l'objectiu de facilitar la provisió d'un servei de seguretat:

- **Serveis de TTP *in-line***: En un intercanvi d'informació la TTP proporcionarà un servei de forma *in-line* si és present en totes les transferències d'informació que es produeixen, encara que no sigui sol·licitat el seu servei per part d'alguna de les entitats involucrades en la comunicació. La TTP està interposada en el camí de l'intercanvi de dades entre originador i receptor dels missatges. Una TTP *in-line* és necessària quan dues o més entitats pertanyen a dominis de seguretat diferents i no utilitzen el mateixos mecanismes de seguretat. En aquest cas, les entitats no són capaces dur a terme directament un intercanvi segur. L'esquema de funcionament seria com el de la figura 2.2.

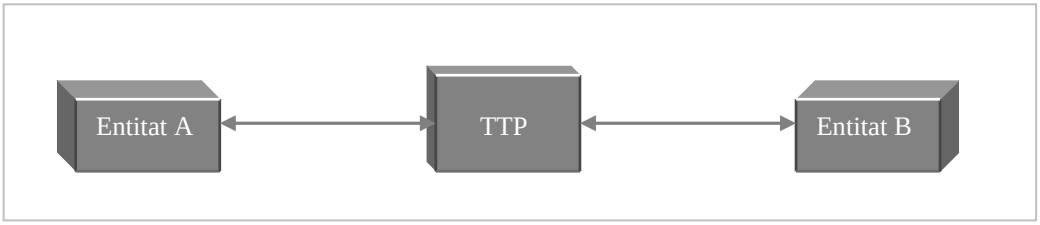

Figura 2.2. TTP *in-line*

Amb aquesta configuració la TTP pot proporcionar serveis de no rebuig, control d'accés, recuperació de claus, confidencialitat i integritat de les dades transmeses.

- **Serveis de TTP *on-line***: La TTP pot estar activament involucrada en cada execució del protocol de seguretat, però no està en el camí entre originador i receptor; és a dir, l'*Entitat A* pot enviar les dades directament a l'*Entitat B* i viceversa. La TTP només hi

intervendrà a petició d'una de les entitats o podrà monitoritzar totes les transaccions com il·lustra la figura 2.3.

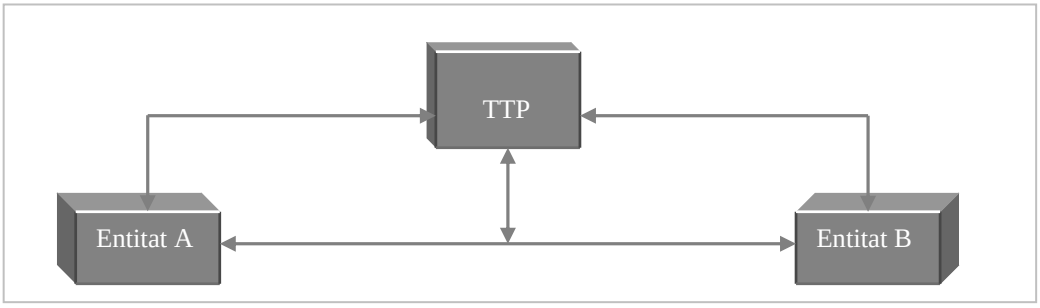

Figura 2.3. TTP *on-line*

Amb aquesta configuració la TTP pot proveir serveis de no rebuig, control d'accés, administració de claus, lliurament de missatges, segellat temporal, confidencialitat i integritat de les dades transmeses.

- **Serveis de TTP *off-line***: La TTP està totalment al marge de la comunicació activa entre les entitats comunicants. És a dir, la TTP no opera interactivament en el protocol. Però les dades generades prèviament per la TTP són utilitzades per les entitats en l'intercanvi segur que mantenen, tal com ho indica la figura 2.4 en línies discontinues.

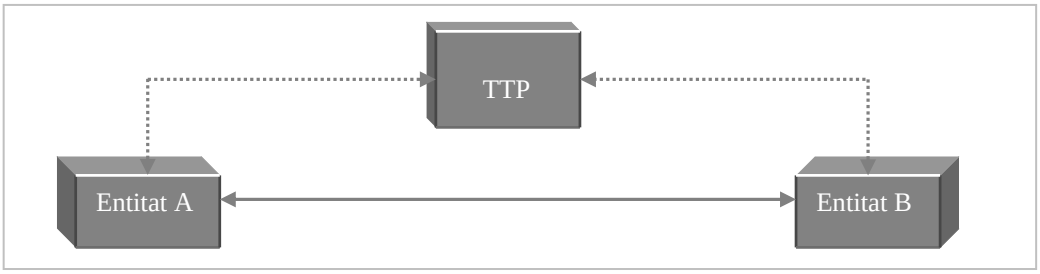

Figura 2.4. TTP *off-line*

Amb aquesta configuració la TTP pot proveir serveis de no rebuig, distribució i recuperació de claus.

2.2.1.1 Interacció entre TTPs i usuaris

Perquè hi hagi una bona cooperació entre TTPs i entitats involucrades en una comunicació és necessari que estiguin clarament definides les interfícies, protocols i formats de les dades. Cada TTP proporciona serveis a les entitats dins del seu domini i d'acord amb la seva política de seguretat. També una TTP pot tenir convenis amb altres TTPs que permetin a una entitat client d'una determinada TTP una comunicació segura amb entitats clients d'altres TTPs. Podem trobar estructures de cooperació entre TTPs a la recomanació X.509 de l'ITU-T [X.509].

Els tipus d'interacció més detectats a [X.842] són:

- **TTP-Usuaris**: El mitjà pel qual un usuari interacciona amb una TTP per sol·licitar o rebre un servei és conegut com a interfície d'usuari. Cada usuari pot interactuar amb la TTP de diferent manera depenent de com sigui ofert el servei.
- **Usuari-Usuari**: Després que la TTP hagi completat la seva feina, la resta de comunicació entre entitats es pot fer sense l'assistència d'aquesta. La relació entre aquestes entitats recau en gran manera en la confiança que cada una de les entitats tengui amb les TTPs.
- **TTP-TTP**: Aquesta interfície suporta comunicacions segures entre usuaris gràcies a l'intercanvi d'informació fet amb els serveis de seguretat proporcionats.

En el següent exemple il·lustram l'ús de distintes interfícies entre usuaris i TTPs quan sol·liciten tenir una comunicació segura. Així un primer escenari s'esdevindria quan una *Entitat A* fa una petició a la *TTP A* demanant una clau secreta per comunicar-se amb l'*Entitat B* (1), la *TTP A* transfereix la clau secreta a l'*Entitat A* (3) i a la *TTP B* (2); llavors, aquesta passa la clau a l'*Entitat B* (3). Amb aquesta clau, les entitats *A* i *B* poden tenir una comunicació segura (4). Una altra alternativa seria la utilització de tecnologia de clau pública. En aquest cas, l'*Entitat A* demana a la *TTP A* tenir una comunicació segura amb l'*Entitat B* (1). La *TTP A* passa el certificat de l'*Entitat A* a la *TTP B* al mateix temps que li demana un certificat de l'*Entitat B* (2). Llavors, la *TTP B* passa a l'Entitat B el certificat de l'*Entitat A* (3) i transfereix a la *TTP A* el certificat de l'*Entitat B* (2), que l'envia a l'*Entitat A* (3). Amb el certificat de l'*Entitat B* en possessió de l'*Entitat A*, i viceversa, es pot establir una comunicació segura entre ambdues entitats (4). A la figura 2.5 podem veure aquesta interacció de TTPs i usuaris de diferents dominis.

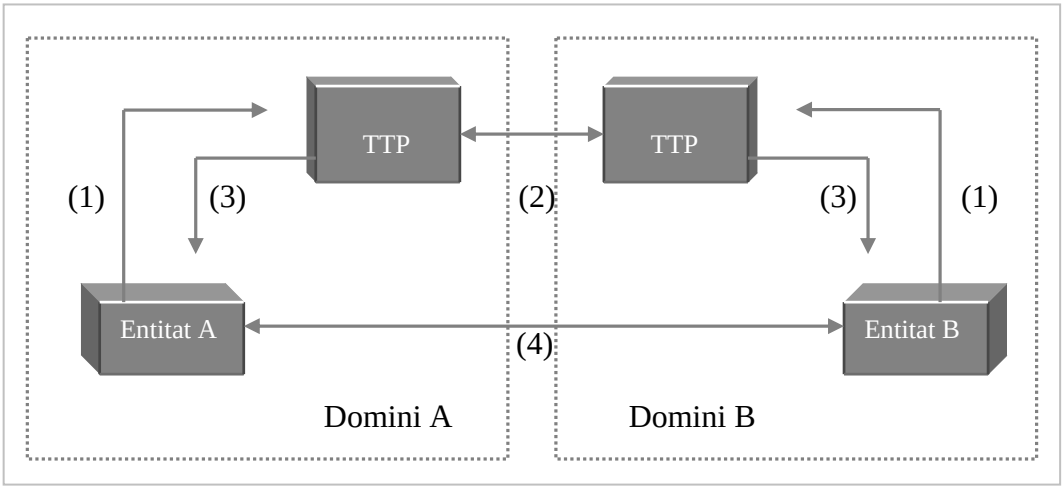

Figura 2.5. Interacció entre TTPs i usuaris

2.2.1.2 Principals categories de serveis de TTPs

Tant en la recomanació [X.842] com en el document [ETSI97], hi podem trobar identificades les principals categories de serveis de TTPs. Així podem veure quins són els tipus de protocols de seguretat on podem trobar involucrades TTPs. Les principals categories de serveis són:

- Serveis de segellat temporal: segella criptogràficament un document digital enllaçant-lo amb un temps de confiança. Els *time-stamps* estan descrits a [ISO13888-1].
- Serveis de no rebuig: Les terceres parts representen un paper molt important en la provisió dels serveis de no rebuig. [X.810] descriu les aplicacions dels serveis de no rebuig en els sistemes oberts i identifica els mecanismes que involucren les TTPs. En general els serveis de no rebuig inclouen la generació, la verificació i l'emmagatzematge d'evidències, i la subsegüent recuperació i reverificació d'aquestes per tal de resoldre disputes. Les TTPs es poden veure involucrades en totes aquestes tasques tal com descriu ISO/IEC 13888 [ISO13888-1]. En aquest entorn s'utilitza el terme 'evidència' per designar un instrument tècnic que proporciona prova.
- Serveis d'administració de claus: Les TTPs donen suport a l'administració tant de claus secretes de criptosistemes simètrics com de parells de claus públiques/privades de criptosistemes asimètrics. Una TTP pot oferir per separat els serveis de generació i de distribució de claus.

- Serveis d'administració de certificats: El format del certificat de clau pública està definit a la recomanació X.509 [X.509]. Les Autoritats de Certificació són TTPs que proporcionen certificats de clau pública i tenen cura de la informació necessària per revocar els certificats emesos.
- Serveis de Notari Electrònic Públic: són serveis d'alt nivell que fan ús dels serveis més bàsics com són els serveis de segellat temporal, certificació, serveis de directori, serveis d'arxiu i no rebuig. En principi, una TTP rep un document i aquesta dóna fe de la recepció o certifica el document.
- Servei d'arxiu electrònic: És un servei que permet guardar documents electrònics d'una forma segura.
- Servei de directori: En molts casos, els serveis de seguretat es basen en informacions com els certificats de clau pública, les llistes de certificats revocats o dels certificats d'atributs. Tots aquests elements poden ser proporcionats per un directori. Un exemple de servei de directori i els seus corresponents protocols d'accés es troba a la sèrie de recomanacions X.500 de l'ITU-T [X.500].
- Servei de control d'accés: Una TTP es pot utilitzar per atorgar privilegis per al control d'accés. A més, una TTP pot ser responsable del control d'accés a la informació. Aquestes funcions estan més especificades a ISO/IEC 11770-1 [ISO11770-1].
- Servei de dipòsit i recuperació o captura de claus (*Key Escrow/Recovery* [D95]): Aquest servei fa referència a la salvaguarda de claus que permetin desxifrar dades. Les àrees típiques d'aplicació són la intercepció legal o accés legal a dades i també l'accés comercial a dades. La diferència entre aquestes àrees d'aplicació són les que determinaran les condicions sota les quals tendrà lloc el desxifratge o xifratge de dades.

2.3 Confiança en les TTPs

L'ús d'una TTP i dels seus serveis depèn fonamentalment que els serveis que proporciona la TTP siguin de confiança per a altres TTPs i entitats. Aquesta confiança parteix de la suposició que la TTP és administrada correctament i els seus serveis operen de forma segura. Per tant, s'hauria d'assegurar que la TTP mateixa i els serveis que proporciona funcionen d'acord amb les especificacions dels protocols i de les polítiques de seguretat establertes. La confiança es pot establir a través d'evidències que mostrin com s'administra i opera la TTP. Aquestes evidències haurien de mostrar que tant els aspectes administratius com els operatius són els adequats per complir els objectius d'una forma efectiva, que minimitzi els riscos i que contraresti les amenaces. Aquestes observacions s'han fet a la recomanació [X.842], però podem trobar comentaris en el mateix sentit a altres documents com [ETS97, ETSI97, IPI, OP98, OII98]. De fet, en aquesta tesi cercam com podem proporcionar aquest tipus d'evidència a nivell d'operació de la TTP dins

l'entorn d'un protocol de seguretat. Això facilitarà que els usuaris utilitzin els nous procediments electrònics i els serveis que les TTPs hi proporcionen, malgrat l'exigència inicial d'haver de dipositar un cert grau de confiança en aquestes entitats. Pretenem, per tant, que els usuaris guanyin confiança en l'ús de les TTPs i que aquest guany provengui de les propietats inherents al disseny del protocols; és a dir, que el disseny dels protocols tengui, entre les seves característiques la propietat de minimitzar el risc que comporta confiar la seguretat de l'intercanvi en una tercera part.

Abans d'abordar d'una forma directa aquest objectiu, volem fer una revisió dels aspectes més teòrics que podem trobar en els darrers treballs fets sobre *confiança* dins l'entorn de les tecnologies de la informació. A les definicions del terme confiança, que hem vist a la introducció d'aquesta tesi, volem afegir-ne algunes de noves en aquesta secció; amb això volem deixar ben clar què comporta a un usuari tenir confiança en algú altre i els riscos inherents. Aquestes definicions són objecte d'estudi per part d'experts de disciplines diverses tant tecnològiques com del camp del dret, les ciències socials i la filosofia, com el grup de treball interdisciplinar *iTrust* de l'*Information Society Technologies* que estudia l'ús de la confiança en les tecnologies de la informació.

2.3.1 Concepte de Confiança

Tal com diuen M. Kinateder i K. Rothermel a [KR03], podem explicar de manera informal la confiança en una entitat com "la creença que sota certes circumstàncies aquesta entitat actuarà d'una determinada manera". Dit més formalment, el Diccionari General de la Llengua Catalana de l'Institut d'Estudis Catalans [IEC] defineix confiança com "la seguretat de qui compta amb el caràcter, la capacitat, la bona fe, la discreció d'algú".

Una altra definició de confiança comunament donada, la trobam al document de D. Gambetta [G00] on es defineix el terme com "un nivell particular de la probabilitat subjectiva amb el qual un agent avalua que un altre agent o grup d'agents realitzarà una acció en particular". L. Mui et al. a l'article [MMH02] s'adapten a aquesta definició per emfatitzar la importància de l'expectativa en lloc de treballar amb probabilitat: "Confiança: una expectativa subjectiva d'un agent sobre la futura conducta d'un altre basada en la història d'anteriors interaccions".

Com queda clar en qualsevol cas, la reputació guanyada per una entitat que mereix la confiança d'altres a base d'experiències anteriors o formalitzada en documents, tal com és la descripció de la política de seguretat, no dóna garantia que aquesta confiança no sigui trencada en un futur i que els greuges que se'n derivin puguin ser compensats o corregits. Com ja explica P. Cofta i S. Crane a [CC03] si una *Entitat A* pot predir perfectament cada acció de l'*Entitat B*, llavors *A* no necessita confiar més en *B*. *A* posseeix coneixement

complet de *B* (la confiança és reemplaçada pel coneixement). Dins els diferents procediments electrònics es fa necessari el dipòsit de confiança en terceres parts, cosa que ve dificultada per l'absència del contacte cara a cara, que és una característica més pròpia de les transaccions en el món "convencional". Així doncs, després d'haver vist allò que representa el concepte de confiança ens refermam en el nostre pensament sobre la importància de la inclusió de noves característiques en els protocols de seguretat que alleugin la quantitat de confiança que un usuari ha de dipositar en una tercera part, sobretot tenint en compte que no podem tenir certesa sobre les accions que farà aquesta tercera part.

2.4 Bases de la confiança en les TTPs: el problema associat a l'ús de TTPs

Com acabam de veure en l'apartat anterior, confiar en una entitat connectada a la xarxa i que diu ser una TTP no està exempt de riscos. Sempre estarà exposat l'usuari a una possible equivocació en l'operació de la TTP, com, per exemple, la generació i emissió d'una evidència per part de la TTP pugui contenir errades. A més, com ja indiquen R.H. Deng et al. a [DGL96] les principals categories de serveis que hem vist abans a l'apartat 2.2.1.2 poden ser proporcionades per un ampli rang d'organitzacions. Llavors, si els nous procediments electrònics creixen i se n'estén l'ús, el nombre de TTPs s'incrementa i l'entorn de seguretat sobrepassa el límits de les organitzacions, per la qual cosa podrà ser difícil per als usuaris assegurar un nivell de confiança adient en les TTPs.

Sembla clar, doncs, que s'han de cercar sistemes que ajudin els usuaris a tenir confiança en les TTPs si volem que s'estengui l'ús d'aquests procediments electrònics. L'ús de TTPs i els seus serveis depèn bàsicament que els serveis proporcionats per una TTP siguin percebuts com a serveis de confiança per les altres TTPs i entitats. Aquesta confiança resulta de la creença que la TTP és administrada correctament i que la TTP opera els serveis d'una forma segura. La confiança es pot establir donant evidència sobre els aspectes d'administració i operació de la TTP. Les evidències haurien de mostrar que els aspectes d'administració són adequats i suficients per aconseguir completament els objectius, que l'administració del sistema és efectiva, convenient per minimitzar el risc i per contrarestar les amenaces. Per això, la recomanació [X.842] i altres informes com [ETSI97, OP98] especifiquen que, per guanyar confiança en aspectes operatius i d'administració de la TTP, s'hauria de proporcionar evidència que:

a) hi ha una apropiada política de seguretat;
b) els problemes de seguretat s'han encarat per mitjà de la combinació de procediments i mecanismes de seguretat implementats correctament;

c) les operacions es duen a terme correctament i guardant una definició clara del conjunt de rols i responsabilitats;
d) les interfícies i procediments de comunicació amb les entitats són apropiats per a les funcions que han de fer i s'utilitzen correctament;
e) el personal segueix les regles i regulacions que són congruents amb un cert nivell de confiança;
f) la qualitat dels processos, operacions i pràctiques de treball han estat convenientment acreditats;
g) la TTP compleix les seves obligacions contractuals amb els seus usuaris;
h) hi ha una clara comprensió i acceptació de les responsabilitats;
i) es manté i es pot fer una auditoria sobre el compliment de les lleis i les distintes regulacions;
j) les amenaces conegudes i les seves possibles solucions es poden identificar clarament;
k) s'ha de fer una anàlisi de riscos i amenaces inicial que s'ha d'actualitzar periòdicament per assegurar que es compleixen els requeriments de confidencialitat, integritat, disponibilitat i fiabilitat;
l) es compleixen les mesures adequades dins de l'organització i el personal;
m) la confiança de la TTP pot ser comprovada i verificada;
n) la TTP és monitoritzada per algun tipus d'autoritat administrativa que vetlli que la seva operació està dins les normes per a les quals ha estat acreditada.

La implementació d'aquests mecanismes encaminats a resoldre el problema associat a l'ús de TTPs en protocols de seguretat té distints enfocaments. D'una banda, és necessari acudir a mecanismes que provenen del món basat en paper, com són els endossos (*endorsements*), autoritzacions (*licensing*), assegurances (*insurance*) i vincles de seguretat (*surety bounds*) per tal de compensar l'esmentada falta de confiança. D'altra banda, aquestes recomanacions haurien de tenir algun reflex en les especificacions dels protocols de seguretat on apareixen TTPs. Ara bé, no és freqüent que les publicacions científiques abordin aquest tema. Quan aquest tema és encarat, algunes vegades es remet a l'apartat *n)* de les anteriors recomanacions com a únic argument perquè l'usuari tengui confiança en la TTP, com N. Asokan et al. a [ASW98]; en altres casos on el problema de la confiança en la TTP és tractat amb més profunditat, les solucions proposades cauen dins dos grans tipus d'enfocaments atenent al fet d'utilitzar terceres parts o no:

- **Protocols sense TTP**. Aquests protocols són anomenats també autocontinguts (*self-enforcing*) i en teoria garanteixen les característiques de seguretat sense la necessitat d'un àrbitre o TTP. Aquest seria el millor tipus de protocol possible, segons afirma B. Schneier a [S96]. Desafortunadament els protocols autocontinguts no tenen una solució pràctica per a cada situació i, per tant, en

molts de casos es fa necessari l'ús de TTPs si volem que la seguretat del procediment quedi garantida.

- **Protocols amb múltiples TTPs**. Aquests protocols pretenen solucionar el problema d'una possible TTP corrupta mitjançant la introducció de múltiples TTPs de tal manera que una minoria de TTPs corruptes no malmeti la seguretat de l'intercanvi, com en els protocols presentats a [FR95, MFH00]. D'aquesta manera es divideix la confiança en un grup de TTPs i així es pot abaixar el nivell de confiança que s'ha de dipositar en una TTP sense comprometre la confiança global en el sistema de TTPs i la seguretat de l'intercanvi, tal i com afirma G. Ateniese et al. a [AMG01]. Malauradament aquestes solucions solen tenir un cost computacional i de comunicacions elevat. Aquesta circumstància fa que difícilment aquests protocols siguin pràctics.

2.4.1 Protocols sense TTP

Les solucions a alguns tipus de problemes inclouen normalment i naturalment l'ús de TTPs. Succeeix així, per exemple, en el cas dels protocols de no rebuig que han estat estudiats a l'ISO/IEC 13888 [ISO13888-1, ISO13888-2, ISO13888-3] on s'hi proposen tres models anomenats M1, M2 i M3. El retret que es fa a aquestes solucions des del punt de vista de la inclusió de TTPs és la consideració d'aquesta entitat com a punt crític, tant des del punt de vista de comunicacions (la TTP es pot convertir en un coll d'ampolla) com de seguretat (una TTP corrupta malmetrà la seguretat del protocol). Per donar solucions a problemes com aquests o al fet que no es pugui trobar una TTP de confiança mútua entre remitent i destinatari es presenten solucions de protocols de seguretat sense TTPs.

Si ens fixam en les solucions proposades per a protocols d'intercanvi equitatiu de valors veurem que són un cas típic d'inclusió de TTPs dins de protocols de seguretat. No obstant això, s'ha intentat resoldre el problema sense la inclusió de terceres parts. Per això, el concepte d'equitat s'enfoca des d'un punt de vista computacional. En aquestes solucions s'utilitza l'anomenat intercanvi gradual d'informació. Això significa que, a cada pas del protocol, es va incrementant la probabilitat que l'intercanvi equitatiu sigui vàlid i aquesta probabilitat tendeix a 1 després de molts d'intercanvis. Si alguna de les parts s'atura abans d'acabar el protocol, totes dues parts hauran de tenir una potència de càlcul similar si volem conservar l'equitat de l'intercanvi. Les principals debilitats d'aquests protocols són aquestes: suposar que les parts han de tenir igual poder computacional perquè es mantengui la seguretat del protocol, l'efecte desconcertant que té l'aturada unilateral prematura de l'intercanvi i la dificultat de provar la correcció de l'intercanvi com detallen M. Ben-Or et al. a [BGM90]. Una altra crítica que es fa a aquests protocols és la ineficiència a causa de la gran quantitat de missatges que s'han d'intercanviar les parts. Podem veure aquests desavantatges (figura 2.6) en aquest senzill protocol de no rebuig amb intercanvi gradual de secrets explicat per J. Zhou a [Z03].

1. A tria un secret K_a de n bits
2. $A \rightarrow B$: eK_a(M), H(M), EOO
3. B tria un secret K_b de n bits
4. $B \rightarrow A$: H(K_b), EOR
5. A i B s'intercanvien K_a i K_b bit a bit

Figura 2.6. Protocol de no rebuig amb intercanvi gradual de secrets

En aquest protocol, eK_a(M) significa el xifratge amb un criptosistema simètric del missatge M emprant la clau K_a. H(M) és el resultat d'aplicar una funció de *hash* al missatge M. EOO és un *token* de no rebuig d'origen i EOR de no rebuig de recepció. En el pas 5 A i B començarien una tanda d'intercanvis bit a bit fins que cada una completàs el secret de l'altra. És prou evident que aquest protocol no és eficient si el comparam amb solucions eficients que inclouen l'ús d'una TTP com [ASW97, ASW98, ZG97, FPH00, KMZ02]. A més, si una part té més potència de càlcul que l'altra, pot aturar l'intercanvi i completar el secret de l'altra part, mentre que aquesta darrera no tendrà potència de càlcul suficient per completar-lo en un temps raonable, rompent així la seguretat de l'intercanvi. Com a exemple, podem dir que, si la part A pot executar 100.000 operacions per segon, mentre que B pot executar-ne 1.000.000.000 el protocol que acabam de presentar no seria acceptable, perquè si l'intercanvi s'interromp quan s'executa el pas 5 del protocol i cada part necessita 10^{12} operacions per obtenir el secret de l'altra, llavors A necessitarà 4 mesos per obtenir el secret, mentre que B només necessitarà 17 minuts. Queda clar, doncs, que aquest tipus de solucions només tendran sentit si les parts tenen la mateixa potència de càlcul; però aquesta suposició és poc realista a la pràctica i indesitjable des d'un punt de vista teòric. En un cas real no podem suposar que, per exemple, una gran firma comercial tengui la mateixa potència de càlcul que un particular. També hi ha la dificultat que comporta per a una part fer una estimació de la potència de càlcul de l'altra.

Hem de remarcar, també, l'efecte desconcertant de que té l'aturada unilateral prematura de l'intercanvi, que es concreta en la manca d'instruccions que hi ha en aquestes propostes per a una entitat si es troba en una situació on l'altra part interromp l'execució del protocol. Aquesta manca d'alternatives és probable que sigui causada per la dificultat de trobar opcions raonables. Podem veure-ho mitjançant l'exemple anterior: si suposam que, en funció de l'èxit de l'intercanvi, es poden prendre determinades decisions en un termini curt de temps, llavors la part A es trobarà en una en una posició difícil, ja que la seva potència de càlcul no li permet completar el secret de l'altra part en aquest termini curt de temps. Exemples d'aquest tipus de protocols són [B83, G84, EGL85, D93, AT94, TEDIS94, EGL95, MR99]. A causa dels desavantatges que acabam d'exposar, els treballs més recents es concentren a trobar solucions que inclouen l'ús de TTPs.

Hem de fer esment a un altre enfocament que permetria la definició de protocols de seguretat sense TTP. Y. Han a [H96] proposa un protocol sense TTP però que utilitza un hardware segur, públic i específic (anomenat *the pub*). El hardware *the pub* guarda, com un notari, cada operació de les parts implicades quan les parts implicades en l'intercanvi es transmeten per exemple la clau de desxifratge (com al protocol de l'exemple anterior). Aquestes solucions substitueixen la confiança en una TTP per la confiança en un dispositiu hardware, però tal com critiquen O. Markowitch et al. a [MR99], per tenir seguretat en aquests dispositius, es necessita una gran confiança i el risc que comporta això no pot ser parametritzat.

2.4.2 Protocols amb múltiples TTPs

Els protocols que involucren moltes TTPs se centren més a resoldre el problema que presenten els protocols sense TTP sobre la reducció de la quantitat de confiança que els usuaris han de dipositar en una TTP que a resoldre la sobrecàrrega en les comunicacions. L'enfocament adoptat per aquests protocols és el de dividir la confiança que els usuaris dipositen en una sola TTP, en el cas dels protocols sense TTP de l'anterior apartat, entre un conjunt de TTPs involucrades en aquest nou tipus de protocols, de tal manera que una minoria de TTPs corruptes no poden comprometre l'equitat de l'intercanvi de valors. Aquí, se suposa que corrompre un grup de TTPs és molt més complicat que corrompre una única TTP.

El mecanisme emprat pels protocols amb múltiples TTPs, com els proposats a [G93, FR95, S96], sol consistir a fer una rèplica de la TTP, de manera que el servei de confiança proporcionat queda distribuït entre les diferents TTPs amb les mateixes característiques i que cooperen en un mateix nivell.

La comunicació entre els usuaris del protocol i les TTPs es fa a través d'un sistema de compartició de secrets. El sistema de compartició de secrets fa que un usuari pugui dividir un missatge en trossos i enviar un tros diferent a cada TTP, de manera que una minoria de TTPs no poden reconstruir el missatge, sinó que per reconstruir el missatge és necessari el consens de la majoria de les TTPs involucrades en el protocol. D'aquesta manera, es pot dir que el protocol definit és resistent a una minoria de TTPs corruptes i, per tant, el protocol garanteix els requeriments de seguretat fins i tot en casos de manipulacions malintencionades.

Els sistemes criptogràfics de compartició de secrets emprats en molts d'aquests protocols són els anomenats esquemes llindar, definits inicialment a [S79, B79]. Les crítiques [S96, ASW97] més habituals a protocols amb múltiples TTPs que utilitzen esquemes llindar sorgeixen a causa de la complexitat que implica l'ús d'aquest tipus de criptografia. Els

esquemes llindar són uns esquemes criptogràfics que comporten als seus usuaris una gran despesa a nivell computacional i normalment també fan augmentar la despesa en comunicacions.

2.4.3 TTP corrupta

Les solucions que acabam de veure en els apartats anteriors van encaminades a minimitzar el risc que corren els usuaris en confiar part de la seguretat del protocol en una tercera part. En aquesta secció veurem amb l'ajuda d'un exemple quines conseqüències podria tenir l'actuació deshonesta d'una TTP en un protocol de seguretat. Per això hem escollit el protocol de signatura de contractes proposat per J.A. Garay et al. a [GJM99]. Aquest protocol, d'una forma prou clara, ens mostrarà com l'actuació esbiaixada de la TTP afavoreix una part sense que l'altra part pugui demostrar que la TTP no ha actuat correctament. En conseqüència, la TTP podrà rompre la seguretat de l'intercanvi sense que ningú ho pugui demostrar.

El protocol proposat a [GJM99] que volem analitzar (l'anomenarem protocol GJM per les inicials del seus autors) permet a dos usuaris, anomenats *O* i *R*, intercanviar signatures sobre un text contractual. Se suposa que abans de l'execució del protocol, les parts estan d'acord amb aquest text i amb la identitat de la tercera part *T* que intervendrà en el protocol en cas de problemes amb l'objectiu de garantir l'equitat de l'intercanvi. Cada participant coneix la clau per poder verificar la signatura de l'altra part i de *T*. Utilitzarem la mateixa nomenclatura que els autors per designar el resultat de signar el text *m* amb la clau de la part *i*: $\text{S-Sig}_i(m)$. És important indicar que els participants en el protocol han de tenir un canal privat de comunicació amb *T*; és a dir, un canal de comunicació inaccessible per a qualsevol intrús.

El protocol és asíncron (sense dependències temporals) i, a mesura que les parts es van intercanviant elements d'informació, aquests interlocutors poden interrompre l'intercanvi entre ells i posar-se en contacte amb la tercera part. Llavors *T* ha de decidir, en funció de les dades rebudes, com resoldre el protocol. Això significa que la TTP o bé lliurarà a una part la signatura sobre el contracte de l'altra part o bé emetrà un *token* d'avortament de l'intercanvi. Aquests missatges d'avortament no són una prova que l'intercanvi s'hagi cancel·lat, sinó que un usuari s'ha posat en contacte amb *T* i aquesta ha actuat d'acord amb les dades rebudes (és important observar que aquesta interacció entre usuari i TTP s'ha pogut fer sense tenir en compte el resultat final de l'intercanvi entre els usuaris). Se suposa que el canal de comunicació és *resilient* o elàstic; és a dir, el canal lliurarà correctament les dades entre els dos extrems de la comunicació amb un retard finit però desconegut. Abans de veure com és aquest protocol per després veure les conseqüències que pot tenir la mala actuació de la TTP, descriurem les principals característiques d'una

primitiva criptogràfica emprada en el protocol perquè aquest sigui *abuse-free*[1]. Aquesta primitiva criptogràfica s'anomena *private contract signature* (PCS).

2.4.3.1 *Private Contract Signatures*

Les signatures PCS estan dissenyades perquè només les pugui verificar una determinada entitat, però es poden convertir en signatures universalment verificables. Aquest esquema ve detallat a [GJM99] i és similar a les *designated-confirmer signatures* i *convertible undenial signatures* suggerides per D. Chaum a [C94]. A l'article original [GJM99] es demostra que l'esquema és segur.

Denotarem la signatura de contracte privada de la part *O* sobre el text *m* per a la part *R* i en relació amb la tercera part *T* com a $PCS_O(m, R, T)$. *R* és conegut com a verificador designat. Les principals propietats de PCS són les següents:

- La complexitat de la verificació de $PCS_O(m, R, T)$ és com la d'una signatura convencional.
- *O* o *R* poden calcular $s = PCS_O(m, R, T)$, però ningú més. Aquesta és la propietat clau que distingeix les signatures PCS d'un esquema convencional de signatura (universalment verificable) que només pot ser calculada per *O*. Quan el verificador designat *R* rep *s*, sabrà amb tota seguretat que l'ha calculat *O*, però, a diferència d'un esquema convencional de signatura, *R* no pot emprar *s* per provar aquest fet davant d'un tercer.
- Es pot convertir $PCS_O(m, R, T)$ en una signatura convencional. La conversió la poden fer *O* o *T*, però ningú més. Anomenam aquestes conversions $S\text{-}Sig_O(m)$ i $T\text{-}Sig_O(m)$ respectivament. Per al nostre propòsit ens concentrarem en una versió de PCS anomenada *third party-invisible* on $S\text{-}Sig_O(m)$ i $T\text{-}Sig_O(m)$ són idèntiques. Això significa que qualsevol que tengui la clau de verificació pot verificar la signatura però no es pot saber si la conversió ha estat feta per *O* o per *T*.

2.4.3.2 El Protocol

El protocol consta de tres subprotocols interdependents: *exchange*, *abort* i *resolve*. Les parts *O* i *R* comencen l'intercanvi executant el subprotocol *exchange*. Si les dues entitats són honestes i no hi ha interferències en la xarxa, al final del protocol cada una obtendrà un contracte vàlid amb la signatura de l'altra part. L'originador *O* té l'opció de demanar a la tercera part *T* que avorti l'intercanvi que ell ha iniciat. Per això, ha d'executar el

[1] És una propietat que intenta garantir que qualsevol de les parts involucrades en un intercanvi no tengui cap tipus d'avantatge sobre les altres durant l'execució del protocol; això significa que una part no ha de poder bloquejar la transacció i demostrar a un tercer que l'intercanvi pot acabar en un sentit o un altre segons el seu desig [SM02]

subprotocol *abort*. A través del subprotocol *resolve* tant l'entitat *O* com *R* tenen la possibilitat de sol·licitar a *T* que resolgui un intercanvi que no s'ha completat. Poden fer això després de rebre de l'altra part el missatge inicial del subprotocol *exchange*, que representa el compromís de l'entitat emissora d'aquest missatge de dur a terme l'intercanvi de signatures sobre el contracte. D'aquesta manera, al final del protocol es pretén garantir que les dues parts acabaran amb la signatura universalment verificable de l'altra part sobre el contracte o amb un *token* que avorta l'intercanvi i està signat per *T* i *O* i té la forma $\text{S-Sig}_T(\text{S-Sig}_O(m, O, R, abort))$. El subprotocol *exchange* és el de la figura 2.7.

1. $O \rightarrow R$: $me_1 = \text{PCS}_O(m, R, T)$
2. $R \rightarrow O$: $me_2 = \text{PCS}_R(m, O, T)$
3. $O \rightarrow R$: $me_3 = \text{S-Sig}_O(m)$
4. $R \rightarrow O$: $me_4 = \text{S-Sig}_R(m)$

Figura 2.7. Subprotocol *exchange*

Al final de l'intercanvi les dues parts obtenen el contracte signat que té la forma $\{\text{S-Sig}_O(m), \text{S-Sig}_R(m)\}$. Si *O* considera que no ha d'esperar més l'arribada d'un missatge de *R*, llavors pot intentar avortar l'intercanvi amb l'execució del subprotocol *abort* que descrivim a la figura 2.8.

1. $O \rightarrow T$: $ma_1 = \text{S-Sig}_O(m, O, R, abort)$
2. $T \rightarrow O$: $ma_2 =$ *O* o *R* ja ha resolt l'intercanvi?

Sí:	$\text{S-Sig}_R(m)$	Si *R* l'ha resolt, o
	$\text{T-Sig}_R(m)$	Si *O* l'ha resolt
No:	$\text{S-Sig}_T(ma_1)$	
	aborted :=true	

Figura 2.8. Subprotocol *abort*

Si *T* té *m* com a resolt, significa que *T* ha resolt prèviament l'intercanvi. Com a resultat d'això i suposant que *T* és honesta, les parts *O* i *R* han pogut acabar l'intercanvi. Per tant, com a resposta a la petició d'*O*, *T* envia a *O*: $\text{S-Sig}_R(m)$ o $\text{T-Sig}_R(m)$. Qualsevol d'aquests elements serveix de prova que *R* ha signat *m*. Un *token abort* és una "promesa" que *T* no resoldrà aquest intercanvi en un futur. No és una prova que l'intercanvi s'hagi avortat, ja que les parts poden completar la signatura de contractes sense involucrar *T*.

Qualsevol de les dues parts pot demanar a *T* que resolgui l'intercanvi. El subprotocol *resolve* per *R* està especificat a la figura 2.9 (el subprotocol per *O* és anàleg).

1. $R \rightarrow T$: mr_1= $PCS_O(m, R, T)$, $S\text{-}Sig_R(m)$
2. $T \rightarrow R$: mr_2= *O* ja ha avortat l'intercanvi?
   - Sí: Enviar: $S\text{-}Sig_T(S\text{-}Sig_O(m, O, R, abort))$
   - No: *O* ha resolt l'intercanvi?
     - Sí: Enviar: $S\text{-}Sig_O(m)$
     - No: Guardar: $S\text{-}Sig_R(m)$
       Convertir $PCS_O(m, R, T)$ a $T\text{-}Sig_O(m)$
       Enviar: $T\text{-}Sig_O(m)$
     resolved :=true

Figura 2.9. Subprotocol *resolve*

Si el contracte no ha estat ni avortat ni resolt per cap de les parts, llavors *T* convertirà PCS a una signatura universalment verificable i ho enviarà a l'entitat que ha demanat l'execució d'aquest subprotocol. A més, *T* guardarà la signatura sobre el contracte de l'entitat que ha fet aquesta petició. Com queda clar, la primera petició que rep *T* determina l'estat permanent d'un intercanvi.

2.4.3.3 Corrupció de la tercera part

En aquesta secció veurem que si *T* és corrupta i per tant no exerceix el seu paper d'àrbitre independent, llavors pot provocar que es perdi l'equitat de l'intercanvi i, a més, no es podrà provar que la seva actuació ha estat errònia o mal intencionada. Tal com s'especifica a [ASW98], per provar això hauríem de menester com a mínim dos missatges inconsistents signats per *T*.

Per il·lustrar la situació suposem que *R* queda d'acord amb *O* per vendre-li la seva casa per un preu determinat. *O* li envia $PCS_O(m, R, T)$ en el primer missatge del subprotocol *exchange* per tal d'intercanviar la signatura de les parts sobre el contracte de compra-venda. Llavors *R* envia $PCS_O(m, R, T)$ a *T*. Si suposam que *T* és corrupta i actua del costat de *R*, convertirà la PCS a una signatura universalment verificable i li enviarà a *R* i a *O* només li enviarà un *token* d'avortament, si es dóna el cas (recordem que un *token abort* no és una prova que l'intercanvi s'hagi avortat). Això significa que s'ha perdut l'equitat de l'intercanvi i, a més, podria ser utilitzat per *R* per vendre a un preu més alt la seva casa; és a dir, per exemple podria mostrar el contracte signat per *O* a un altre comprador competidor per convèncer-lo que necessita pagar més que *O* si vol la casa.

La pèrdua de seguretat d'aquest protocol s'ha produït per culpa d'una tercera part corrupta i ningú no podrà demostrar aquest fet, ja que el missatge que *T* envia a *R* és T-Sig$_O$(*m*) i recordem que en la versió de PCS anomenada *third party-invisible* les distribucions de S-Sig$_O$(*m*) i T-Sig$_O$(*m*) són idèntiques.

Aquest problema podria generalitzar-se en els protocols de seguretat que pretenen que la TTP sigui transparent (és el cas del protocol que ara tractam). Aquesta propietat de les TTPs pretén que per mitjà de les evidències emeses durant una execució del protocol no es pugui saber si la TTP ha intervingut o no i així evitar mala publicitat tal i com expliquen O. Markowitch et al. a [MK01]. Per evitar això, els autors de l'anterior protocol proposen a [GJM99] una versió de PCS anomenada *third party-accountable* on les distribucions de S-Sig$_O$(*m*) i T-Sig$_O$(*m*) es poden distingir. En aquest cas, la TTP no seria transparent però evitaríem l'atac que acabam de descriure. El nom d'aquesta versió de PCS prové d'una propietat dels protocols de seguretat anomenada *accountability* que està definida per V. Shmatikov et al. a [SM02]. La propietat assegura que si una de les parts no segueix les passes del protocol i comet frau, els missatges del protocol mostraran sense ambigüitats qui és la part que ha comès el frau.

Ara bé, suposant aquesta nova versió de PCS, ens podem imaginar una nova situació on *O* no envia la signatura sobre el contracte a *R* (pas 3 del subprotocol *exchange*). Llavors *R* enviarà mr_1= PCS$_O$(*m*, *R*, *T*), S-Sig$_R$(*m*) a *T* com a petició perquè resolgui l'intercanvi. Però si *T* és corrupta i actua d'acord amb *O* poden fer creure a *R* que *O* ha cancel·lat la transacció (enviant-li S-Sig$_T$(S-Sig$_O$(*m*, *O*, *R*, *abort*))). Després *T* pot lliurar a *O* la signatura de *R* sobre el contracte: S-Sig$_R$(*m*). Aquesta mala actuació de la TTP que romp l'equitat de l'intercanvi (una part obté de la TTP una cancel·lació de la transacció i l'altra part obté la signatura sobre el contracte) no es pot provar, ja que no hi ha dos missatges signats per la TTP que siguin contradictoris.

Sembla evident que davant de situacions com les que acabam de descriure és difícil convèncer els usuaris d'una xarxa telemàtica que emprin el protocol per a qualsevol tipus d'intercanvi de signatures sobre un contracte. La TTP ha de garantir la seguretat de l'intercanvi però, com hem vist en el cas anterior, una errada seva (intencionada o no) pot tirar a baix la seguretat de l'intercanvi sense possibilitat de demostrar-ho i, en conseqüència, complica molt qualsevol rectificació que es vulgui fer.

2.5 Solucions al problema

Com podem observar es poden utilitzar una gran quantitat de mecanismes per a intercanvis comunicatius segurs. Això possibilita distints nivells de seguretat en funció dels mecanismes emprats per les TTPs en donar suport a un servei determinat. L'objectiu

principal d'aquesta tesi és trobar mecanismes que augmentin el nivell de seguretat de la prestació d'un servei per part de la TTP, cosa que facilita la confiança dels usuaris en aquesta entitat i així també facilitam l'ús dels nous procediments electrònics en l'aplicació dels quals es fa necessària o convenient la intervenció de TTPs. Per això, d'acord amb el que hem explicat, en els següents capítols mostrarem el camí que hem seguit per intentar donar la millor solució possible al problema dels usuaris reticents a emprar els nous procediments electrònics per les possibles conseqüències d'una mala actuació d'una TTP.

Inicialment pensàrem que la solució podria venir de l'enfocament que inclou múltiples terceres parts en el protocol. Per això vàrem idear una solució per un protocol tipus de protocol de seguretat que inclou múltiples TTPs preservant les característiques de seguretat encara que una minoria de les TTP involucrades sigui corrupta. La solució minimitza la sobrecàrrega en el càlcul i en les comunicacions que tradicionalment tenen aquest tipus de solucions, gràcies a l'ús exclusiu de criptografia simètrica i de clau pública i a un enfocament optimista del protocol. Ara bé, com és natural, aquests tipus de solucions tenen un cost intrínsec pel fet d'incloure múltiples terceres parts en un protocol. Per això, un segon pas ha estat el desenvolupament del concepte de verificabilitat per terceres parts de confiança. Sense cap dubte la introducció de la verificabilitat en els protocols de seguretat aporta una solució directa i eficient al problema plantejat com podrem deduir de les solucions que aportam en els capítols següents d'aquesta tesi.

Capítol 3

Protocol de correu electrònic certificat resistent a una minoria de terceres parts corruptes

3.1 Introducció

En aquest capítol presentam el disseny d'un protocol per al correu electrònic certificat (abreujat *cem*, per la seva escriptura en anglès). Aquesta proposta comporta el primer pas en la investigació duta a terme, ja que amb aquest protocol intentam fer un disseny que minimitzi els principals inconvenients de les propostes publicades anteriorment per altres autors. Els inconvenients als quals ens referim són els derivats de la inclusió de terceres parts en els protocols de seguretat. Les TTPs s'involucren en els protocols per donar solucions més simples i pràctiques a problemes plantejats com l'intercanvi equitatiu de valors. A canvi, els usuaris d'aquests procediments han de dipositar una certa confiança en les TTPs en el sentit que aquestes entitats podran actuar en ocasions en nom dels mateixos usuaris i podran emetre ítems d'informació que supleixen els que originalment ha pogut emetre l'usuari. En qualsevol cas, una mala operació de la TTP malmetrà la seguretat de l'intercanvi i això implica que el grau de confiança que els usuaris han de tenir en les terceres parts ha de ser elevat, sempre, com és natural, en funció de la importància de la transacció en curs. Hem vist en el capítol anterior distints enfocaments, proposats per altres autors, que pretenen minimitzar les conseqüències negatives que podria tenir la mala conducta d'una TTP dins d'un protocol. Fins i tot, alguns autors no inclouen l'ús de terceres parts en els seus protocols, però, com ja hem explicat, les seves solucions no són catalogades com a pràctiques, perquè per resoldre segons quins problemes (el correu electrònic certificat és un d'ells), no incloure de tercers parts de confiança comporta més inconvenients que no avantatges, com hem explicat en el capítol anterior.

Així, doncs, la proposta que presentarem tot seguit minimitza l'efecte negatiu que pot tenir la mala actuació d'una TTP en el protocol involucrant-hi un conjunt de terceres

parts. Aleshores, aconseguim que el protocol sigui resistent a una minoria de TTPs corruptes; és a dir, si una majoria de les terceres parts involucrades en el protocol actuen correctament la seguretat de l'intercanvi està garantida. D'aquesta manera aconseguim que el sistema sigui més robust i no fa falta que els usuaris hagin de dipositar tanta confiança en una TTP, ja que la seva actuació no és tan crítica.

Aquest tipus de solucions ja han estat investigades per altres autors, amb els inconvenients que ja hem esmentat anteriorment. No obstant això, nosaltres hem aplicat aquí aquest enfocament d'una nova forma que evitar en gran mesura les crítiques fetes. Reduïm la sobrecàrrega en les comunicacions i en el càlcul, que són els principals inconvenients d'aquestes solucions, aplicant de forma exclusiva la criptografia simètrica i de clau pública i, a més, reduïm les comunicacions plantejant un protocol optimista. Això vol dir que les terceres parts tan sols s'involucraran en el protocol en cas d'excepció i només a petició d'una de les dues parts protagonistes de l'intercanvi. Així, doncs, en aquest capítol proposarem un protocol de correu electrònic certificat on hem augmentat la confiança dels usuaris en el sistema ja que una minoria de terceres parts corruptes no poden comprometre l'equitat de l'intercanvi, perquè totes les terceres parts prenen les decisions de forma consensuada.

El correu certificat és un valor afegit a un sistema de correu electrònic. El correu certificat s'ha de correspondre amb el model d'un intercanvi equitatiu, perquè al final de l'intercanvi s'ha de garantir que cada una de les parts que intervenen en el protocol hagi rebut allò que esperava rebre provinent de l'altra part o que cap de les dues parts no hagi rebut res útil que el pugui posar en una posició d'avantatge respecte de l'altra. D'una banda, per tal de garantir un intercanvi equitatiu de valors, l'emissor del correu electrònic ha de poder provar que el receptor l'ha rebut. De l'altra banda, el receptor ha de poder provar que el suposat emissor és el veritable emissor del missatge. Llavors, com a mecanisme per proporcionar aquestes característiques al protocol, utilitzarem els serveis de no rebuig. Alguns serveis de no rebuig estan definits al documents ISO [ISO13888-1, ISO13888-2, ISO13888-3], dels quals ens interessen especialment aquest dos següents:

- *No rebuig d'origen* (NRO): aquest servei ve definit per protegir el receptor del missatge quan l'originador en nega falsament el contingut real i nega també el fet d'haver-lo emès; i
- *No rebuig de recepció* (NRR): aquest servei ve definit per protegir l'originador del missatge quan el receptor nega falsament haver-lo rebut.

En qualsevol protocol es fa difícil obligar les parts implicades a enviar una evidència[2] de no rebuig. Com a conseqüència, alguns protocols per al correu electrònic certificat involucren una tercera part per tal d'assegurar l'equitat de l'intercanvi. Algunes vegades, aquestes terceres parts es veuen involucrades d'una forma activa en el protocol [F94, ZG96b, AT94, DGL96]. En altres solucions proposades, les terceres parts només es veuen involucrades en cas d'excepció [ASW97, FHM98, FRH94]. En canvi, altres tipus de protocols per al correu electrònic certificat intenten aconseguir equitat a través de l'emissió gradual de secrets, emprant molts d'intercanvis d'informació [TEDIS94, AT94, B83]. Els avantatges i inconvenients de cada un d'aquests tipus de protocols ja ha estat objecte d'estudi en el capítol anterior.

Els protocols que utilitzen una tercera part en cada execució poden tenir problemes de comunicacions, ja que la tercera part podria convertir-se en un coll d'ampolla. A més a més, la mala conducta d'aquesta tercera part pot comprometre la seguretat de l'intercanvi. Nosaltres presentam aquí una proposta de protocol de correu electrònic certificat, en el qual les terceres parts només es veuen involucrades en cas d'excepció i pot tolerar (és a dir, l'equitat no es veu compromesa) la mala conducta d'una minoria de terceres parts. Com que les terceres parts només intervendran en casos excepcionals, difícilment es convertiran en un coll d'ampolla. Per aquest protocol és necessari que l'emissor i el receptor del correu electrònic certificat es posin d'acord amb una *deadline* (termini de temps). Nosaltres assumim que, abans d'aquest termini, l'originador i el receptor poden establir contacte amb la tercera part si ells creuen que es veu compromesa l'equitat de l'intercanvi.

3.2 Preliminars

En aquesta secció, revisarem algunes primitives que utilitzarem en les seccions següents. Aquest protocol que presentam empra criptosistemes simètrics i de clau pública. Naturalment podem trobar criptosistemes d'aquests tipus computacionalment segurs (per exemple, a les següents referències [S96, S95] trobarem explicacions d'alguns d'aquests criptosistemes segurs). L'ús de funcions unidireccionals de *hash* també és important per a la signatura digital feta amb criptografia de clau pública [S96, S95] i, per això, agafam la sortida de la funció de *hash* com a entrada d'un criptosistema de clau pública. El receptor d'un missatge xifrat pot obtenir d'una manera fiable la clau pública de l'originador del missatge mitjançant l'ús de certificats X.509 [X.509].

[2] Una *evidència* és una informació que, o bé per ella mateixa o bé emprada en conjunció amb altra informació, s'utilitza per establir una prova sobre algun esdeveniment o acció [ISO13888-1].

A les nostres propostes empram la següent notació *nombre.*{*acció*}:{*descripció*} per descriure cada una de les accions individuals dutes a terme pels participats en el protocol, on *nombre* és el número de seqüència dins del protocol de l'acció concreta que descrivim, {*acció*} pot ser, per exemple, l'enviament d'un missatge de l'usuari *X* a l'*Y* (designat per $X \rightarrow Y$) o l'execució d'algun càlcul d'un participant (designat pel seu nom). La {*descripció*} és una breu explicació del tipus de contingut del missatge intercanviat o del tipus d'acció executada localment. A la figura 3.1, detallam la notació que empram per descriure accions concretes dels usuaris en el protocol:

L'originador *X* envia els missatges *m* i *n* al receptor *Y*	$X \rightarrow Y$: m, n
El missatge *m* és enviat a l'usuari *Y*. Aquest missatge conté els ítems *a*, *b*, ...	$X \rightarrow Y$: $m = [a, b, ...]$
Els missatge *m* és enviat per l'usuari *X* als receptors TP_1, TP_2 ... TP_n	$X \rightarrow TP_1 ... TP_n$: m
Els originadors TP_1, TP_2 ... TP_n envien a *X* els missatges m_1, m_2 ... m_n respectivament	$TP_i \rightarrow X$: $m_i \quad (1 \leq i \leq n)$
Xifratge del missatge *m* amb la clau privada de l'usuari *X*. En aquest xifratge, tots els càlculs estan fets amb un criptosistema amb les mateixes característiques del criptosistema RSA descrit a [RSA78]	$PR_X(m)$
Sortida d'una funció unidireccional de *hash h* que agafa el missatge *m* com a cadena d'entrada	$h(m)$
El missatge *m* està format pels ítems m_1, m_2 ... m_n	$m = \Sigma_{i=1..n} m_i$

Figura 3.1. Notació

3.3 El protocol de correu electrònic certificat

El correu electrònic certificat consisteix en l'intercanvi d'un missatge i juntament amb l'intercanvi d'una evidència de no rebuig d'origen a canvi d'una evidència de no rebuig de recepció. En el nostre protocol, un usuari que desitja enviar un correu electrònic certificat ha de tenir un contracte amb una tercera part. Quan ocorre una excepció en el protocol de correu electrònic certificat, qualsevol part involucrada en aquest hauria d'establir contacte amb aquesta tercera part, per tal de resoldre l'excepció que s'ha produït. En aquest protocol, la tercera part és membre d'una organització de terceres parts que prenen decisions de forma consensuada sobre els casos d'excepció que ocorren en els protocols. Aquestes decisions es prenen d'acord amb les especificacions del protocol descrites en aquest capítol per als casos d'excepció. Això significa que tant l'emissor com el receptor

d'un correu electrònic certificat confien en l'organització de terceres parts i no necessiten confiar en només una tercera part. El protocol és resistent a una minoria de terceres parts corruptes, perquè les decisions són preses per l'organització de terceres parts. Les terceres parts es veuen involucrades en el protocol de correu electrònic certificat només en cas d'excepció (per exemple, una de les dues parts involucrades en el protocol no ha rebut el missatge apropiat d'acord amb les especificacions fetes).

Quan l'emissor té un contracte signat amb una tercera part, durant el temps de vida d'aquest contracte pot enviar qualsevol quantitat de missatges; és a dir, no fa falta crear un contracte nou amb una TTP cada vegada que s'hagi d'enviar un correu certificat. Naturalment, abans d'enviar el correu electrònic certificat, és necessari que el receptor accepti la mediació de les terceres parts en cas d'excepció.

3.3.1 Descripció del protocol

En aquesta secció, descriurem més detalladament el nostre protocol de correu electrònic certificat. En primer lloc, un usuari que vol emetre aquest tipus de missatges ha d'executar l'anomenat *protocol de contracte* per poder obtenir el contracte amb l'organització de terceres parts. Llavors pot enviar tants de missatges de correu certificat com vulgui mitjançant l'execució del protocol que hem anomenat *protocol bàsic*. Després d'això, si no ha ocorregut cap excepció, el receptor tendrà el missatge de correu electrònic juntament amb una prova de no rebuig d'origen i l'emissor tendrà una prova de no rebuig de recepció. Però, si hi ha hagut algun problema i algunes de les parts no pot completar l'intercanvi, llavors serà necessari que es posi en contacte amb les TTPs perquè l'intercanvi acabi amb els requisits de seguretat complerts. En l'especificació que fem aquí del protocol, volem remarcar que hem deixat alguns aspectes al marge, sempre en benefici d'una millor comprensió dels aspectes fonamentals de seguretat que són els que aquí volem assenyalar de forma especial. Alguns d'aquests aspectes que no detallam però que més endavant veurem que són necessaris per a la implementació del protocol són, per exemple, com s'estableix una associació de terceres parts i com s'acredita davant d'un usuari o algunes qüestions de sincronia, com el format del termini de temps t_A i respecte a quin rellotge es faria aquest segellat temporal.

3.3.1.1 El protocol de contracte

Recordem que un usuari (el qual anomenarem *A*) ha de tenir un contracte amb una tercera part per poder enviar correus electrònics certificats. Per tant, abans de començar a enviar correus, l'usuari haurà d'establir contacte amb una tercera part que col·labori amb una associació de terceres parts. En el primer pas del protocol, l'usuari *A* envia a les seves credencials (per exemple, un identificador com a usuari Id_A) i un termini t_A cap a aquesta tercera part, TP_0. El termini t_A representa el temps límit abans del qual la TP_0 (o la seva

organització) intentarà resoldre de forma equitativa els casos d'excepció que puguin ocórrer quan l'usuari *A* enviï un correu electrònic certificat. En el segon pas del protocol, si la TP_0 ha acceptat aquesta petició, llavors passa a notificar a les altres terceres parts que l'usuari ha demanat la intervenció de les terceres parts en cas d'excepció. Finalment, després que totes les terceres parts hagin acceptat la petició de l'usuari, la TP_0 envia a l'usuari *A* el contracte de suport per a casos d'excepció (indicat de forma esquemàtica a la taula següent com a C_A). Amb l'execució d'aquest protocol l'usuari *A* haurà obtingut d'un grup de terceres part el compromís d'arbitrar de forma col·legiada els problemes de seguretat que puguin afectar l'equitat de l'intercanvi en l'enviament d'un correu electrònic certificat. També, d'aquesta manera, el receptor del correu (l'usuari *B*) podrà decidir a l'inici de l'intercanvi si accepta o no accepta, en funció de la confiança que hi pugui tenir, la mediació d'aquest conjunt de TTPs en cas d'excepció. El *protocol de contracte* està especificat a la figura 3.2.

1. $A \rightarrow TP_0$: Id_A, t_A, n+1
2. $TP_0 \rightarrow TP_1 \ldots TP_n$: Id_A, t_A, n+1
3. $TP_i \rightarrow TP_0$: $C_{Ai} = PR_{TPi}$ (Id_A, t_A, n+1) $(1 \leq i \leq n)$
4. $TP_0 \rightarrow A$: $C_A = [\Sigma_{i=1..n} C_{Ai}, PR_{TP0}$ (Id_A, t_A, n+1)]

Figura 3.2. Protocol de contracte

C_{Ai} és el conjunt de missatges que cada TP_i (i = 1 ... n) envia a la TP_0 per indicar que accepta la petició de l'usuari. Si una o més terceres parts no accepten aquesta petició, llavors l'organització no intervindrà en el protocol. El missatge C_A està format pel conjunt d'ítems C_{Ai} i per l'ítem mitjançant el qual TP_0 accepta la petició de l'usuari. Hem d'observar que dins de C_A hi ha la signatura de totes les terceres parts lligades a l'identificador de l'usuari, a el termini t_A i, també, a la quantitat de terceres parts que intervendran en el protocol (n+1). Naturalment, l'organització de terceres parts estarà operativa fins a t_A com a mínim. En cas contrari, la TP_0 podria suggerir a l'usuari un altre temps de cobertura per a aquestes situacions d'excepció.

3.3.1.2 El protocol bàsic

El *protocol bàsic* servirà a un usuari per emetre un correu electrònic certificat i està dividit en dos subprotocols. El primer subprotocol és el de la configuració de la transmissió que es vol realitzar, en el qual l'originador, l'usuari *A*, envia al receptor, l'usuari *B*, els paràmetres de la transmissió del correu electrònic certificat. Si *B* accepta aquests paràmetres, llavors pot començar el segon subprotocol, on es duu a terme la transmissió del missatge de correu electrònic certificat i l'intercanvi d'evidències de no rebuig. El

subprotocol de *configuració de la transmissió* ve especificat en els dos passos de la figura 3.3.

1. A $\rightarrow$ B: p = [h, t'_A, C_A, I, m], $s_A = PR_A(h(p))$
2. B $\rightarrow$A: $s_B = PR_B(h(p))$

Figura 3.3. Subprotocol de *configuració de la transmissió*

on el missatge p conté els paràmetres de la figura 3.4.

t'_A	És un termini fixat per l'usuari A, abans del qual l'emissor o el receptor han d'establir contacte amb la TP_0 en cas d'excepció perquè aquesta resolgui la situació. Naturalment, t_A representa un temps posterior a t'_A.
M	És un nombre inferior o igual a n+1 i més gran que (n+1)/2; representa la mínima quantitat de terceres parts que han d'actuar d'acord amb el protocol (això és, les terceres parts que no han d'ésser corruptes), perquè d'aquesta manera es garanteixi l'equitat de l'intercanvi.
I	És una cadena de caràcters que identifica de forma única la transacció.

Figura 3.4. Paràmetres

El missatge s_B representa l'acceptació dels paràmetres per part del receptor B. Quan A rep el missatge s_B, pot generar una clau K d'un criptosistema simètric i xifrar el missatge de correu M; llavors pot començar la transmissió. Però, si l'usuari B no accepta els paràmetres enviats, llavors no enviarà s_B i el protocol es dóna per acabat. El subprotocol de *transmissió* està especificat en la figura 3.5.

1. A $\rightarrow$ B: $c = E_K(M)$, $h_A = PR_A(h(c, I))$
2. B $\rightarrow$ A: $h_B = PR_B(h(c, I))$
3. A $\rightarrow$ B: $k_A = PR_A(K, I)$
4. B $\rightarrow$ A: $k_B = PR_B(K, I)$

Figura 3.5. Subprotocol de *transmissió*

on *c* és el missatge de correu xifrat a través de la clau *K*. Quan *B* rep h_A, després envia h_B. L'ítem h_B representa el compromís del receptor a rebre el missatge de correu. Després l'usuari *B* rep la clau *K*, signada per l'usuari *A*, i llavors pot desxifrar el missatge *c*. Els ítems h_A i k_A són l'evidència de no rebuig d'origen. Finalment, *B* envia k_B. Els ítems h_B i k_B són l'evidència de no rebuig de recepció.

Ara acabam de descriure els dos darrers subprotocols de forma separada, ja que tenen un objectiu diferent, el primer configura la transmissió i el segon la duu a terme. No obstant això, per tal de fer més eficient el subprotocol *bàsic*, podem agrupar els dos subprotocols anteriors de la manera descrita a la figura 3.6.

1. A $\rightarrow$ B: p, c, h_A
2. B $\rightarrow$ A: s_B, h_B
3. A $\rightarrow$ B: k_A
4. B $\rightarrow$ A: k_B

Figura 3.6. Execució dels dos subprotocols en paral·lel

Amb l'esquema de la figura 3.4, durant el pas 1 i 2 s'executa el subprotocol de *configuració de la transmissió*, al mateix temps que es poden començar a executar els dos primers passos del subprotocol de *transmissió*. L'única conseqüència que té això és que el *subprotocol bàsic* s'executa en només quatre passos en lloc de sis i, per tant, podem obtenir una major eficiència.

3.3.2 Excepcions al protocol bàsic

Quan l'emissor o el receptor de l'anterior protocol de correu electrònic certificat no reben el missatge apropiat d'acord amb les especificacions de l'intercanvi, aleshores la part afectada ha d'establir contacte amb la tercera part TP_0 per poder restablir l'equitat de l'intercanvi. En qualsevol situació d'excepció, la TP_0 provarà d'establir contacte amb la part que suposadament no ha seguit el *protocol bàsic*. Si aquesta part respon com hem especificat a l'apartat anterior, aleshores el protocol es podrà completar tal i com ja hem explicat. Però si això no és possible, les tercers parts actuaran de la manera que descrivim a les seccions que venen a continuació, exceptuant, com és natural, que alguna d'aquestes terceres parts fos corrupta.

Hem de remarcar el fet que, quan l'emissor o el receptor del protocol (descrits com *A* i *B* a l'apartat anterior) signen s_A i s_B respectivament, estan acceptant la intervenció de les TTPs

en aquesta transacció; per tant, les autoritzen a actuar en nom seu, emetent evidències de no rebuig tal i com estableix el protocol per a casos d'excepció que descriurem a les seccions següents.

3.3.2.1 No recepció de l'ítem k_B

Quan l'usuari *A* diu[3], abans del termini t'_A, que no ha rebut de *B* l'ítem k_B, llavors, per tal de posar-se en contacte amb les terceres parts, hauria d'executar el protocol que especificam a la figura 3.7.

1. $A \rightarrow TP_0$: p, s_B, c, h_A, h_B, k_A
2. $TP_0 \rightarrow TP_1 \ldots TP_n$: p, k_A
3. $TP_1 \ldots TP_n \rightarrow TP_0$: $ACK = \Sigma_i\, PR_{TPi}$ ('ok', I) [mín. m]
4. $TP_0 \rightarrow A$: $k_T = PR_{TP0}(h(c, I, ACK))$, ACK

Figura 3.7. Protocol d'excepció k_B

En aquest protocol, *A* envia a la TP_0 tota la informació que té sobre la transacció de correu que està duent a terme. Llavors la TP_0 pot verificar que l'usuari *B* desitjava rebre el missatge de correu electrònic certificat (la TP_0 ho pot comprovar verificant l'ítem h_B). Seguidament la TP_0 notifica aquest fet a les altres terceres parts. Quan la TP_0 rep l'aprovació (el missatge xifrat amb la clau privada del text 'ok' lligat amb l'identificador de la transacció) de com a mínim *m* terceres parts (indicat a la taula en el tercer pas del protocol per [mín. *m*]), llavors la TP_0 envia k_T a l'usuari *A*. L'ítem k_T que acaba de rebre *A* té el mateix efecte que l'ítem k_B (la tercera part ha actuat en nom de *B*, ja que s_B l'autoritza a fer-ho).

No obstant això, existeix la possibilitat que *A* no pugui establir contacte amb la TP_0 abans de t'_A. En aquest cas, i entre els terminis t'_A i t_A, si l'usuari *A* encara desitja completar l'evidència de no rebuig de recepció, llavors haurà d'establir contacte amb totes les terceres parts de l'organització d'acord amb els passos especificats a la figura 3.8.

1. $A \rightarrow TP_0 \ldots TP_n$: p, s_B, c, h_A, h_B, k_A
2. $TP_0 \ldots TP_n \rightarrow A$: $k_{Ti} = PR_{TPi}(c, I)$ [mín. m]

Figura 3.8. Alternativa al protocol d'excepció k_B

[3] Cal observar que *A* diu que no ha rebut k_B, però que aquesta afirmació no ha estat provada.

Aquí, les terceres parts després de comprovar el compromís de *B* a rebre el missatge de correu, envien el corresponent ítem k_{Ti} a l'usuari *A*. Una quantitat de *m* ítems k_{Ti} tenen el mateix efecte que l'ítem k_B .

Podem trobar un altre cas especial: quan l'usuari *B* executa el protocol especificat en la següent secció, aleshores pot obtenir una evidència de cancel·lació de la transacció. En aquest cas, *B* diu abans del termini t'_A que *A* ha seguit els passos que hi ha especificats en el *protocol bàsic*, però que no l'ha arribat a completar, perquè l'usuari *A* no li ha enviat l'ítem k_A que li fa falta per poder desxifrar el missatge. Per això, en aquestes circumstàncies, el segon pas del protocol que hem acabat d'especificar ha d'ésser el de la figura 3.9.

2. TP_0 ... $TP_n \rightarrow$ A: $k'_{Ti} = PR_{TPi}(c, l,$ 'cancellation_ alert')

Figura 3.9. Alternativa al protocol de la figura 3.6

En aquests missatges, les terceres parts signen el text "cancellation_ alert" per tal de notificar a l'usuari *A* que *B* ha cancel·lat la transacció.

3.3.2.2 No recepció de l'ítem k_A

Quan l'usuari *B* diu[4], abans del termini t'_A, que no ha rebut d'*A* l'ítem k_A, llavors, per tal de posar-se en contacte amb les terceres parts, hauria de posar en marxa el protocol que especificam a la figura 3.10.

1. B $\rightarrow$ TP_0: c, h_A, h_B, p
2. $TP_0 \rightarrow$ B: $s_T = PR_{TP0}(h(p))$
3. $TP_0 \rightarrow TP_1$ ... TP_n: p, $PR_{TP0}(s_T,$ 'cancellation')
4. (when t'_A) $TP_0 \rightarrow$ B: $c_{T0} = PR_{TP0}(h($'cancellation', c, $l))$

Figura 3.10. Protocol d'excepció k_A

En aquest protocol *B* envia a la TP_0 tota la informació que té sobre la transacció. En el segon pas la TP_0 envia l'ítem s_T a *B* en senyal que admet la petició. Després la TP_0 pot verificar que ha estat l'usuari *A* qui ha començat la comunicació i, per tant, la TP_0 prova d'establir contacte amb aquest usuari, encara que, per claredat, no ho hem descrit a la figura 3.8 . Si *A* no contesta (per tant, això significa que el *protocol bàsic* no pot acabar

[4] Cal observar que *B* diu que no ha rebut k_A, però que aquesta afirmació no ha estat provada.

normalment), llavors la TP_0 envia a l'usuari *B* la cancel·lació de la transacció (representat per l'ítem c_{To}) a l'instant de temps t'_A. La TP_0 notifica la petició de *B* a les altres terceres parts, enviant-los els paràmetres de la transacció de correu amb el text "cancellation".

Si abans o durant l'execució d'aquest protocol, l'usuari *A* executa el protocol especificat a la secció 3.3.2.1, llavors el darrer pas del protocol d'aquesta secció s'ha de modificar i han d'executar-se els dos passos descrits a la figura 3.11 en el seu lloc.

4. $TP_0 \rightarrow B$: $k_{AT0} = PR_{TP0}(k_A, l)$
5. $TP_0 \rightarrow TP_1 ... TP_n$: k_{AT0}

Figura 3.11. Modificació al protocol de la figura 3.8

Podria passar que l'usuari *B* no pogués establir contacte amb la TP_0 abans del temps especificat al termini t'_A. En aquest cas, i entre els terminis t'_A i t_A, si *B* diu que no ha rebut l'ítem k_A provinent d'*A*, llavors haurà d'establir contacte amb totes les terceres parts de l'organització seguint els passos especificats a la figura 3.12.

1. $B \rightarrow TP_0 ... TP_n$: c, h_A, h_B, p
2. $TP_0 ... TP_n \rightarrow B$: $c_{Ti} = PR_{TPi}(h(\text{'cancellation'}, c, l))$ [mín. m]

Figura 3.12. Alternativa al protocol d'excepció k_A

on una quantitat *m* d'ítems c_{Ti} té el mateix efecte que l'ítem c_{T0}. No obstant això, si l'usuari *A* ha executat el protocol de no recepció de l'ítem k_B (figures 3.5 i 3.6), llavors el segon pas del protocol especificat a la figura 3.10 ha d'ésser tal i com especifica la figura 3.13.

2. $TP_0 ... TP_n \rightarrow B$: $k_{ATi} = PR_{Ti}(k_A, l)$

Figura 3.13. Modificació al protocol de la figura 3.10

3.4 Discussió del protocol

Ara revisarem per què el nostre protocol compleix amb el requeriment d'equitat per al correu electrònic certificat emprant els mecanismes de no rebuig que hem descrit a la primera secció d'aquest capítol. Quan el *protocol bàsic* acaba amb èxit, llavors l'equitat de l'intercanvi està naturalment assegurada: l'emissor té una evidència de no rebuig de

recepció (el conjunt format pels ítems h_B i k_B) i el receptor té el missatge i una evidència de no rebuig d'origen (el conjunt format pels ítems h_A i k_A).

En cas d'excepció, si a l'instant de temps t que ens trobam és inferior a t'_A, llavors el protocol aconsegueix l'equitat tant per a l'emissor com per al receptor. Perquè les terceres parts poden generar un ítem de reemplaçament per l'evidència de no rebuig d'origen o bé per l'evidència de no rebuig de recepció quan l'emissor o el receptor estableixen contacte amb la TP_0. Això passa sempre i quan hi hagi com a mínim m terceres parts que actuen d'acord amb el protocol, és a dir, que no són corruptes, perquè llavors elles poden fer una d'aquestes accions:

- Generar un ítem de reemplaçament per a l'emissor (l'ítem k_T)
- Revocar l'ítem h_B enviat per l'usuari B (amb l'ítem c_{T0})
- Generar un ítem de reemplaçament per al receptor B (l'ítem k_{AT0})

Si B estableix contacte amb les terceres parts després del temps especificat al termini t'_A i els diu que no ha rebut l'ítem k_A que espera d'A, llavors pot rebre de les terceres parts un d'aquests dos missatges:

- Un conjunt de com a mínim m ítems c_{Ti}, que és l'evidència de cancel·lació del seu compromís de completar el *protocol bàsic* amb l'ítem h_B que havia emès
- Un ítem k_{ATi}, com a mínim, on B pot aconseguir l'ítem k_A i d'aquesta manera completar l'evidència de no rebuig d'origen que s'havia compromès a enviar l'originador en el *protocol bàsic*.

Per tant, tal i com hem especificat, el protocol també proporciona equitat per al receptor del missatge en aquest cas.

Quan l'usuari A es posa en contacte amb les terceres parts després del termini t'_A, aleshores rep de les terceres parts el conjunt de missatges k_{Ti} que són equivalents a l'ítem k_B perquè A no havia rebut l'ítem k_B provinent de l'usuari B. Per tant, l'equitat de l'intercanvi per a l'usuari A, s'aconsegueix a partir de la situació descrita. No obstant això, en el cas especial que el receptor B ja hagi cancel·lat l'intercanvi, les terceres parts no poden enviar a A l'ítem per poder completar l'evidència de no rebuig de recepció. Consegüentment, només poden alertar A que, encara que diu que ha enviat l'ítem k_A, B ha dit que no l'ha rebut. Per tant, les terceres parts només poden emetre els ítems k'_{Ti}, que fan de testimoni d'allò que ha passat durant l'intercanvi. L'usuari A sempre pot utilitzar el conjunt d'ítems k'_{Ti} en un sistema extern de resolució de disputes per tal d'aconseguir l'equitat.

Hem d'observar que en aquest darrer cas especial, quan l'usuari *B* ja ha aconseguit l'equitat gràcies a l'evidència de cancel·lació, com ja hem dit, les terceres parts no poden enviar a l'usuari *A* l'equivalent a una prova de no rebuig de recepció, perquè, de cap manera, les terceres parts no poden degradar l'equitat que ha aconseguit qualsevol usuari, *B* en aquest cas.

Hem definit t'_A com a una estimació del temps abans del qual l'emissor o el receptor han d'establir contacte amb la TP_0 en cas d'excepció. El termini t'_A hauria de representar un temps relativament proper al temps *t* actual, és a dir, al temps en què es configura el protocol per emetre un nou missatge de correu certificat. Aquest temps ha de servir per poder solucionar qualsevol excepció possible garantint l'equitat en un temps raonablement curt. És a dir, la distància entre *t* i t'_A ha d'ésser suficient per poder completar el *protocol bàsic* i, en cas d'excepció, els usuaris han de poder posar-se en contacte amb la TP_0 per enviar-li la informació adient i aquesta ha de contestar amb l'ítem adient, fins i tot si les connexions de xarxa entre al TP_0 i l'usuari no són fiables. No obstant això, en cas d'excepció el protocol preveu que un usuari pugui establir contacte amb les terceres parts després del termini t'_A, però l'equitat en aquest cas no es garanteix de forma directa.

Hem vist que les terceres parts poden generar ítems de reemplaçament o revocar l'ítem h_B, però una TTP no corrupta no generarà missatges de reemplaçament en nom d'una part que té una conducta correcta, només ho poden fer en nom d'una part que suposadament no es comporti tal i com el protocol especifica. Consegüentment, quan l'emissor o el receptor d'un correu electrònic certificat invoquen una tercera part no corrupta, primerament aquesta comprova la correcció dels missatges, per poder saber si l'usuari, que ha reclamat el seus serveis, ha rebut cap missatge de compromís per part de l'altre usuari. Després la tercera part prova de posar-se en contacte amb la part que suposadament no ha seguit el protocol i finalment generarà un ítem de reemplaçament només en el cas que no rebi resposta segons especifica el *protocol bàsic* provinent d'aquesta tercera part. Ara bé, un aspecte important a tenir en compte és que no és necessari que els usuaris dipositin una confiança incondicional en les terceres parts. Qualsevol ítem de reemplaçament emès per les terceres parts només té el seu valor i significat correctes si com a mínim *m* terceres parts hi estan d'acord. Llavors, el protocol garanteix equitat si com a mínim *m* terceres parts de l'organització actuen correctament. La resta de terceres parts (*n*-*m* terceres parts) poden ser corruptes (per exemple, poden negar el servei a la petició d'un usuari) i el protocol continuarà garantint l'equitat de l'intercanvi.

És important observar que l'equitat es garanteix fins i tot si la TP_0 és una d'aquestes terceres parts corruptes. En el pitjor dels casos, quan la TP_0 és una tercera part corrupta i un error en les comunicacions en la xarxa ocorre quan l'usuari *A* està enviant k_A, aleshores *A* pot creure que el missatge ha arribat a la seva destinació i demana a la TP_0 corrupta que faciliti l'equitat de l'intercanvi. Podem suposar que la TP_0 seguirà el protocol i retornarà a

A un ítem vàlid k_T. Mentrestant, l'usuari *B* demana la cancel·lació i a l'instant t'_A a la TP_0 corrupta i aquesta li envia el missatge c_{T0}. Per tant, al mateix temps, l'usuari *A* té una evidència de no rebuig de recepció i *B* té una evidència de cancel·lació de la transacció vàlida. *A* i *B* han actuat de bona fe, i sembla que la TP_0 hagi romput el sistema. No obstant això, si posteriorment l'usuari *A* o *B* se senten perjudicats pel funcionament maliciós de la TP_0, llavors poden anar a un sistema extern de resolució de disputes (com és ara un tribunal de justícia) per aconseguir l'equitat de l'intercanvi. Llavors quedarà bastant clar que la TP_0 ha signat dos missatges amb un significat oposat i, per tant, queda clar que la TP_0 no ha seguit les especificacions del protocol. És a dir, la mala actuació de la tercera part no només es detectarà sinó que també es podrà demostrar.

Per tant, amb aquest protocol, els usuaris no han de tenir una confiança incondicional en la tercera part; només han d'esperar que *m* de les *n* terceres parts actuïn d'acord amb el protocol per a casos d'excepció. Aquesta característica del protocol s'assoleix sense haver d'utilitzar cap esquema criptogràfic llindar.

3.5 Conclusions

En aquest capítol hem presentat el disseny d'un protocol pràctic per al correu electrònic certificat. L'originador del missatge té un contracte de suport per a casos d'excepcions amb una organització de terceres parts. Quan el protocol ha acabat, si no ha passat cap excepció, el receptor té el missatge de correu amb una prova de no rebuig d'origen, l'emissor té una prova de no rebuig de recepció del missatge i no ha estat necessària la intervenció de cap tercera part.

Les terceres parts només es veuen involucrades en el protocol en casos d'excepció. Aquestes garanteixen l'equitat de l'intercanvi quan ocorre una excepció, fins i tot si una minoria d'aquestes és corrupta. Consegüentment, es redueix la quantitat de confiança que els usuaris han de dipositar en una tercera part. El protocol aconsegueix aquestes característiques sense la utilització dels costosos esquemes criptogràfics llindar, només utilitza un criptosistema simètric, un de clau pública i una funció unidireccional de *hash*.

Amb aquest protocol ens hem acostat a les propostes que només involucren una tercera part, ja que les TTPs no tenen una forta intervenció en el protocol (*Optimistic Approach* d'acord amb la nomenclatura que varen introduir N. Asokan et al. a [ASW97]) i utilitzen esquemes criptogràfics convencionals. A més, el protocol té l'avantatge de donar més confiança als usuaris que puguin ser reticents a la intervenció de la tercera part, perquè, com ja hem esmentat abans, una minoria de terceres parts corruptes no pot rompre la seguretat de l'intercanvi. No obstant això, sembla prou evident que el protocol, per la seva naturalesa, requereix de més intercanvis de comunicació que els protocols optimistes per

al correu electrònic certificat que només compten amb la intervenció d'una TTP. Això significa que aquesta és una bona proposta, però no en totes les situacions. És a dir, aquest protocol pot ser especialment indicat en casos on la desconfiança és elevada ja que garanteix la seguretat de l'intercanvi, fins i tot en casos de terceres parts corruptes, a canvi d'un petit *overhead* en comunicacions. Per tant, pensam que la proposta feta és una bona primera passa per a la definició de protocols pràctics on el grau de confiança que es demana als usuaris sobre l'actuació d'una TTP no sigui tan gran; ara bé, consideram que hi ha marge per a la millora. I la millora podria passar per la definició de protocols de seguretat amb solament una tercera part de confiança on no sigui necessari requerir que l'usuari hagi de dipositar una confiança incondicional en l'actuació d'aquesta entitat perquè la seguretat de l'intercanvi estigui garantida.

Capítol 4

Anàlisi dels serveis de seguretat

4.1 Introducció

A mesura que les comunicacions electròniques s'han fet cada vegada més importants, especialment en els procediments actuals de comerç electrònic, els serveis de seguretat hi juguen un paper més important per tal de protegir-les de possibles amenaces. Aquests serveis de seguretat s'apliquen a comunicacions amb aspectes diversos com, per exemple, l'autenticació, el control d'accés, la confidencialitat de dades, la integritat de dades o no rebuig. Els serveis de seguretat tenen aplicació en molts diversos camps, com per exemple en les transaccions electròniques en la WWW, el correu electrònic, el servei de directori (DNS, X.500, LDAP), EDI o en sistemes de pagament electrònics. Dins d'aquest context, doncs, de la implantació de procediments electrònics, de vegades, el servei de seguretat pretén ser garantit per entitats remotes independents anomenades terceres parts de confiança.

Recordem que una *tercera part de confiança* (TTP) és una autoritat de seguretat que és de confiança per a altres entitats amb relació a les activitats de seguretat que duu a terme tal com s'expressa a [X.810]. També hem vist que, depenent del protocol i de la política de seguretat, podem veure que les TTPs es poden involucrar de diferents formes per tal d'ajudar els usuaris a aconseguir els requeriments de seguretat en una determinada transacció electrònica.

En general, d'acord amb la recomanació [X.509], podem dir que una entitat confia en una altra quan la primera assumeix que la segona entitat es comportarà exactament com la primera espera. Ha de quedar clar, doncs, que hi ha un marge d'error en el qual la TTP podria (intencionadament o no) rompre la confiança que els usuaris han dipositat en l'entitat i, d'aquesta manera, malmetre la seguretat d'una determinada transacció electrònica. La confiança a la qual fem esment, tal com indica el document [ETS97], pot

referir-se a diversos aspectes: la integritat de les dades, qui n'és el responsable, qui pot accedir-hi i com estan disponibles.

Les TTPs proporcionen una àmplia varietat de serveis de confiança. En documents com [ETS97, FMH00, N97, X.842] en podem trobar una bona mostra, com per exemple, la certificació de clau pública, generació de claus i recuperació de claus, expedició de diners electrònics, time-stamping, servei de testimoniatge (servei de notaria), registre d'evidències. A causa d'aquesta gran varietat de serveis de seguretat, han aparegut diferents tipus de TTPs. Per tant, en un protocol podem trobar diferents TTPs que proporcionen distints serveis de confiança. Així, podem parlar d'Autoritats de Certificació, Autoritats de registre, Autoritats de lliurament, Bancs electrònics, Notaris electrònics, Jutges electrònics. No obstant això, tal i com ja destaca A. Nilson a [N97], és interessant observar que, malgrat la seva diversitat, les TTPs operen de forma semblant encara que donin suport a serveis de seguretat molt diversos.

En resum, els usuaris de diferents serveis de seguretat tenen, doncs, el problema d'haver de interactuar amb diferents tipus de TTPs, que són vistes com a entitats virtuals remotes i si l'usuari no coneix o no té garanties sobre el seu funcionament pot tenir reticències a utilitzar-ne els serveis. Així, en aquest capítol proposarem un mètode per poder classificar i analitzar (en definitiva, conèixer) l'actuació de les TTPs quan donen un servei de seguretat als usuaris dins l'entorn d'un determinat protocol. L'objectiu final d'aquest estudi sobre els serveis de les TTPs ha estat la recerca d'aquella característica o propietat (la *verificabilitat* de la TTP) que posteriorment hem introduït dins dels protocols de seguretat i que ens ha fet augmentar la confiança dels usuaris en l'ús d'aquestes entitats. Aquest nou tipus de solució, que desenvoluparem en els capítols següents, millora la confiança dels usuaris sense haver d'involucrar moltes TTPs en un protocol amb la consegüent reducció de costs.

4.2 Anàlisi dels serveis de seguretat de les TTPs

Podem veure una TTP com una organització independent amb un nivell de seguretat suficient perquè sigui de confiança per a altres organitzacions en referència als serveis que proporciona. La relació de confiança no només s'estableix amb els usuaris finals d'una xarxa telemàtica sinó també amb altres TTPs amb les qual té relació. No obstant això, aquest tipus de relació pot ésser diferent; és a dir, el grau de confiança dipositat en les TTPs pels usuaris finals pot variar, depenent de la forma en qual la TTP proporciona el servei de seguretat i de les característiques pròpies de cada servei. Per exemple, en protocols on la TTP dóna un servei de testimoniatge (notaria), a vegades, aquesta TTP actua com una autoritat de lliurament sense saber el contingut dels missatges i, en altres casos, la TTP té accés al contingut. Per consegüent, a l'últim cas, els usuaris han de

dipositar un nivell més alt de confiança que en el primer, perquè una mala conducta de la TTP en el protocol pot produir pitjors conseqüències que en el primer cas.

No obstant això, el nivell de confiança que els usuaris han de dipositar en les TTPs és difícil d'avaluar, perquè és complicat tenir una visió global dels serveis de confiança i de les diferents maneres de donar cobertura a aquests serveis, ja que depenen de molts de factors, entre els quals es troben les especificacions del protocol i de la política de seguretat de cada TTP.

El paper de la TTP en un protocol de seguretat també pot determinar el cost en comunicacions del protocol, perquè la TTP pot fer de coll d'ampolla, sobretot en les aplicacions a gran escala. A més, la interacció amb la TTP implica un increment en els costos de comunicacions, en particular quan la TTP està activament involucrada en cada execució del protocol. Per aquesta raó, un dels objectius del disseny de protocols eficients és reduir la intervenció de la TTP. Aquest és el cas dels anomenats protocols optimistes com els que es descriuen a [ASW97, FMH00, MFH00, S96].

En aquest capítol presentarem un mètode per classificar els serveis de confiança que ens permetrà clarificar les característiques de cada servei i donarà una idea del grau general de la participació de la TTP en l'intercanvi d'informació. Pensant en els usuaris, aquesta classificació els permetrà conèixer el nivell de confiança que han dipositar en una TTP si executen un determinat protocol de seguretat, perquè tendran un sistema per mesurar objectivament la confiança i la sobrecàrrega en les comunicacions que introdueix la TTP, en relació amb les funcions que realitza dins del protocol.

Podem trobar algunes llistes relativament simples de funcions que les TTPs duen a terme als documents [ISO13888-1, X.813] i també en podem trobar de més exhaustives en aquestes referències [ETS97, OP98, ZG96b]. En els documents [ETSI97, X.842] es categoritzen els serveis proporcionats per les TTPs emprant un esquema funcional des del punt de vista de l'usuari final. Analitzant els distints serveis proporcionats per les TTPs, trobam un conjunt reduït de criteris o punts de vista que ens permeten classificar i avaluar el paper d'una TTP en un protocol de seguretat. Així doncs, analitzarem com s'involucren les TTPs en els protocols de seguretat, segons els missatges intercanviats i el seu contingut entre els usuaris finals i les TTPs. Hem de dir que per aquest treball no hem fet cap consideració sobre criteris institucionals i legals, que poden canviar amb independència del protocol. És a dir, la nostra classificació està relacionada amb els intercanvis de dades definides en el protocol entre els usuaris i les TTPs, però no se relaciona amb l'administració de la TTP ni amb les lleis i regulacions nacionals i internacionals.

Pensam que el conjunt de criteris escollit per avaluar les TTPs ha de ser reduït. Hi ha documents que proposen sistemes d'avaluació segons un conjunt ampli de criteris (per exemple, [MW97] assenyala 30 criteris que serveixen per descriure un sistema de pagament); en aquests sistemes, la taula d'avaluació és difícil mesurar i, per als usuaris, és molt complex analitzar i comparar els distints serveis de confiança.

Hem reunit un conjunt de criteris o punts de vista, que resumeixen la forma d'actuar d'una tercera part dins del protocol, mitjançant els quals podem avaluar qualsevol TTP. Normalment, aquests diferents punts de vista apareixen aïllats en articles i documents per ressaltar alguna característica especial sobre la participació de la TTP en els protocols proposats. Aquí, anomenarem classe a qualsevol punt de vista sota el qual classificam l'actuació de la TTP. Això significa que el mateix servei pot ésser catalogat de distinta forma, depenent del punt de vista. Per aquesta raó, primer, proposam una sèrie de classes per tal de definir la naturalesa i els requeriments de seguretat de cada servei de confiança. Llavors, d'acord amb el punt de vista seleccionat, un servei de confiança serà classificat del tipus *a* o *b* dins d'una classe determinada. En funció de cada punt de vista, hem descrit les set classes de servei a la figura 4.1.

CLASSE 1	**punt de vista: confiança**
Tipus de servei	Característica del servei
a. servei verificable	L'usuari pot detectar i provar que la TTP no ha proporcionat el servei de forma correcta (això és, quan la TTP o bé s'equivoca o bé traeix la confiança que hi ha dipositat l'usuari).
b. servei no verificable	L'usuari no pot provar que la TTP ha proporcionat el servei de forma incorrecta.

CLASSE 2	**punt de vista: intervenció en el protocol**
Tipus de servei	Característica del servei
a. servei optimista	Les TTPs només s'involucren en el protocol en cas d'excepció.
b. servei arbitrat	Les TTPs es veuen involucrades en cada execució del protocol.

Figura 4.1. Tipus de serveis

CLASSE 3	**punt de vista: confidencialitat**
Tipus de servei	Característica del servei
a. servei operacional	La TTP no té accés a dades confidencials de l'usuari.
b. servei incondicional	La TTP té accés a dades confidencials de l'usuari.

CLASSE 4	**punt de vista: usuari del servei**
Tipus de servei	Característica del servei
b. servei de suport	Quan el servei s'utilitza per activitats internes o com a suport a altres serveis.
a. servei final	Quan el servei és visible i accessible per als usuaris.

CLASSE 5	**punt de vista: organització de la TTP**
Tipus de servei	característica del servei
a. servei col·legiat	Les TTPs prenen les decisions relatives al servei de forma col·legiada.
b. servei no col·legiat	Una TTP pren totes les decisions relatives al servei.

CLASSE 6	**punt de vista: equitat**
Tipus de servei	Característica del servei
a. servei transparent	Si la TTP traeix un usuari, l'usuari se n'adonarà[5].
b. servei opac	Si la TTP traeix un usuari, aleshores l'usuari podria no adonar-se'n.

CLASSE 7	**punt de vista: temporització**
Tipus de servei	Característica del servei
a. servei asíncron	No és necessari especificar una data límit per a l'acabament del protocol amb tots els requisits de seguretat garantits. Les comunicacions entre TTP i usuaris són independents de qualsevol paràmetre temporal.
b. servei síncron	Per assegurar les característiques de seguretat del protocol, la TTP ha de rebre o transmetre alguns ítems d'informació en un moment precís.

***Figura 4.1* (continuació).** Tipus de serveis

[5] El fet que l'usuari se n'adoni no significa que ho pugui demostrar. En canvi, si el servei és verificable (classe 1) podrà demostrar si la TTP ha actuat correctament o no.

D'aquesta manera, per exemple, des del punt de vista de l'usuari (classe 4), un *servei final* podria ésser un servei de missatgeria notaritzat i confidencial. Aquest *servei final* és visible per a l'usuari i pot servir de base per a un protocol de signatura electrònica de contractes [BGM90]. Per donar suport a aquest servei es requereixen altres serveis, tal com el servei de certificació de claus, serveis de confidencialitat i serveis de time-stamping [ETS97].

Els set punts de vista prèviament definits no són mútuament excloents, sinó que són complementaris. Quan seleccionam un punt de vista, estam seleccionant una classe i, aleshores, podrem classificar el servei com a tipus *a* o *b* d'aquesta classe. Canviant de punt de vista, observarem com una TTP encaixa en aquest model de classificació multidimensional. Per exemple, el servei de certificació de claus *Class 1 Digital ID* [VITS] pot ésser classificat com un *servei verificable* des del punt de vista de confiança. En segon lloc, podem considerar aquest mateix servei com a *optimista* des del punt de vista de la intervenció, si nosaltres estam emprant el protocol S/MIME [S/MIME]. A més, també podem dir que és *servei operacional* des del punt de vista de confidencialitat, perquè la TTP no coneix la clau privada de l'usuari (d'altra manera l'usuari hauria de dipositar una quantitat més gran de confiança en la CA ja que el servei seria considerat com a *incondicional*). També, quan estam emprant el protocol per aconseguir un certificat, llavors el servei de certificació de claus és un *servei final* des del punt de vista de l'usuari. Però si estam utilitzant aquest servei a S/MIME llavors és un *servei de suport*. A més, el servei de certificació de claus *Class 1 Digital ID* [VITS] és un *servei no col·legiat* des del punt de vista de l'organització de la TTP. Des del punt de vista de l'equitat classificarem el servei com a *opac* ja que la TTP pot trair l'usuari i aquest no adonar-se'n. Finalment, podem classificar el servei com a *asíncron* perquè ni la TTP ni els usuaris necessiten rebre els missatges dins d'un interval de temps determinat. Resumint, un mateix servei té diferents aspectes a tenir en compte, depenent dels objectius i de les necessitats. De totes formes, a la secció número cinc d'aquest capítol, veurem detalladament com podem analitzar un protocol amb la intenció de classificar el servei de la TTP d'acord amb aquests criteris.

Classificar els serveis de confiança entre aquestes classes o tipus ens ajudarà en l'especificació d'un determinat protocol si volem que les TTPs que hi puguin intervenir i els seus serveis tenguin unes determinades característiques. Però classificar els serveis de confiança també ens permet mesurar la quantitat de confiança que els usuaris han de dipositar en les TTPs. Naturalment, per exemple, un punt de vista serà més rellevant per a qüestions de seguretat mentre altres punts de vista ho seran per a qüestions relatives al rendiment. Així, si consideram aspectes de seguretat hem de fer més èmfasi en uns punts de vista que en altres. No obstant això, aconseguir un equilibri entre seguretat i rendiment és la millor forma de definir protocols pràctics.

Anem a veure quins són els criteris que estan relacionats amb la quantitat de confiança que els usuaris han de dipositar en la TTP i quins amb la sobrecàrrega en les comunicacions que introdueix la intervenció de la TTP en el protocol. Com ara veurem i justificarem seguidament, les classes de servei relacionades amb la confiança dipositada pels usuaris són: 1, 3, 5, 6 i 7. D'acord amb el nostre esquema, classificar un servei com a tipus *a*, implica dipositar menys quantitat de confiança que si el classificam de tipus *b*. A la figura 4.2 hi ha les taules que argumenten aquest fet.

CLASSE 1	**tipus *a*: servei verificable**
Comentari	Els usuaris poden demostrar, per exemple, davant d'un àrbitre independent, que la TTP no compleix el servei d'acord amb les especificacions del protocol.

CLASSE 3	**tipus *a*: servei operacional**
Comentari	La TTP no té cap dada confidencial; conseqüentment no pot revelar informació confidencial de l'usuari.

CLASSE 5	**tipus *a*: servei col·legiat**
Comentari	Un servei col·legiat és resistent a la mala conducta d'algunes TTPs que intervenen en el protocol. Així doncs, és possible que l'incompliment del servei per part d'algunes TTPs no afecti la seguretat del protocol.

CLASSE 6	**tipus *a*: servei transparent**
Comentari	Els usuaris han de dipositar menys confiança en una TTP perquè si la TTP traeix la confiança que hi ha dipositat, els usuaris se n'adonaran encara que no disposin de cap prova per demostrar-ho.

CLASSE 7	**tipus *a*: servei asíncron**
Comentari	Si el canal de comunicació entre TTP i els usuaris no està permanentment romput, la TTP podrà proporcionar el servei a l'usuari malgrat hi pugui haver problemes de comunicació temporals. A més, d'aquesta manera, evitam problemes com la negació temporal de servei i altres problemes relacionats amb la sincronització de rellotges.

Figura 4.2. Classes relacionades amb la confiança

Les classes de serveis que estan relacionades amb el nivell de sobrecàrrega en les comunicacions introduïda per la TTP són 2, 4 i 5. A la figura 4.3 hi ha les taules on argumentam quins són els tipus de servei que suggereixen poca sobrecàrrega en les comunicacions.

CLASSE 2	**tipus *a*: servei optimista**
Comentari	Si la TTP només està involucrada en el protocol ocasionalment, aleshores tenim una menor sobrecàrrega en les comunicacions que si hi està involucrada en cada execució del protocol.

CLASSE 4	**tipus *a*: servei de suport**
Comentari	El servei és *off-line*, així doncs, la TTP no és causa de cap comunicació afegida ja que la relació de confiança entre la TTP i els usuaris prové d'altres interaccions.

CLASSE 5	**tipus *b*: servei no col·legiat**
Comentari	La sobrecàrrega en les comunicacions serà més petita si només hi ha involucrada en el protocol una sola TTP enlloc d'un protocol arbitrat per múltiples TTPs.

Figura 4.3. Classes relacionades amb les comunicacions

4.3 Nivells de confiança

D'acord amb l'apartat anterior, tenim cinc classes de serveis que, de forma individual, permeten avaluar la confiança que s'ha de dipositar en el servei ofert. Podem pensar a utilitzar aquestes classes per mesurar d'una manera senzilla la quantitat de confiança que s'ha de dipositar en una TTP. Per això, hem d'avaluar el servei sota cada un dels criteris descrits a la figura 4.2. Així, en la mesura que avaluam cada criteri podem dir que aplicam una funció d'avaluació al servei proporcionat per la TTP; anomenem τ(TTP) aquesta funció.

Com a resultat d'aplicar la funció τ() obtenim un vector binari de cinc coordenades. El resultat de referència, és a dir, el resultat que representa el dipòsit més petit de confiança, és τ(TTP) = (*a*,*a*,*a*,*a*,*a*), d'acord amb allò que hem exposat a l'apartat anterior. Com més lluny estigui el resultat de τ(TTP) del vector (*a*,*a*,*a*,*a*,*a*), més gran podria ser la quantitat de confiança que els usuaris han de dipositar en la TTP. La quantitat de coordenades diferents que hi ha entre un i altre vectors marca la distància que hi ha entre τ(TTP) i el

resultat òptim. La valoració final de la quantitat de confiança que s'hagi de dipositar en la TTP dependrà de la ponderació que cada usuari faci de les coordenades.

Per exemplificar el que acabam d'exposar al paràgraf anterior, suposarem ara que **v** i **w** són dos vectors. Aleshores la distància entre **v** i **w**, que denotarem per $d(\mathbf{v},\mathbf{w})$, serà el número de posicions diferents que tenen. Així doncs, si la quantitat de coordenades és n = 5, la distància entre **v** = (*a*,*a*,*a*,*a*,*a*) i **w** = (*b*,*b*,*a*,*a*,*b*) és 3.

Si tenim en compte que el resultat de τ(TTP) és un vector binari de cinc coordenades, podem tenir tan sols 32 resultats diferents. Hem fixat el nivell mínim de confiança en τ(TTP) = (*a*,*a*,*a*,*a*,*a*). En conseqüència, proposam quantificar el nivell de confiança que els usuaris dipositen en una TTP com la distància entre el vector resultant d'avaluar τ(TTP) i el nivell mínim de confiança que hem establert anteriorment. En aquest cas, obtendrem només sis possibles resultats diferents que provenen d'avaluar la distància entre el vector òptim i qualsevol dels 32 possibles resultats de la funció τ(TTP). Hem expressat gràficament els sis possibles resultats a la figura 4.4.

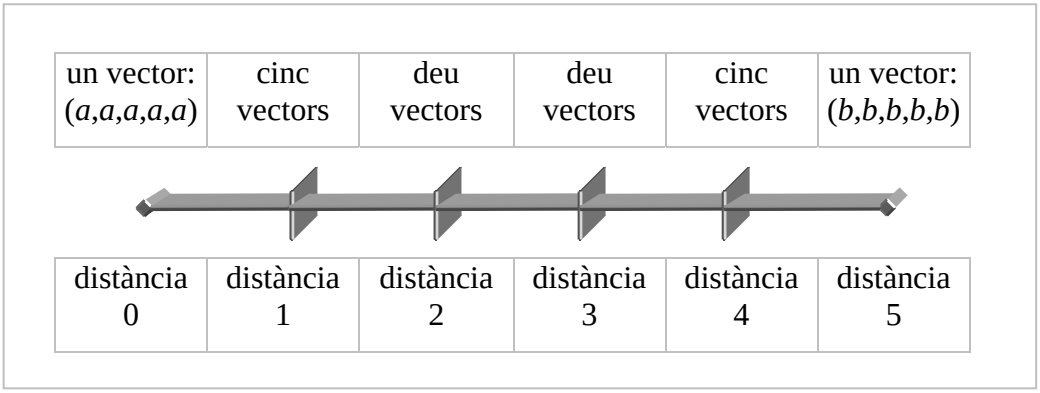

Figura 4.4. Nivells de confiança

Així, d'acord amb aquest mètode, tenim sis nivells de confiança diferents (de 0 a 5). Per exemple, si avaluam τ(TTP) = (*a*,*b*,*b*,*a*,*a*) per a un hipotètic servei de confiança, significarà que hem obtingut un dels deu vectors amb una distància igual a 2 respecte al vector de referència. En aquest cas, el nivell de confiança dipositat pels usuaris d'aquest servei en la TTP és 2. No obstant això, el resultat no ha de ser necessàriament millor o pitjor que el d'un vector a una distància superior. Això és així perquè deixam, de moment, la ponderació de cada coordenada a la consideració de cada usuari. Més endavant, en el capítol 10, comentarem aquest aspecte.

4.4 Nivells de sobrecàrrega en les comunicacions

Com ja hem esmentat abans, la participació de TTPs en un protocol per assegurar els requisits de seguretat sol comportar un augment del cost de les comunicacions; és a dir, s'augmenta el nombre d'intercanvis per poder garantir la seguretat mitjançant la intervenció de la TTP. Però, aquest augment depèn, entre altres coses, de com estigui involucrada la TTP en el protocol. Com s'ha explicat anteriorment, les classes de servei 2, 4 i 5 definides a la secció 4.2 qualifiquen aquesta sobrecàrrega en les comunicacions des de tres punts de vista diferents. Com en la secció anterior, podem veure l'avaluació d'aquestes tres classes com l'aplicació d'una funció; anomenem π(TTP) aquesta funció. Com a resultat, obtenim un vector binari de tres coordenades amb el valor *a* o *b* a cada una d'aquestes.

Segons les taules definides a la secció 4.2, el resultat de π(TTP) que expressa el nivell de sobrecàrrega en les comunicacions més petit és π(TTP) = (*a*,*a*,*b*). Òbviament, el primer valor és el resultat d'avaluar la classe 2; el segon nivell ve de la classe 4 i el tercer de la classe 5. Com en el cas de l'avaluació del nivell de confiança, per trobar la quantitat d'intercanvis introduïts per la intervenció de la TTP en un determinat protocol de seguretat, emprarem la diferència entre els valors de les coordenades del vector (obtingut aplicant π(TTP) per al cas concret) i el vector que representa el nivell de sobrecàrrega mínim. Així, si comparam els vuit possibles vectors amb el vector que representa el millor valor s'obté el diagrama de la figura 4.5.

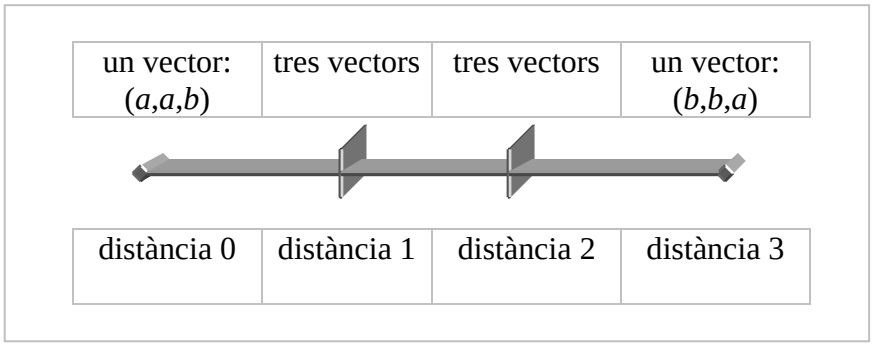

Figura 4.5. Nivells de sobrecàrrega en les comunicacions

Així doncs, d'acord amb la figura 4.4, tenim quatre nivells de sobrecàrrega diferents (de 0 a 3). Per exemple, si avaluam π(TTP) = (*b*,*b*,*b*), en un hipotètic servei de confiança, significarà que hem obtingut un dels tres valors la distància del qual amb el seu millor vector és 2. En aquest cas, el nivell de sobrecàrrega en les comunicacions introduït per la

TTP és 2. Com ja hem assenyalat en el cas de l'avaluació del nivell de confiança, aquest resultat no ha de ser necessàriament millor o pitjor que el d'un vector a distància superior (cada usuari pot ponderar de forma diferent les coordenades).

4.5 Exemple

Per il·lustrar el nostre mètode d'avaluació de la quantitat de confiança dipositada en una TTP i del nivell de sobrecàrrega en les comunicacions que aquesta introdueix en el protocol de seguretat, analitzarem un exemple de TTP en un protocol de seguretat: el paper d'una institució financera en l'esquema de diners electrònics irrastrejables definits per D. Chaum et al. a [CFN89].

En aquest capítol, utilitzarem per descriure el protocol de seguretat els diagrames d'esdeveniments. Aquest diagrames ens permetran definir el protocol, deixant prou clar quin és el paper que hi té la TTP que serà objecte de la nostra anàlisi. Els diagrames d'esdeveniments, escollits del camp de l'anàlisi orientada a objectes dels quals en podem trobar una bona referència a [RBP91], ens poden ajudar a descriure els protocols de seguretat per facilitar la valoració de les set classes de servei prèviament definides. Els diagrames d'esdeveniments són un mètode gràfic d'anàlisi basada en objectes i estan dissenyats per descriure les interaccions entre un joc d'objectes d'un sistema. Aquests diagrames mostren cada objecte com una línia vertical i cada esdeveniment com una fletxa horitzontal de l'objecte del remetent a l'objecte del receptor. Les fletxes estan etiquetades amb el contingut del missatge intercanviat. A més de la línia de l'objecte vertical, hi pot haver descripcions de les accions que l'objecte fa com a resposta a la recepció d'un missatge provinent de l'altre objecte. El temps avança de dalt a baix del diagrama, però l'espai és irrellevant.

En alguns casos, per fer la nostra classificació haurem de fer algunes hipòtesis perquè les característiques tècniques del protocol de l'exemple no estan especificades tan detalladament com seria necessari per a la seva implementació.

4.5.1 Rol d'una institució financera en un esquema de diners electrònics irrastrejables.

Considerarem el paper que representa un banc en el conegut esquema de monedes electròniques irrastrejables definit per D. Chaum et al. a l'article [CFN89]. En aquest cas, el banc administra els comptes dels clients i ajuda el client a generar les monedes electròniques. Abans de classificar el paper de l'entitat de confiança (el banc), descriurem el protocol per emetre i gastar aquest tipus de monedes. En el protocol l'usuari *A* treu una moneda del banc i després fa un pagament a l'usuari *B* amb aquesta moneda. Finalment

l'usuari *B* ingressa la moneda electrònica. A la figura 4.6 i 4.7 descrivim el protocol emprant els diagrames d'esdeveniments.

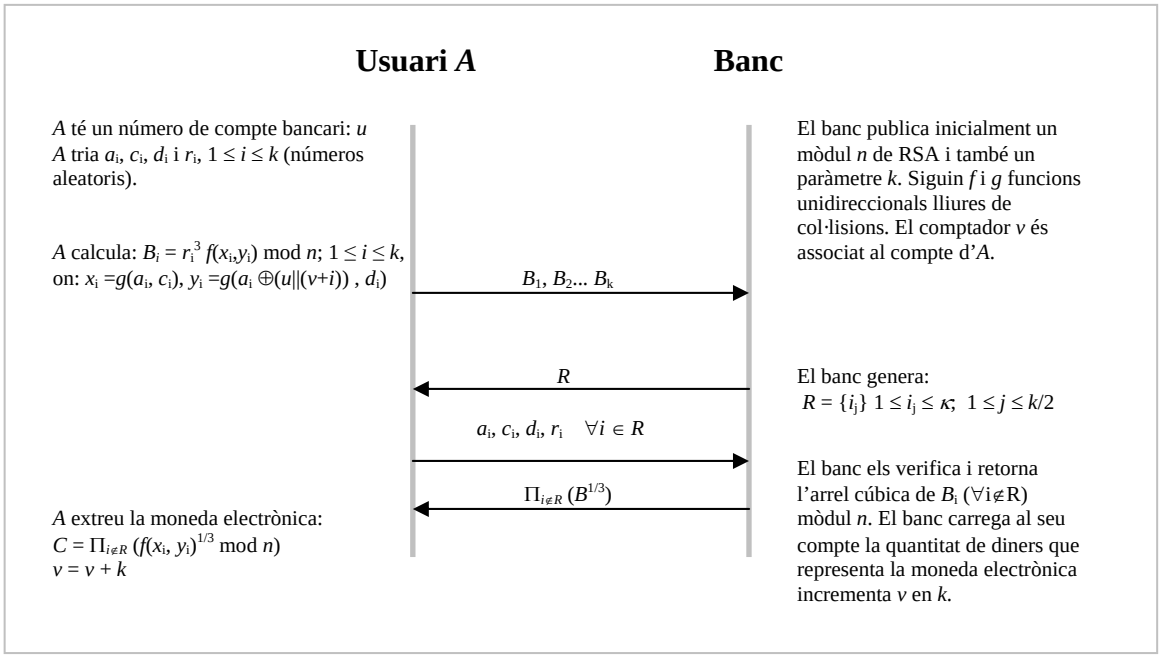

Figura 4.6. Reintegrament d'una moneda electrònica

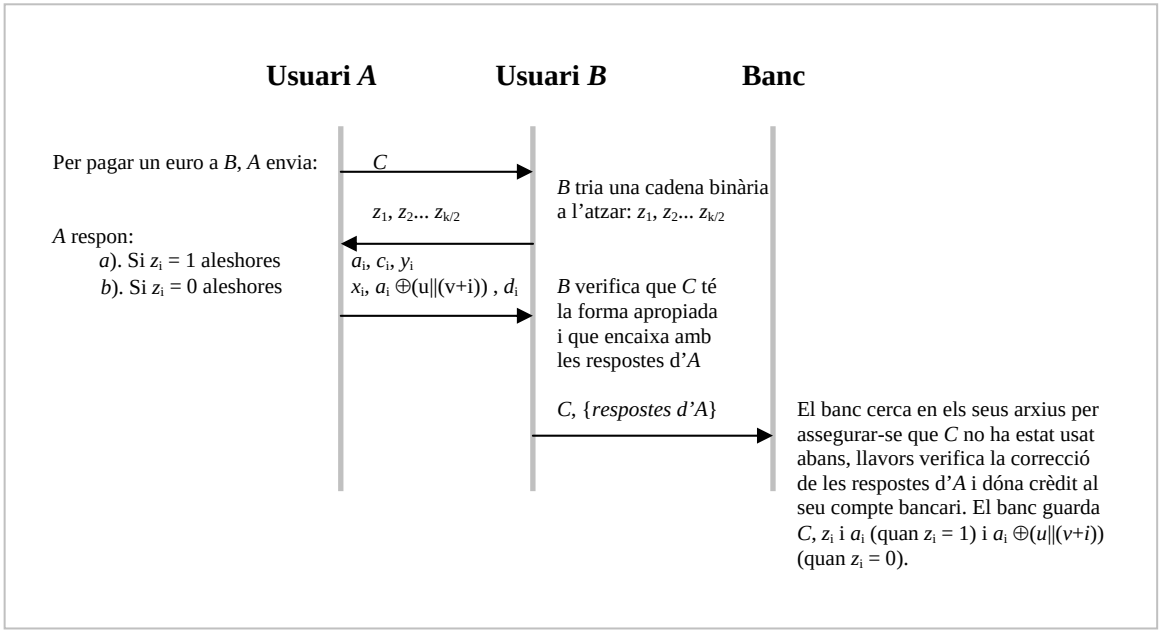

Figura 4.7. Pagament i dipòsit d'una moneda electrònica

El banc ha de ser de confiança per als usuaris perquè ha de donar el suport adequat en aquest protocol d'emetre i de gastar monedes electròniques. És a dir, en primer lloc, el banc ha de signar una moneda de format correcte que ha de ser carregada al compte de l'usuari; i en segon lloc, el banc ha de donar crèdit quan un usuari diposita una moneda correcta al banc. A la figura 4.8 hi ha les taules on podem veure els resultats de la classificació de l'actuació de la TTP dins d'aquest protocol.

CLASSE 1	**punt de vista: confiança**
Tipus de servei seleccionat	*b*. no verificable
Comentari	D'una banda, el comptador *v* està dins de la moneda i el banc ho ha signat; per consegüent, l'usuari que l'ha retirat pot comprovar si el banc ha retirat la quantitat correcta de diners del seu compte, i ha incrementat el seu comptador correctament. Si no fóra així, l'usuari no pot demostrar l'actuació incorrecta del banc, ja que el nivell de concreció del protocol expressat a [CFN89] no deixa obtenir proves sobre el valor del comptador anterior al reintegrament actual. Això significa que l'usuari no té evidències per demostrar a un àrbitre independent que el banc no ha fet correctament les operacions sobre el seu compte en el reintegrament d'una moneda. Ens trobam en la mateixa situació quan realitzam un dipòsit. L'apartat 5.3.3 amplia els arguments sobre la no verificabilitat de la TTP en aquest protocol.

CLASSE 2	**punt de vista: intervenció en el protocol**
Tipus de servei seleccionat	*b*. arbitrat
Comentari	El banc està directament involucrat en cada execució del protocol. En ambdós casos (quan es retiren els diners i quan es dipositen) els usuaris han de posar-se en contacte amb ell.

CLASSE 3	**punt de vista: confidencialitat**
Tipus de servei seleccionat	*a*. operacional
Comentari	El banc no té accés a dades confidencials quan s'està executant el protocol d'emissió o de despesa dels diners electrònics, perquè si l'usuari només gasta una vegada cada moneda, llavors els diners són irrastrejables.

Figura 4.8. Classificació de l'actuació de la TTP

CLASSE 4	**punt de vista: usuari del servei**
Tipus de servei seleccionat	*b*. final
Comentari	El banc dóna suport al servei d'una manera directa.

CLASSE 5	**punt de vista: organització de la TTP**
Tipus de servei seleccionat	*b*. no col·legiat
Comentari	Només un banc està involucrat en el protocol quan un usuari retira o diposita una moneda.

CLASSE 6	**punt de vista: equitat**
Tipus de servei seleccionat	*a*. transparent
Comentari	Els usuaris poden verificar els seus comptes després de retirar o dipositar una moneda electrònica, per verificar el bon funcionament del banc. També poden inspeccionar la signatura del banc sobre els diners electrònics.

CLASSE 7	**punt de vista: temporització**
Tipus de servei seleccionat	*a*. asíncron
Comentari	Els requisits de seguretat del servei de confiança són independents de qualsevol paràmetre temporal.

***Figura 4.8* (continuació).** Classificació de l'actuació de la TTP

Ara podem mesurar el nivell confiança i el nivell de sobrecàrrega en les comunicacions que el banc (B) introdueix a l'esquema de monedes electròniques irrastrejables que acabam de descriure. En relació amb la confiança, hem de considerar les classes de servei 1, 3, 5, 6 i 7. És dir, el vector resultant és $\tau(B) = (b,a,b,a,a)$. Aleshores, la distància entre el millor resultat possible ($t=(a,a,a,a,a)$) i $\tau(B)$ és $d(\tau(B),t) = 2$. Per tant, en referència en aquest model de classificació, el nivell de confiança dipositat pels usuaris d'aquestes monedes en el banc emissor és 2.

Per mesurar l'actuació (el nivell de sobrecàrrega en les comunicacions) del banc en el protocol, hem de considerar les classes 2, 4 i 5. El vector binari resultant és $\pi(B) = (b,b,b)$.

Així, la distància entre el millor resultat possible (t=(a,a,b)) i el resultat de π(B) és $d(\pi(B),t) = 2$. Consegüentment, el nivell de sobrecàrrega introduïda pel banc en el protocol és 2.

4.6 Conclusions

En el disseny de nous protocols de seguretat, idealment, seria interessant aconseguir que tots els requeriments de seguretat d'una part estassin garantits sense que hagués de tenir la necessitat de confiar en altres parts. És a dir, només hauria de fer falta que una part confiàs en ella mateixa i, com és natural, en la jurisdicció en cas de problemes en la transacció electrònica duta a terme. No obstant això, per garantir els requeriments de seguretat, inevitablement, en alguns protocols de seguretat algun grau de confiança s'ha de dipositar en terceres parts. Algunes d'aquestes TTPs poden ésser agències de certificació estatals, comitès de control tècnics o organitzacions de consumidors. Per tot això que acabam d'explicar, podem trobar en molts documents referències a la intenció de reduir la quantitat de confiança que una part ha de dipositar en una TTP [BBC94, ETS97, N97, OP98, SET97].

Aquí hem proposat unes classes de serveis per categoritzar des de distints punts de vista les operacions fetes per TTPs quan duen terme la seva funció en un protocol de seguretat. Com a conseqüència, podem conèixer la naturalesa dels serveis i podem tenir una referència sobre el grau de confiança que un usuari ha de dipositar en les TTPs en funció de la distància entre el vector obtingut i el vector que representa el millor resultat que es pot obtenir. Així, aconseguim avaluar la quantitat de confiança posada en una TTP i mesurar la sobrecàrrega en les comunicacions que aquesta introdueix en el protocol.

En l'esquema de classificació que hem presentat, hem fet un esforç de concentració i simplificació dels distints criteris de classificació, amb la pretensió de facilitar la ponderació de cada un d'aquests criteris als usuaris perquè una de les crítiques que reben normalment aquests mètodes de classificació és la complexitat que comporta als usuaris l'anàlisi i comparació dels resultats obtinguts. Més endavant, en el capítol 10 sota el títol de conclusions, proposam com a línia d'investigació futura la recerca d'un sistema que sigui capaç d'unir els distints tipus de servei i ponderar-los en funció de les preferències de cada usuari.

L'anàlisi i la classificació dels serveis de seguretat proporcionats per les TTPs ens han permès conèixer millor la naturalesa dels serveis de seguretat. A l'inici d'aquest apartat fèiem referència a la intenció de reduir la quantitat de confiança que els usuaris han de dipositar en les TTPs; després de la proposta que fem en aquest capítol ens va quedar clar que la classe 1 de servei (*verificable*/*no verificable*) influeix d'una forma més directa i

efectiva que les altres classes sobre la quantitat de confiança que els usuaris han de dipositar en la TTP. Hem de tenir en compte que, per exemple, la classe 1 de servei és més restrictiva que la classe 6 (*transparent*/*opac*) i més efectiva que la classe 5 (*col·legiat*/*no col·legiat*) ja que no hi ha la necessitat d'incloure en el protocol múltiples TTPs. A més, tal i com l'hem desenvolupada en els capítols posteriors, la classe 1 també comporta restriccions sobre la temporalització (servei *asíncron*/*síncron* de la classe 7).

Així doncs, el camí que seguirem en els capítols següents és l'especificació de protocols de seguretat pensant en les característiques que convendria que tengués el servei que hi proporciona la TTP. D'aquesta manera, si ens preocupa la dificultat que puguin tenir els usuaris quan dipositen la confiança en entitats remotes com les TTPs, podem pensar com definir protocols que tenguin com a característica la verificabilitat del servei de la tercera part. Es tracta, per tant, de desenvolupar i investigar la forma d'introduir aquesta característica com una propietat de seguretat més en els protocols i saber, també, les conseqüències que d'això es poden derivar (tant pel que fa a la solució de problemes de seguretat originats per l'actuació d'una TTP corrupta, com les implicacions que pot tenir la inclusió de la verificabilitat de la TTP en el disseny del protocol).

Capítol 5

La propietat de verificabilitat

5.1 Introducció

Hi ha nombroses referències que tracten sobre protocols de seguretat amb TTPs. B. Crispo et al. a l'article [CEF03] afirmen que el fet que una tercera part no respongui als seus errors o faltes es qualifica d'important debilitat del protocol en qüestió. Aquesta debilitat significa que si la TTP falla i no compleix amb la feina que li encomana el protocol, l'usuari del servei no té forma de demostrar que la tercera part ha fallat. Aquest fet és una limitació pràctica crucial ja que, per aquest motiu, els protocols de seguretat amb involucració de terceres parts han de suposar que l'usuari tengui una confiança il·limitada en les accions de la TTP i que aquesta no fallarà mai. En canvi, a la pràctica, hem de recordar que, fins i tot amb una tercera part plenament de confiança que no fallàs mai, l'usuari podria ser víctima d'un atac de negació de servei (*denial of service attack – DoS*) que podria malmetre la seguretat de qualsevol intercanvi.

És relativament freqüent trobar protocols de seguretat on la mediació de la tercera part resulta mancada de responsabilitat, en el sentit que, si aquesta entitat no actua correctament i en conseqüència romp la seguretat d'una transacció, aleshores el protocol no proporciona evidències de l'error en l'operació als usuaris ni permet restablir la seguretat de l'intercanvi. D'aquesta manera la mala actuació de la TTP queda impune i això comporta que els usuaris d'aquests protocols hagin de dipositar una confiança il·limitada en les TTPs. Com es pot disminuir el grau de confiança que els usuaris han de dipositar en una tercera part és una qüestió que encara resta oberta, com expliquen B. Crispo et al. a [CEF03]. Aquest inconvenient decisiu podria prevenir, en certa mesura, un desplegament i un ús més ampli d'aquestes nous procediments electrònics especificats en forma de protocol de seguretat. El problema ha estat reconegut per diversos autors [ASW98, ETS97, ETSI97, FPH00, GJM99, SM02, X.842] i, com hem vist en el segon capítol d'aquesta tesi, ha estat estudiat i s'han fet propostes que van des de la no inclusió

de TTPs en els protocols fins a incloure múltiples TTPs amb els inconvenients que ja hem esmentat en el capítol 2. A l'apartat 5.3 d'aquest capítol farem un repàs ampli de distints tipus de protocols que compten amb la intervenció de TTPs i veurem com, en algunes operacions, la TTP pot actuar de forma incorrecta (intencionadament o no) rompent així la seguretat del protocol i com, en aquesta situació, l'usuari afectat no disposarà de cap evidència que li permeti corregir la situació.

En aquesta tesi hem argumentat les motivacions que poden justificar la necessitat d'introduir la propietat de verificabilitat dins els protocols de seguretat amb terceres parts de confiança. En documents com [ETSI97, IPI, X.509, X.842] també podem trobar arguments en el sentit que esmentàvem abans, ja que es parla de la necessitat desenvolupar eines que ajudin a disminuir el grau de confiança que els usuaris han de dipositar en una TTP. Podem resumir aquests arguments en els següents tres apartats:

- Rebaixar el grau de confiança que s'ha de dipositar en una TTP facilita que possibles usuaris reticents utilitzin els nous procediments telemàtics, ja que la manca de tradició en l'ús d'aquests nous procediments i de les noves TTPs associades a ells indueixi a aquestes reticències.
- Des d'un punt de vista conceptual podem dir que si l'entitat *A* pot perfectament predir cada acció de l'entitat *B*, indica que *A* no necessita confiar més en *B*. *A* posseeix coneixement complet de *B* (confiança és reemplaçada per coneixement) [CC03]. Això significa que la confiança (en contraposició amb el coneixement) dóna un marge d'incertesa sobre les accions d'una determinada entitat (com podria ser una TTP) que és convenient rebaixar.
- Moltes vegades els participants en una comunicació electrònica prefereixen tenir evidència del que succeeix en l'altre extrem de la xarxa, ja que pel fet que la interacció és remota, la comunicació és entre entitats remotes (potser a vegades difícilment localitzables) i la infrastructura de comunicació no és sempre fiable.

Per tot això, nosaltres pensam que trobarem millors solucions al problema que tractam sobre el dipòsit de confiança en les TTPs a través de la introducció de noves característiques o propietats de l'actuació de les terceres parts, en lloc d'eliminar o afegir terceres parts en els protocols de seguretat. B. Crispo et al. a [CR96] demostren que la confiança que cal dipositar en una TTP pot ésser reduïda a una confiança funcional o operacional en lloc d'incondicional, cosa que concorda amb la característica o punt de vista número tres que descrivim en el capítol 4, on analitzam i descrivim l'actuació d'una TTP en funció d'un conjunt de característiques. Aquest punt de vista ha estat expressat en el capítol 4 tal com ara recordam a la figura 5.1.

CLASSE 3	punt de vista: confidencialitat
Tipus de servei	característica del servei
a. servei operacional	La TTP no té accés a dades confidencials de l'usuari.
b. servei incondicional	La TTP té accés a dades confidencials de l'usuari.

Figura 5.1. Tipus de servei classe 3

Això significa que, en funció de les característiques de la intervenció de la TTP en un protocol, serà necessari dipositar més o menys confiança en aquesta. Per exemple, com demostra B. Crispo et al. a [CR96], si aconseguim definir protocols on el servei de la tercera part és operacional, aleshores significarà que la TTP no tendrà mai accés a dades confidencials de l'usuari i, en conseqüència, una mala actuació de la TTP no podrà mai desvetllar dades crítiques per a l'usuari. Des d'aquest punt de vista aconseguim rebaixar la necessitat de dipositar confiança en les terceres parts i direm que la confiança que tenim en la TTP és només funcional i no incondicional. Així doncs, si tenguéssim la forma d'arribar sempre a aquest objectiu[6], aleshores aconseguirem definir protocols on hauríem reduït el grau de confiança que els usuaris dipositarien en les TTPs, sense la necessitat d'haver d'eliminar les terceres parts del protocol o d'haver d'involucrar-ne una multitud, amb els problemes que això comporta.

La inclusió d'aquesta propietat en la definició de protocols pot ajudar a aconseguir que alguns procediments electrònics s'implantin més fàcilment. No obstant això, pensam que un servei operacional proporciona una petita reducció del grau de confiança que els usuaris han de dipositar en les TTPs ja que no només continuam sense poder responsabilitzar la tercera part de les seves possibles errades (intencionades o no), sinó que ni tan sols podem assegurar que qualsevol mal funcionament de la TTP serà detectat per l'usuari. Una passa definitiva en aquest sentit seria aconseguir que les accions de les terceres parts en un determinat protocol fossin verificables. Dit d'una altra manera, si el servei que ofereix la tercera part és verificable, aleshores significarà que respon a la classe *a* del criteri número 1 de classificació per als serveis de terceres parts de confiança que hem presentat a l'anterior capítol tal com podem veure a la figura 5.2.

[6] Hi ha tècniques que en situacions molt concretes es poden utilitzar per aconseguir aquesta fita. És el cas de les signatures cegues introduïdes per D. Chaum i aplicades, per exemple, a un esquema de diners electrònics a [CFN89] per amagar certa informació a la TTP (en aquest cas un banc) i, d'aquesta manera, quan es diposita una moneda electrònica, la tercera part no té informació del camí que ha seguit la moneda per arribar a aquest punt.

CLASSE 1	punt de vista: confiança
Tipus de servei	característica del servei
a. servei verificable	L'usuari pot detectar i provar que la TTP no ha proporcionat el servei de forma correcta (això és, quan la TTP o bé s'equivoca o bé traeix la confiança que hi ha dipositat l'usuari).
b. servei no verificable	L'usuari no pot provar que la TTP ha proporcionat el servei de forma incorrecta.

Figura 5.2. Tipus de servei classe 1

La propietat de verificabilitat fou introduïda inicialment per N. Asokan et al. a [ASW98] i posteriorment ha estat reformulada per J.L. Ferrer et al. a [FPH00] com a:

- *Verificabilitat de la tercera part*: Si la tercera part no actua correctament, aleshores es perd la seguretat de l'intercanvi però la víctima pot provar aquest fet davant d'un àrbitre imparcial.

L'especificació d'aquesta propietat concorda amb la nostra definició de servei verificable. És prou evident que la introducció d'aquesta propietat dins dels protocols pot ajudar a resoldre el problema que hem plantejat a l'inici d'aquest capítol (suposant que és inevitable que una TTP pugui cometre errades, encara que sigui de forma molt ocasional). Es tracta, per tant, d'aconseguir fórmules per introduir la propietat en els protocols sense que això provoqui altres problemes de seguretat o ineficiències (per exemple, sobrecàrrega en les comunicacions) en el protocol.

5.2 Entorn de verificabilitat. Definicions

En els capítols següents d'aquesta tesi desenvolupam la idea exposada a l'anterior paràgraf. Veurem com hem estudiat distints protocols de seguretat tot analitzant si la tercera part involucrada en aquests és verificable o no. Per això, aquí, hem volgut resumir en aquesta secció els conceptes que hem emprat i que hem definit entorn d'aquesta propietat.

Com és natural, hem pogut detallar més les característiques de la propietat de verificabilitat a mesura que hem anat introduint la propietat a distints tipus de protocols de seguretat. Així doncs, l'experiència ha estat un element cabdal per poder desenvolupar i aplicar amb cura la propietat de verificabilitat d'una tercera part involucrada en un

intercanvi segur. Aquí presentam els conceptes tal i com els hem concebuts després de realitzar tot el procés d'anàlisi dels serveis de seguretat que les terceres parts proporcionen als usuaris.

Per realitzar aquestes definicions hem partit de la nomenclatura i els conceptes descrits en el model de seguretat abstracte per a la transferència de missatges [X.400]. D'aquesta manera aconseguirem una formulació dels conceptes més apropada als estàndards internacionals i un reconeixement més immediat i clar de les diferents definicions, ja que el model de seguretat proporciona un marc per a la descripció dels serveis de seguretat entesos com una eina que serveix per contrarestar els riscos potencials.

Tal i com estableix la sèrie de recomanacions internacionals X.400, els *serveis de seguretat* es faciliten mitjançant l'ús dels anomenats *elements de servei*, entenent per element de servei una *unitat funcional* que segmenta i descriu les característiques del tractament dels missatges intercanviats. Això significa que el problema de la no verificabilitat de la TTP que hem plantejat aquí el podem expressar, emprant aquesta terminologia, de la següent forma:

- Problema de la verificabilitat de la TTP: si la TTP, que proporciona un servei de seguretat a un usuari, falla (és a dir, la TTP no executa correctament algun element de servei), aleshores l'usuari no té forma de demostrar que la TTP ha proporcionat el servei de forma incorrecta i ha romput, amb tota probabilitat, la seguretat de l'intercanvi.

Així doncs, seguint la nomenclatura de les recomanacions internacionals, entenem la propietat de verificabilitat com una *capacitat de seguretat* ja que l'utilitzarem com a mecanisme per protegir els usuaris contra amenaces de seguretat, en aquest cas, contra l'actuació incorrecta d'una tercera part. En aquest punt, doncs, introduirem les definicions que hem fet al voltant de la propietat de verificabilitat i que seran necessaris per dissenyar protocols de seguretat amb terceres parts verificables:

- *Activitat de Seguretat*: una TTP ha de proporcionar un servei a un usuari en resposta a una petició seva. Una activitat de seguretat és un element de servei, això és, una unitat funcional que segmenta i descriu les característiques del servei de seguretat proporcionat per la TTP.
- *Activitat de Seguretat Verificable*: una activitat de seguretat és verificable si l'usuari, que ha enviat una petició a una TTP, rep una evidència de no rebuig de les operacions que ha fet la TTP per dur a terme aquesta activitat de seguretat.
- *Servei de Seguretat Verificable*: si totes les activitats de seguretat emprades per proporcionar un servei són verificables, aleshores el servei és verificable.

- *Verificabilitat On-line*: la verificabilitat d'un servei de seguretat és *on-line* si un cop examinades les evidències que han estat rebudes per l'usuari del servei, aleshores l'usuari pot immediatament saber si la TTP ha operat correctament o no. En cas de problemes, l'usuari pot acudir a un àrbitre imparcial per corregir la situació.
- *Verificabilitat Off-line*: la verificabilitat d'un servei de seguretat és *off-line* si un cop examinades les evidències que han estat rebudes per l'usuari del servei, aleshores no té informació suficient per saber si la TTP ha proporcionat el servei de forma correcta. Però si sorgeix una disputa entre les parts involucrades en el protocol, llavors les evidències rebudes podran utilitzar-se (comparades amb les rebudes per l'altra part) per demostrar si la TTP ha actuat correctament o no.
- *Tercera Part Verificable*: una TTP és verificable si els serveis de seguretat que proporciona són verificables i la verificabilitat d'aquests serveis és *on-line*.

Com ja hem esmentat abans, el concepte primari de verificabilitat fou presentat inicialment a [ASW98]; no obstant això, aquí no tan sols hem reformulat i desenvolupat el concepte, sinó que, per primera vegada, hem distingit entre dues formes de verificabilitat que determinaran la immediatesa, la forma i la conducta de l'usuari a l'hora de conèixer o confirmar si el servei de seguretat ha estat proporcionat correctament o no i, en cas d'incorrecció, poder demostrar aquest extrem. La verificabilitat *off-line* només ens permetrà saber si la TTP ha actuat correctament en cas que, per exemple, ocorri una disputa entre les dues parts directament involucrades en l'intercanvi i, com a conseqüència d'això, es comparin les evidències emeses per la TTP a un i altre usuari. Aleshores, si la TTP no ha actuat correctament es podrà detectar un mínim de dos missatges contradictoris signats per la TTP, que és la prova que típicament es té en compte per donar fe del mal funcionament d'aquesta entitat, com exposen N. Asokan et al. a [ASW98]. En canvi, la verificabilitat *on-line* permetrà saber a cada part implicada de l'intercanvi si la TTP ha seguit correctament el protocol o no, sense la necessitat d'haver de comparar els missatges que ha rebut amb la resta de missatges de l'intercanvi. Aquesta distinció és molt important, perquè la verificabilitat *off-line* no assegura a l'usuari la detecció (en el moment més adequat possible) d'una mala actuació de la TTP ja que, després de concloure el protocol, és probable que les parts no tenguin ocasió de comparar els missatges que han rebut amb els corresponents de l'altra part o, com a mínim, abans que la part que obté un cert avantatge de l'errada de la TTP no se n'aprofiti.

Així doncs, l'exigència a un protocol de complir amb una forma de verificabilitat o amb una altra tendrà conseqüències en el seu disseny i, com és natural, la verificabilitat *on-line* serà més exigent que la *off-line*. Hem de remarcar que els mecanismes de no rebuig no són un requeriment primari de la propietat de verificabilitat, però sí que seran una eina molt útil per resoldre les subsegüents disputes que puguin ocórrer un cop finalitzat el protocol,

com indica la recomanació [X.813]. En els següents capítols introduirem la propietat de verificabilitat en distints protocols de seguretat; cosa que ens permetrà demostrar que efectivament podem definir d'una forma sistemàtica protocols de seguretat amb terceres parts verificables resolent d'aquesta manera el problema que plantejàvem a l'inici d'aquest capítol.

5.3 Terceres parts no verificables dins la bibliografia

En el capítol 2 d'aquesta tesi hem fet una revisió de les característiques que pot tenir la intervenció d'una tercera part de confiança en els protocols de seguretat i, en especial, hem fet menció d'aquells aspectes que, segons recomanacions internacionals com la [X.842], poden ser la base de la confiança que els usuaris han de dipositar en aquestes entitats. A l'apartat 2.4.3 del capítol 2 posam un exemple d'allò que podria passar si els usuaris d'un determinat protocol es troben amb una TTP corrupta.

Ara volem fer un repàs de les situacions en les quals es podrien trobar els usuaris de coneguts protocols de seguretat que compten amb la intervenció de terceres parts no verificables. En aquesta situació, determinades accions de les TTPs rompen la seguretat de l'intercanvi d'informació i els usuaris afectats no poden demostrar davant d'un tercer (per exemple, un jutge) la mala conducta d'aquestes entitats. Fins i tot, en ocasions, els usuaris ni tan sols s'adonaran que han estat víctimes d'un frau.

Les terceres parts que intervenen en aquests protocols no són verificables ja que aquesta propietat no ha estat gaire estudiada fins ara, probablement pel fet de ser una propietat que en podríem dir transversal, és a dir, és una propietat que afecta la seguretat de tot tipus de protocols on intervenen TTPs però no és la propietat de seguretat central de cap d'aquests. Podem exemplificar aquest fet fàcilment: en els protocols d'autenticació, el compliment o no de la propietat de verificabilitat de la TTP pot tenir conseqüències molt importants en la seguretat del sistema (com veurem en el següent apartat) però la propietat de seguretat que podríem anomenar central o la que capta la principal atenció del protocol és, lògicament, l'autenticació dels usuaris.

Tot seguit farem aquest repàs a diferents protocols de seguretat on les TTPs no són verificables i descobrirem les conseqüències que podria tenir això sobre la seguretat del sistema. Hem escollit protocols de seguretat amb moltes referències en el seu àmbit i els hem dividit en tres apartats diferents segons la finalitat de cada un d'ells. En els dos primers apartats hem escollit alguns exemples significatius de protocols d'autenticació i d'intercanvi equitatiu de valors. Aquests dos tipus de protocols ja fa temps que s'estan estudiant i normalment inclouen en les seves solucions terceres parts de confiança; a més, és aquí on ha aparegut per primera vegada la referència a l'actuació correcta de la TTP

com a una propietat de seguretat més. Per completar aquesta revisió, en el tercer apartat hem fet un breu repàs a altres tipus de protocols de seguretat on també comprovarem que si la TTP que intervé en el protocol no és verificable, aleshores les conseqüències per a l'usuari són tan negatives com en els protocols estudiats en els dos apartats anteriors.

5.3.1 Protocols d'autenticació

És en els protocols d'autenticació on més aviat varen aparèixer terceres parts de confiança. En aquest apartat descriurem breument alguns problemes que podrien tenir els usuaris de coneguts sistemes d'autenticació com a conseqüència d'errades (intencionades o no) de la tercera part no verificable que opera en el protocol. Primerament veurem el cas de la tercera part anomenada *Authentication Server* que opera en el protocol descrit a [NS78] i que és la base del servei d'autenticació de Kerberos [KNT94]. Després revisarem el cas de l'autoritat de certificació (*CA* per *Certification Authority*) que opera en els protocols d'autenticació descrits a la recomanació [X.509].

En un article seminal de Needham i Schroeder [NS78] es descriuen uns servidors d'autenticació (anomenats *AS* per *Authentication Server*) que no són res més que terceres parts les quals, en el primer protocol que es presenta a l'article de Needham i Schroeder, comparteixen una clau d'un criptosistema simètric amb cada un dels usuaris. Quan un usuari (anomenat *A*) vol mantenir una comunicació autèntica amb un altre usuari (anomenat *B*) s'ha de connectar a l'*AS* i aquest genera una nova clau perquè els dos usuaris puguin mantenir una comunicació confidencial i autèntica. La nova clau és enviada als dos usuaris xifrada amb les claus secretes que cada un d'ells comparteix amb el servidor. Aquest servidor és de confiança per a les parts, però podria fer un atac de suplantació de personalitat i fer-se passar per un determinat usuari davant d'un altre. Mirant la proposta feta a [NS78], és bastant clar que l'*AS* podria generar missatges suplantant la personalitat de l'usuari *A* i, si aquest s'adonàs del frau i entràs en disputa amb la tercera part, seria pràcticament impossible per a un jutge determinar si ha estat *A* o *AS* qui ha generat el missatge. El servei d'autenticació Kerberos [KNT94] està basat en aquest protocol i, per tant, està sotmès a aquest tipus d'atac on el servidor de confiança és capaç de violar la política de seguretat declarada, sense que els usuaris ho puguin provar davant d'un àrbitre independent.

Un altre enfocament dins dels protocols d'autenticació consisteix en el fet que cada client tria un parell de claus (una de pública i una altra de privada) i una autoritat de certificació certifica les claus públiques. Molts d'aquests esquemes permeten que la tercera part (la *CA* en aquest cas) pugui cometre atacs de suplantació de personalitat com els esmentats a l'anterior paràgraf i es fa molt difícil que el client pugui provar allò que realment ha passat. Per exemple, en els protocols d'autenticació presentats a [X.509], quan l'usuari *A* vol mantenir una comunicació autèntica amb l'usuari *B*, li envia el següent missatge: (C_A,

$D_A(M)$), on C_A és el certificat de la clau pública de l'usuari *A* generat per l'autoritat de certificació *CA* i $D_A(M)$ és el xifratge amb la clau privada d'*A* del missatge *M* (essent $M = (T_A, R_A, I_B,$ *dades*) on T_A és un *timestamp*, R_A és un nombre aleatori i I_B és la identitat de l'usuari receptor *B*). Llavors *B* ha de verificar el certificat C_A per obtenir la clau pública E_A del seu interlocutor. La intervenció de la tercera part certificant la clau pública d'*A* és fonamental per mantenir l'autenticitat de l'intercanvi. Ara bé, si la *CA* traeix la confiança que els usuaris han dipositat en ella, aleshores podria falsificar un certificat de clau pública de qualsevol usuari i realitzar un atac fent-se passar per una altra entitat. És a dir, la *CA* es podria fer passar per l'usuari *A* en una comunicació suposadament autèntica amb l'usuari *B*. Aquest atac podria fàcilment tenir més èxit si *B* no s'hagués comunicat mai amb *A* i no sabés la seva clau pública (no tendria cap certificat de clau pública d'*A*). Aleshores la *CA* pot crear un nou certificat on diu que *A* té una clau diferent i utilitzar-la juntament amb la corresponent clau privada per signar missatges que aparentment provenguin d'*A*. Alternativament si *B* vol comunicar-se confidencialment amb *A*, la *CA* podria emprar el nou certificat per convèncer *B* per xifrar els missatges amb la clau fraudulenta; després la *CA* pot realitzar el desxifratge usant la corresponent clau privada. D'aquesta manera, la *CA* pot rompre la seguretat del protocol sense que ningú tengui evidències que demostrin aquest fet.

Després d'aquest atac podria ser que les parts afectades no s'adonassin del frau i, en cas d'adonar-se'n, tendrien problemes per demostrar que l'actuació de la *CA* no ha estat correcta. Un aspecte important que podria influir sobre l'èxit o la detecció de l'anterior atac és la revocació de certificats, que tot esquema de certificació rigorós ha de tenir en compte. Imaginem una disputa on el demandant (*A*) diu que l'acusat (*CA*) ha falsificat un nou certificat de clau pública i l'ha utilitzat per fer-se passar per *A* en una determinada transacció electrònica. Suposem que *A* té, fins i tot, el parell de certificats que entren en conflicte (un de la clau correcta i l'altre de la clau fraudulenta), aleshores la *CA* podria replicar dient que efectivament ha generat aquests certificats però que ho ha fet a petició d'*A*, dient que: "*A* em va dir que havia perdut la seu clau privada i jo (la *CA*) vaig actualitzar la corresponent llista de certificats revocats i després em va sol·licitar un nou certificat de clau pública". Com un jutge podria resoldre aquesta disputa? En els procediments convencionals de resolució de disputes podríem esperar trobar algun paper que oficialment ens pogués donar una pista d'allò que ha passat en realitat. El que volem cercar nosaltres és alguna cosa anàloga a això, però traslladada al "món electrònic". Per exemple, el cas es podria resoldre si el protocol per obtenir un certificat de clau pública obligàs els usuaris a lliurar a la *CA* alguna petició de certificació que tengués la propietat de no rebuig d'origen. Llavors, per provar que la *CA* no ha falsificat un certificat, aquesta entitat hauria de mostrar aquesta petició; en cas contrari, significaria que l'autoritat de certificació ha generat un certificat de clau pública d'un usuari sense el consentiment d'aquest i, per tant, estaria cometent un frau.

5.3.2 Protocols de no rebuig i intercanvi equitatiu de valors

Durant els darrers anys, Internet s'ha desenvolupat enormement. Com a conseqüència d'això han sorgit i s'han estudiat nous problemes de seguretat, com el no rebuig i l'intercanvi equitatiu. S'han proposat diferents solucions parcials a aquests problemes que genèricament podem dividir en dues classes, d'acord amb la utilització o no de terceres parts de confiança (vegeu el capítol 2 d'aquesta tesi o documents com [CLM00]). A l'any 1980 Even i Yakobi a [EY80] varen demostrar que no hi havia cap protocol determinista que solucionàs el problema d'un intercanvi equitatiu sense TTP. Així doncs, els protocols de no rebuig i intercanvi equitatiu compten freqüentment amb la participació de terceres de parts de confiança que ajuden a resoldre problemes de seguretat.

Els protocols que revisarem en aquest apartat remarcaran que una debilitat important en moltes de les solucions proposades és que la TTP, que hauria de garantir l'equitat de l'intercanvi, pot vulnerar (intencionadament o no) la seguretat del sistema sense que se li pugui imputar aquesta errada. Com destaca B. Crispo et al. a [CEF03] aquesta és una limitació pràctica molt gran, com també és poc realista assumir que l'usuari té il·limitada confiança en la TTP i que aquesta mai falla. El tipus de solucions que nosaltres voldríem aconseguir són aquelles que compleixen amb allò que G. Ateniese et al. a [AMG01] anomenen un *Realistic Trust Model*; és a dir, un model de confiança que estigui basat en suposicions més realistes i sobre el qual l'usuari es pugui sentir confortable, tenint en compte que un sistema que necessita dipositar menys confiança en terceres parts serà probablement més acceptat.

Tot i que els protocols de no rebuig i intercanvi equitatiu de valors són uns dels camps on més s'ha estudiat la responsabilitat de les TTPs en els protocols, en aquesta secció repassarem algunes de les principals solucions aportades i veurem que, en aquestes solucions, no sempre s'ha tengut en compte allò que en el paràgraf anterior hem anomenat *Realistic Trust Model*. Els primers protocols que observarem seran els presentats per N. Asokan et al. a [ASW97, ASW98] que introduïren la noció de protocol optimista. Després veurem que els protocols presentats per J. Zhou et al. a [ZDB99] i per S. Kremer et al. a [KM00] presenten problemes de seguretat similars quan la TTP no actua correctament. Finalment veurem també els problemes de seguretat que poden tenir les solucions per a aquests tipus de protocols quan la TTP s'involucra en una transacció de forma *in-line* i de forma *on-line* (veure el capítol 2). Aquest és el cas dels protocols presentats per J. Zhou et al. a [ZG96a] i per M. Abadi et al. a [AGH02].

Començarem doncs per dos dels articles més referenciats quan es parla de protocols d'intercanvi equitatiu de valors, els presentats per N. Asokan et al. a [ASW97, ASW98]. En el primer article els autors presenten un protocol optimista i genèric per a l'intercanvi equitatiu de valors que es pot adaptar als diferents casos particulars d'aquests tipus

d'intercanvis. Per exemple, per al cas de la signatura electrònica de contractes[7], si l'originador de l'intercanvi no es posa en contacte amb la TTP, aleshores aquesta entitat, encara que volgués, no podria fer trampes ni donar avantatge a cap de les parts involucrades en el protocol (aquesta característica és exposada a l'article original com un requeriment de l'originador de l'intercanvi i és anomenada *no unconditional trust in third party*). Ara bé, si l'originador es posa en contacte amb la TTP llavors la tercera part, intencionadament o no, podria rompre la seguretat de l'intercanvi sense que la part afectada pugui provar-ho davant d'alguna autoritat amb potestat per restablir l'equitat de l'intercanvi. És a dir, la tercera part pot fer que la segona part que intervé en l'intercanvi acabi el protocol amb èxit i amb les evidències del protocol bàsic (com si no hagués intervingut la TTP) i l'originador del protocol podria només tenir una evidència, que els autors anomenen EOD (evidència de lliurament), que no significa que l'intercanvi hagi acabat amb èxit. A més, en aquesta proposta presentada a [ASW97] (no és així en el cas de [ASW98]) la resposta de la TTP depèn d'un factor temporal o de sincronia entre la tercera part i les parts involucrades directament en el protocol, aleshores, si suposam que el canal té un retard arbitrari en el lliurament dels missatges (canal *resilient* [ASW98, KMZ02]), la TTP pot emprar d'excusa el retard del canal per poder emetre qualsevol evidència dient que la petició de l'usuari ha arribat tard. Queda clar, doncs, que aquests tipus de sincronies no són desitjables si volem que els serveis de les terceres parts siguin verificables ja que el moment de recepció de la petició de l'usuari per part de la TTP difícilment ho serà i, a partir d'aquí, el servei que ha d'oferir, que està en funció de l'instant de recepció.

El protocol que presenten Asokan et al. a [ASW98] no té les dependències temporals de l'anterior i s'acosta més al tipus de verificabilitat que nosaltres demanam. El protocol es divideix en un protocol bàsic o principal i, en cas de problemes, les parts poden posar-se en contacte amb la TTP a través dels protocols anomenats *abort* i *recovery*. El problema de la verificabilitat aquí està en el fet que la resposta de la tercera part depèn de l'estat del protocol (*recovered* o *aborted*) i aquest estat no és conegut a priori per l'usuari que fa la petició a la TTP; això significa que no podrà saber de forma immediata si la resposta de la TTP és correcta o no (no podrà verificar l'actuació de la TTP). És a dir, l'usuari no pot estar segur si ha aconseguit l'equitat de l'intercanvi o no, però el protocol sí que li garanteix que les evidències rebudes de la tercera part serviran per restablir l'equitat si entra en conflicte amb l'altra part per l'intercanvi en qüestió. Tot i que nosaltres consideram la tercera part involucrada en aquest protocol no verificable, estam d'acord amb els seus autors amb un altre aspecte sobre la verificabilitat de les terceres parts que

[7] En un protocol optimista per a la signatura electrònica de contractes les dues parts implicades s'han d'intercanviar de forma equitativa la signatura sobre un document electrònic. La TTP està en posició subsidiària. Si una de les dues part pensa que l'altra part no compleix (no segueix les especificacions del protocol d'intercanvi), aleshores pot posar-se en contacte amb la TTP per completar o cancel·lar l'intercanvi de signatures.

diu que qualsevol modificació del protocol que faci *invisible*[8] la tercera part determinarà que aquesta no sigui verificable. És a dir, aquestes dues propietats de les TTPs en els protocols de seguretat (TTP *verificable* i TTP *invisible*) són incompatibles.

Els protocols presentats per J. Zhou et al. a [ZDB99] i per S. Kremer et al. a [KM00] tenen el mateix enfocament que el protocol examinat a l'anterior paràgraf [ASW98]. Tenen un protocol bàsic on les parts poden realitzar l'intercanvi sense la intervenció de la tercera part i, en cas de problemes, poden posar-se en contacte amb aquesta entitat a través del protocol d'*abort* o de *recovery*. De la mateixa manera que ocorre en el protocol [ASW98], la resposta de la tercera part depèn de l'estat de protocol (*recovered* o *aborted*) i aquest estat no és conegut a priori per l'usuari que fa la petició a la TTP. Per tant, aquests protocols de J. Zhou i S. Kremer tenen els mateixos problemes de verificabilitat de la tercera part que els comentats a l'anterior paràgraf per a la proposta feta a [ASW98].

Altres propostes de protocols d'intercanvi equitatiu de valors estan basades en la intervenció *in-line* d'una tercera part com el protocol proposat per T. Coffey et al. a [CS96]; és a dir, la TTP actua com una autoritat de lliurament i intervé en cada transmissió. Actualment aquest tipus de solucions ha estat descartat pels inconvenients que comporta, ja que la tercera part pot convertir-se en un coll d'ampolla tant des del punt de vista de comunicacions com computacional (els problemes d'aquestes solucions han estat comentats en el capítol 2). Una alternativa i una millora en aquestes propostes són els protocols que utilitzen una TTP *on-line*. Alguns exemples d'aquest tipus de protocols més referenciats són els protocols de J. Zhou et al. i M. Abadi et al. definits a [ZG96a, AGH02]. Podríem qualificar la intervenció de la TTP en aquestes propostes com a determinista, en el sentit que la tercera part només pot actuar d'una manera o no actuar (negació del servei).

Per exemple, en el cas del protocol de J. Zhou de [ZG96a][9] la tercera part, en el tercer pas del protocol, rep la clau de l'usuari *A* que permetrà a l'usuari *B* desxifrar el missatge que ha rebut d'*A* en el primer pas del protocol; posteriorment la TTP només pot actuar en un sentit: publicar la clau i els *tokens* de no rebuig de recepció i d'origen del missatge intercanviat entre els usuaris *A* i *B* respectivament. L'actuació tan simple de la tercera part en aquest protocol té l'avantatge d'ésser fàcilment verificable. No obstant això, el protocol presenta greus inconvenients perquè, a causa d'aquest disseny, no compleix alguna de les principals propietats que es demanen als intercanvis equitatius de valors. Aquest és el cas de la propietat anomenada *timeliness*, que poden trobar definida a [KMZ02], o les de propietats no tan exigides com la d'*abuse-freeness*, definida a [SM02]. Concretament, això significa que, en el protocol presentat per J. Zhou et al. a [ZG96a], l'usuari *A* pot

[8] Concepte semblant a la definició de TTP transparent definit per S. Kremer et al. a [KMZ02]

[9] En aquest protocol l'usuari *A* ha d'intercanviar un missatge seu a canvi de rebre un acusament de rebut de l'usuari *B*. La TTP està situada entre els dos usuaris per facilitar la consecució de l'intercanvi.

bloquejar una transacció en el tercer pas del protocol i l'usuari *B* no pot fer res perquè aquesta transacció s'acabi i s'acabi preservant l'equitat de l'intercanvi. A més, durant aquest període de bloqueig, l'usuari *A* pot demostrar a un tercer que, si ell vol, pot fer acabar el protocol amb èxit o no, mentre l'usuari *B* està esperant a mercè del que decidirà *A*. Aquest tipus de problemes s'il·lustren fàcilment en situacions en les quals el protocol d'intercanvi equitatiu de valors s'utilitza per a l'intercanvi de signatures sobre un contracte. Per exemple, podem suposar que *A* ha quedat d'acord a vendre la seva casa per un preu determinat a *B*, aleshores *A* pot mostrar el compromís de *B* per concloure el protocol a un competidor de *B* per comprar la casa i així convèncer-lo que pagui més si la vol comprar. Després *A* pot acabar el protocol amb *B* o avortar-lo en funció de la negociació amb aquest usuari competidor.

El protocol presentat per Abadi et al. a [AGH02] té els problemes que hem descrit en el paràgraf anterior per a la proposta de Zhou et al. a [ZG96a], amb l'única diferència que l'usuari que pot interrompre el protocol i decidir si l'acaba o l'avorta és l'usuari *B*, mentre que l'usuari *A* no pot fer res més que esperar la decisió de *B* en un sentit o en l'altre. Per acabar la revisió de protocols d'intercanvi equitatiu de valors que hem fet en aquest apartat, volem recordar que la nostra intenció no és incloure en els protocols una tercera part verificable que comporti la renúncia a les propietats bàsiques per a la seguretat de l'intercanvi. L'objectiu és fer una anàlisi acurada dels protocols de seguretat per aconseguir que les terceres parts involucrades siguin verificables sense que això impliqui una pèrdua de la resta de propietats de seguretat de l'intercanvi.

5.3.3 Altres protocols de seguretat

Acabam de veure que hi ha intercanvis d'informació que plantegen problemes de seguretat no trivials quan es duen a terme d'una manera electrònica. Les solucions proposades que hem revisat involucren una tercera part que pretén donar seguretat a canvi que les parts involucrades directament en el protocol dipositin un cert grau de confiança en ella. Per exemple, hem vist protocols per a la signatura electrònica de contractes, el correu electrònic certificat o protocols d'autenticació i d'identificació. El rang dels protocols que involucren terceres parts de confiança és molt més ampli, especialment, encara que no exclusivament, en totes aquelles aplicacions relacionades amb el comerç electrònic i amb l'anomenada administració electrònica. Ara bé, com acabam de dir, el rang dels protocols amb TTPs és ampli. Per exemple, podem trobar terceres parts dins de protocols relacionats amb els drets intransferibles, és a dir, protocols on una autoritat pot donar drets a un client per utilitzar uns determinats serveis i alhora assegurar-se que no podrà transferir aquests drets a tercers sense el concurs de l'autoritat.

En aquesta secció volem posar de manifest, per mitjà d'alguns exemples, com la manca de verificabilitat de la tercera part pot causar greus problemes en la seguretat en distints tipus

de protocols, de la mateixa manera que ho hem comprovat en les seccions anteriors per a altres tipus de protocols. Per fer-nos una idea sobre la varietat de serveis que poden oferir les TTPs, hem escollit per a aquesta secció una sèrie de protocols de seguretat amb objectius molt diferents que també ens permetran entreveure com la propietat de verificabilitat de les terceres parts pot tenir aplicació dins d'una gran varietat de procediments electrònics. Inicialment veurem com una tercera part involucrada en un conegut sistema de pagament electrònic proposat per D. Chaum et al. a [CFN89] podria rompre la seguretat del sistema sense que cap dels usuaris pugui tenir cap prova que posi en evidència aquest fet. Veurem que aquesta situació es pot repetir en el protocol de votació electrònica exposat per H. Nurmi et al. a [NSS91], de segellat temporal definit a [RFC3161, ISO18014-2], de drets intransferibles descrit per J. Domingo a [D94] i de telefonia mòbil especificat a [GSM].

Actualment, la manera més habitual de dur a terme transaccions monetàries per mitjà d'Internet consisteix a fer que el comprador enviï una informació determinada sobre la seva targeta de crèdit, o bé que obri un compte a un venedor amb antelació respecte al moment de l'operació. No obstant això, la crítica més important que es pot fer a la compra per Internet basada en targetes de crèdit és que no és anònima [DH99]. Efectivament, és possible monitoritzar les transaccions, atès que la identitat del client s'estableix cada vegada que fa una compra. Per això, dins l'entorn del comerç electrònic, s'han fet propostes de protocols de pagament amb diners electrònics, que és una alternativa que a la vida real també tenim. Els protocols de diners electrònics pretenen recrear el concepte de compres en metàl·lic a Internet. Una de les propostes de referència de pagament amb diners electrònics és l'esquema proposat per D. Chaum et al. a [CFN89]. En aquest protocol l'usuari *A* treu una moneda del seu compte bancari i després pot fer un pagament a un usuari *B* emprant aquesta moneda electrònica. L'usuari *B* després farà l'ingrés de la moneda en el seu compte bancari. L'anonimat del pagador queda preservada gràcies a l'ús de signatures cegues i només es revelarà si l'usuari *A* gasta la mateixa moneda més d'una vegada, i així es podrà detectar l'autor del frau.

En aquesta proposta intervé una TTP anomenada banc, tant en el moment del reintegrament com en el de l'ingrés de la moneda. Els serveis que ofereix el banc als usuaris dins d'aquest esquema de diners electrònics no és sempre verificable, cosa que deixaria les mans lliures a aquesta entitat per cometre algun frau sense que aquesta falta de seguretat es pugui demostrar. Per exemple, les operacions que fa el banc per fabricar la moneda són verificables, hom pot comprovar la validesa de la moneda electrònica que ha tret l'usuari *A* del seu compte (la moneda té la signatura del banc). En canvi, quan l'usuari *B* executa el protocol per ingressar una moneda, el banc pot respondre que aquesta moneda ja fou ingressada anteriorment (encara que només s'hagi utilitzat un cop per realitzar un pagament) i, per tant, no incrementarà el saldo del compte de *B*. És a dir, que l'esquema de diners electrònics proposat a [CFN89] necessita de la confiança total dels

usuaris en el banc, perquè aquest pot invalidar qualsevol ingrés amb l'excusa que la moneda ja ha estat ingressada anteriorment i és impossible per als usuaris saber si aquesta afirmació del banc és certa o no; més encara, en cas de no ésser certa, l'usuari no té cap evidència per poder demostrar davant d'un àrbitre (capaç de resoldre les possibles disputes que sorgeixin en el protocol) el procediment incorrecte del banc.

Un altre camp on podem trobar nombroses propostes de protocols amb TTPs és en aplicacions relacionades amb l'anomenada democràcia digital. Dins d'aquest camp s'ha de remarcar de forma especial les nombroses propostes que hi ha per a esquemes de votació electrònica a través d'una xarxa telemàtica. Un dels esquemes més coneguts i que compta amb nombroses referències és el descrit per H. Nurmi et al. a [NSS91]. En aquest protocol de votació electrònica hi ha involucrada una tercera part de confiança que rep els vots dels votants i publica el resultat de la votació. Per això tota la gent que té dret a vot ho ha de comunicar a la TTP; després la TTP publica la llista amb tota la gent que té la intenció de votar i a través d'un protocol del tipus *all-or-nothing disclosure of secrets* [S96] la TTP distribueix anònimament un nombre identificatiu a cada usuari. Aquest nombre identificarà cada vot. El següent servei que fa la TTP és rebre el vot de cada usuari (el vot, juntament amb el nombre identificatiu, estan xifrats i la clau de desxifratge només la coneix el votant). La tercera part publica una llista amb tots els vots xifrats rebuts, després tots els votants envien la clau perquè la TTP pugui desxifrar els vots i publicar els resultats. Algun dels serveis oferts per la TTP són verificables, com per exemple la publicació de la llista d'usuaris amb intenció de votar, que serà un servei verificable si el llistat té la propietat de no rebuig d'origen. En canvi, la publicació de la llista amb els vots xifrats rebuts no ho és (encara que el llistat tengués la propietat de no rebuig d'origen), perquè, tal i com està dissenyat el protocol, la tercera part pot incloure en el llistat tants de vots com gent ha respost a la primera cridada per votar però que després no ha enviat el seu vot xifrat. Com podem veure en aquest cas, les conseqüències de tenir una TTP no verificable pot conduir-nos fins a l'extrem que aquesta entitat cometi un frau en una votació i, no només no podrà demostrar-se, sinó que ni tan sols serà detectat.

També podem trobar terceres parts de confiança en protocols de segellat temporal com el *Time-Stamp Protocol* (TSP) especificat a [RFC3161, ISO18014-2] que compta amb la intervenció d'una TTP anomenada *Time Stamping Authority* (TSA). El protocol TSP pot utilitzar-se en distintes situacions, per exemple podem plantejar el cas en què els usuaris tenguin la necessitat de certificar que un document existeix a partir d'una certa data. Pensem en el cas d'una disputa per uns drets d'autor: la part que ha produït la primera còpia del treball en disputa guanyarà el cas. A l'apèndix B del RFC 3161 es proposa un exemple d'un possible ús del servei genèric de *time-stamping* presentat en el mateix RFC. En aquest exemple d'aplicació del servei de *time-stamping*, la TSA certifica que una signatura digital sobre un determinat document s'ha realitzat dins d'un interval de temps.

Posteriorment, l'usuari pot mostrar el *TimeStampResp* (estructura d'informació definida a l'estàndard [RFC3161] que és utilitzada per la TSA per certificar la data de la signatura en qüestió) per resoldre una disputa sobre els drets d'autor d'un document com la que hem plantejat en aquest mateix paràgraf. En aquest cas, *TimeStampResp* és una evidència generada per la TSA que prova l'existència d'un determinat document electrònic en mans d'un determinat usuari a una data concreta. Des del punt de vista de verificabilitat de la TTP (la TSA en el nostre cas), el protocol presenta inconvenients semblants als exposats per als protocols de no rebuig i intercanvi equitatiu amb dependències temporals (vegeu l'apartat 5.3.2) ja que suposam que el canal té un retard arbitrari en el lliurament dels missatges, aleshores la TSA pot emprar d'excusa el retard del canal per poder emetre una evidència (*TimeStampResp*) que tengui un temps superior a l'esperat i, d'aquesta manera, podria afavorir els interessos d'un altre usuari. De fet, el problema és detectat en el mateix estàndard i recorda que un atac del tipus '*man-in-the-middle*' pot introduir retards en la resposta de la TSA. D'aquesta manera no podem verificar si és la tercera part que actua de forma incorrecta o el problema és a un altre lloc. La resposta de l'estàndard [RFC3161] a aquest problema de seguretat és afirmar que qualsevol *TimeStampResp* que empra més d'un període de temps acceptable ha de considerar-se sospitós (deixant que cada usuari determini allò que és acceptable esperar).

Després de veure alguna de les conseqüències que podria tenir la TTP no verificable involucrada en el protocol TSP, ara veurem el cas d'una altra TTP no verificable, però dins d'un altre tipus de protocol de seguretat. Els protocols relacionats amb la concessió de drets intransferibles també compten amb terceres parts que, en cas de no ser verificables, poden corrompre impunement la seguretat del protocol. El context on ens podem imaginar fàcilment la utilitat dels protocols de concessió de drets és en un sistema informàtic distribuït on les entitats que requereixen identificació són els ordinadors, els usuaris i els processos. Considerem un escenari distribuït consistent en una gran xarxa amb una autoritat central, un conjunt de servidors fiables (en el sentit que només proporcionen el servei després d'haver comprovat que el pretès client té el dret d'obtenir-lo) que donen accés a certs recursos i una comunitat de clients. Per exemple, podem pensar que l'autoritat és un banc i que parlam d'una xarxa de caixers automàtics que funcionen com a servidors. En el protocol presentat per J. Domingo Ferrer a [DF93] trobam un exemple d'allò que aquí volem aplicar d'una forma sistemàtica; és a dir, la tercera part present en el protocol té operacions verificables, encara que no és del tot verificable. Per veure això necessitarem explicar un poc en detall el protocol. A [DF93] l'autoritat central actua com una tercera part de confiança, que per donar un dret a un client, li dóna (z, E(r)) on E() és una transformació de xifratge amb clau pública, r és un nombre aleatori i z compleix l'equació $x + r = az$ on a és la identitat de l'usuari (només coneguda pel mateix usuari i la TTP). La tercera part publica una llista certificada amb cada un dels drets $y = \alpha^x \bmod p$ i el seu significat. Després, per obtenir accés al servei representat pel dret y, un client c ha d'enviar a un servidor $A= \alpha^a \bmod p$ i (z, E(r)). El

servidor comprova que el client té accés al dret en qüestió si les dades aportades satisfan l'equació: $y\alpha^{D(E(r))} \bmod p = A^z \bmod p$. Això significa que la TTP no pot donar un dret de forma incorrecta i la llista de drets és pública i està certificada amb la qual cosa els usuaris i els servidors poden verificar les equacions i, d'aquesta manera, l'assignació de drets. S'ha de remarcar que els servidors i la TTP no comparteixen cap secret, només *a* és compartit de forma secreta entre la TTP i l'usuari. Això significa que la TTP es podria fer passar per un client qualsevol i emprar un determinat dret a un servidor, sense que ningú pugui demostrar que l'usuari del servei és realment el client o la TTP. També, l'autoritat central podria revelar *a* a un tercer client i aquest es podria aprofitar dels drets assignats a un altre client ja que (z, E(r)) són lliurats públicament. En conclusió podem afirmar que la TTP involucrada en el protocol no és verificable tot i que moltes de les operacions que realitza sí que són verificables.

El paper de les TTPs en els serveis telemàtics no es circumscriu només als protocols de la capa d'aplicació. Així doncs, per acabar aquesta revisió, considerarem finalment el sistema de telefonia GSM (*Global System for Mobile Communications*) [GSM] on hi ha la possibilitat d'afegir seguretat en una comunicació, tant des d'un punt de vista d'autenticació com des del vessant de la confidencialitat. En aquest conjunt de protocols l'operadora de telefonia actua com una tercera part de confiança entre les dues parts comunicants. El procés general del telèfon mòbil és el següent: quan un telèfon vol fer una trucada es connecta per mitjà d'ones a una estació base (una antena propietat de l'operadora de telefonia). Aquesta estació base està connectada normalment per cable a altres estacions base per mitjà del que es coneix com a *centres de commutació mòbils*. Finalment, l'estació base receptora de la trucada emet les ones corresponents al telèfon mòbil que ha de rebre la trucada.

La tecnologia GSM aconsegueix resoldre la seguretat utilitzant criptografia de clau compartida i, concretament, xifratge de flux. Ara bé, el problema que presenten els criptosistemes de clau compartida és l'intercanvi de clau. En el cas de la tecnologia GSM el problema es resol amb un intercanvi de claus en el moment en què l'usuari adquireix l'aparell de telèfon mòbil (de fet aquesta informació és a la targeta intel·ligent que incorpora l'aparell). Això significa que les claus de xifratge no estan compartides pels usuaris finals, sinó entre usuari i operadora de telefonia. La clau és diferent per a cada comunicació i es calcula entre telèfon i l'estació base durant el procés d'autenticació, emprant l'algorisme conegut com a *A8* i la clau *k* que comparteixen l'usuari i l'operadora. L'operadora coneix les claus de xifratge per a qualsevol comunicació entre dos usuaris finals de telefonia GSM. Per tant, els clients han de tenir una confiança il·limitada en la TTP referent a la confidencialitat de les seves comunicacions ja que l'operadora podria rompre la seguretat de l'intercanvi (en aquest cas la confidencialitat) sense deixar cap evidència que permeti acusar-la d'haver romput el servei.

5.4 Consideracions finals

En aquest capítol hem revisat alguns protocols de seguretat amb TTPs que, d'acord amb les definicions i conceptes que hem presentat a l'apartat 5.2 d'aquest mateix capítol, no podem qualificar com a verificables. En els següents capítols veurem més casos com aquests i els estudiarem amb profunditat amb l'objectiu de fer noves propostes en les quals les TTPs involucrades en els protocols siguin verificables. D'aquesta manera, oferirem als usuaris uns protocols amb una característica de seguretat diferent, és a dir, una TTP verificable. Llavors, dependrà de cada aplicació i de cada usuari en particular l'elecció d'una proposta o d'una altra. L'estudi d'aquests protocols ens ha servit per exposar d'una forma acurada tot l'entorn de verificabilitat, així com també ens ha permès elaborar un seguit de recomanacions que ens ajudaran a dissenyar protocols de seguretat amb terceres parts verificables (podem veure l'aplicació d'aquestes recomanacions en un cas concret al capítol 9).

Capítol 6

Verificabilitat en un sistema de pagament amb diners electrònics

6.1 Introducció

En aquest capítol començam a aplicar la propietat de verificabilitat dins dels protocols de seguretat. Es tracta d'aconseguir que la tercera part que intervé en un protocol determinat compleixi amb els requeriments de verificabilitat. D'aquesta manera els usuaris d'un servei de seguretat proporcionat per una TTP podran obtenir evidències sobre com la tercera part ha servit la petició de l'usuari. Aquestes evidències demostraran d'una forma irrefutable si la TTP ha dut a terme les operacions per donar el servei correctament o no.

Com hem explicat en anteriors capítols, amb la introducció de la propietat de verificabilitat, augmentam la seguretat del protocol amb l'objectiu de vèncer les possibles reticències que puguin tenir els usuaris sobre l'actuació d'una tercera part que arbitra el protocol. Les evidències que obtendrà l'usuari sobre l'actuació de la TTP podran ser utilitzades per corregir possibles errades en l'execució del protocol per part de la TTP. És a dir, l'usuari pot comprovar si l'actuació de la tercera part ha estat correcta o no i, si no ho ha estat, ho podrà demostrar davant d'un àrbitre imparcial i demanar una esmena a la situació creada. Amb aquests arguments pensam que podem facilitar l'ús dels distints procediments electrònics ja que així no demanam que l'usuari dipositi una confiança incondicional sobre la tercera part.

En els capítols 6, 7, 8 i 9 veurem com es pot aplicar la propietat de verificabilitat en distints tipus de protocols. Hem escollit una mostra de protocols de seguretat que pugui ser representativa dels diferents serveis que poden proporcionar i del tipus d'involucració que tenen les terceres parts en aquests intercanvis. L'experiència que ens ha donat l'aplicació d'aquesta propietat a distints protocols ens ha fet millorar i trobar nous matisos al concepte de verificabilitat així com la manera d'introduir-lo dins d'un determinat

protocol. Per això, hem partit de la noció de verificabilitat, que hem descrit en el primer apartat del capítol anterior, fins arribar als conceptes de verificabilitat *on-line* i *off-line* que hem exposat en el segon apartat del capítol anterior. L'experiència ha estat necessària per fer evolucionar aquest conceptes i poder aplicar-los cada cop d'una forma més acurada. Aquí, en aquest capítol, introduirem la propietat de verificabilitat de la TTP en un protocol relacionat amb el comerç electrònic: un esquema de diners electrònics.

6.2 Sistemes de pagament

Tant les comunicacions com el comerç electrònic estan cobrant una gran importància en la societat actual. En canvi, alguns usuaris tenen un cert temor sobre la seguretat de les transaccions, probablement a causa de la naturalesa global i virtual del comerç electrònic que fa que els compradors, venedors i bancs no tenguin necessitat de tenir cap contacte físic o coneixement directe un de l'altre. No obstant això, la confiança dels usuaris és necessària per establir els nous procediments de comerç electrònic i, en especial, la confiança amb les terceres parts encarregades d'oferir serveis de seguretat.

Si parlam de confiança i seguretat en l'entorn del comerç electrònic haurem de fixar-nos especialment en els sistemes de pagament. Tant els clients com els venedors estan esperant algun sistema de pagament amb diners electrònics que tengui unes propietats de seguretat similars als sistemes convencionals. Per això serà necessari construir entorns tècnics en els quals els usuaris puguin confiar. En aquest capítol volem incrementar la seguretat d'un conegut sistema de diners electrònic posant una atenció especial en el paper que representa el banc en el sistema i els serveis que proporciona. Per aconseguir això volem transformar la tercera part (el banc en aquest cas) en verificable i, d'aquesta manera, obtenir un nou esquema de diners electrònics sobre el qual els usuaris podran dipositar la confiança amb més facilitat. L'anàlisi i les modificacions que farem en el sistema de diners electrònics pot ser fet sobre qualsevol esquema, però hem escollit la proposta de Brands a [B94] ja que també ha estat escollit per altres investigadors com a model de referència bàsic [CPS96, DFT97, LAK02, PFH02, PP97].

En el cas dels esquemes de diners electrònics, el *banc emissor* actua com una TTP pel fet d'actuar en aquest protocol com una autoritat de seguretat de confiança per a altres entitats (per als usuaris o clients i per als comerços) pel que fa a activitats relatives a la seguretat [X.509, X.810, X.842]. Aquí volem classificar cada una de les operacions o activitats de seguretat (elements de servei) que utilitza el *banc* per proporcionar el servei a un usuari en un esquema de diners electrònics. L'anàlisi es farà des del següent punt de vista: una activitat de seguretat qualificada com a *verificable* implica un dipòsit menor de confiança que una de *no verificable* ja que partim de la definició de verificabilitat expressada als capítols 4 i 5 d'aquesta tesi on vàrem fer la consideració que ara repetim a la figura 6.1.

CLASSE 1	**punt de vista: confiança**
Tipus de servei	característica del servei
a. servei verificable	L'usuari pot detectar i provar que la TTP no ha proporcionat el servei de forma correcta (això és, quan la TTP traeix la confiança que ha dipositat en ella l'usuari).
b. servei no verificable	L'usuari no pot provar que la TTP ha proporcionat el servei de forma incorrecta.

Figura 6.1. Tipus de servei classe 1

Com acabam de veure a la taula anterior aquesta és la forma en què inicialment definim un servei de seguretat verificable o no, des del punt de vista de la confiança que els usuaris han de dipositar en una tercera part. També, en el capítol 5, hem definit activitat de seguretat com a:

- *Activitat de Seguretat*: una TTP ha de proveir un servei a un usuari en resposta a una petició seva. Una activitat de seguretat és un element de servei, això és, una unitat funcional que segmenta i descriu les característiques del servei de seguretat proporcionat per la TTP.

A partir d'aquí, en aquest capítol, analitzarem cada una de les activitats de seguretat que duu a terme el *banc* per oferir el servei en aquest esquema de diners electrònic i, per als serveis *no verificables* (hem de tenir en compte que per considerar un servei verificable totes les activitats relacionades amb aquests servei ho han de ser), proposarem noves solucions per convertir-los en *verificables on-line*, millorant, per tant, la seguretat global del sistema per a tots els seus usuaris [MFH03]. Aquesta millora es fa sense haver de canviar el format de la moneda proposat per S. Brands a [B94], amb la idea que la nostra proposta s'assembli formalment a l'esquema original i així es puguin preservar les seves característiques de seguretat.

Així, doncs, podem fàcilment entendre que un usuari, amb el temor sobre la seguretat en les seves transaccions al qual fèiem referència a l'inici d'aquest apartat, prefereixi un sistema de pagament amb diners electrònics on el banc proporcioni serveis verificables en lloc de no verificables, ja que una errada o la mala conducta del banc podrà ser corregida si els serveis que dóna són verificables (per exemple els usuaris podran iniciar un judici on puguin rebre una compensació a causa d'aquest mal funcionament). Això és així perquè, com ja hem dit, els usuaris d'un sistema on la tercera part proporciona uns serveis

verificables hauran de dipositar un nivell més baix de confiança en el sistema i seran també més receptius a l'hora d'utilitzar aquest sistema per a les seves transaccions. Hi ha nombrosos documents que fan referència a la bona pràctica que pot suposar el fet d'introduir mecanismes en els protocols que ajudin els usuaris a dipositar confiança en les transaccions electròniques i en els serveis de seguretat proporcionats per TTPs [ETSI97, OP98, S96, X.810, X.509, X.842].

Per aconseguir uns serveis de la tercera part verificables haurem d'emprar els serveis de no rebuig, que protegeixen les parts que duen a terme una transacció qualsevol contra la falsa negació sobre un determinat fet o acció que efectivament ha ocorregut. Per això, el protocol haurà de generar evidències que permetin la resolució de disputes com apunten J. Zhou et al. a [ZDB99]. Nosaltres utilitzarem alguns conceptes definits a [X.813]:

- *Evidència*: ítem d'informació que pot ser utilitzada per resoldre una disputa.
- *No rebuig d'origen*: proporciona al receptor una evidència que és la garantia que l'originador d'un missatge no podrà negar falsament haver-lo generat.

En aquest protocol assumim que el canal de comunicació entre usuaris i banc és del tipus *resilient* (recordem que un canal de comunicació és *resilient* si tot missatge col·locat en el canal arriba al seu destinatari encara que amb un retard arbitrari [ZDB99]).

6.3 Serveis del banc emissor a l'esquema de diners electrònics

El sistema bàsic de diners electrònics de Brands està basat en el logaritme discret i en particular en l'anomenat *representation problem.* La seguretat del sistema depèn de l'existència d'una funció de *hash* lliure de col·lisions i de la dificultat de calcular el logaritme discret. Algunes característiques importants del sistema són:

- Els pagaments són anònims, és a dir, són irrastrejables i no vinculables.
- L'usuari està protegit davant d'una acusació fraudulenta del banc d'haver comès una doble despesa (això significa que el banc no podrà rastrejar els diners si l'usuari només els utilitza un cop).
- Té la propietat de no rebuig. Per tant, l'usuari no pot negar haver fet un pagament vàlid.
- El sistema de pagament és *off-line*, això significa que el banc no és present en el moment d'efectuar un pagament, tot i que posteriorment podrem detectar un usuari que hagi fet una doble despesa.
- Es pot guardar d'una forma eficient la informació d'un pagament (17 bytes per pagament).

Nombres primers	p, q on q divideix p-1
Generadors	g, g_1, g_2 de G_q ($G_q \subset Z_p^*$)
Clau identificadora secreta de l'usuari	u_1
Clau pública de l'usuari	$I = g_1^{u1} \bmod p$
Identificador de l'usuari signat pel banc	$M = I * g_2$
Clau privada del banc	x
Nombre aleatori del banc	w
Clau pública del banc	$h = g^x \bmod p$
Pseudo-clau pública del banc	$a = g^w \bmod p$
Identificador de l'usuari signat	$z = M^x \bmod p$
Identificador de l'usuari pseudo-signat	$b = M^w \bmod p$
Funció de *hash* lliure de col·lisions	H
Repte al banc	c
Resposta del banc al repte	$r = cx + w \bmod q$
Verificació que la signatura x és sobre g ($h = g^x$) i M ($z = M^x$)	$g^r \bmod p = h^c a$, $M^r \bmod p = (Ig_2)^r = z^c b$
Nombres aleatoris generats per l'usuari	x_1, x_2, u, v, $s \in Z_p$
Identificador cec de l'usuari (element de la moneda)	$A = M^s = (Ig_2)^s$
Element de la moneda addicional	$B = g_1^{x1} g_2^{x2}$
Identificador cec de l'usuari signat	$z' = z^s = A^x$
Pseudo-clau pública cega	$a' = a^u g^v$
Pseudo-identificador cec de l'usuari	$b' = b^{su} A^v$
Repte cec (valor de funció de *hash*)	$c' = H(A, B, z', a', b')$
Repte retornat al banc	$c = c'/u \bmod q$
Resposta transformada calculada per l'usuari	$r' = ru + v \bmod q$
Moneda	{A, B, sign(A, B)} on sign(A, B) = (z', a', b', r') tals que: $g^{r'} \bmod p = h^{c'} \cdot a'$, $A^{r'} \bmod p = z'^{c'} \cdot b'$
Repte del comerç	$d = H_0(A, B, I_S, date/time)$ on I_S és l'identificador de la comerç
Resposta de l'usuari al repte del comerç	$r_1 = d(u_1 s) + x_1 \bmod q$, $r_2 = ds + x_2 \bmod q$
Verificació del comerç	$A^d B = g_1^{r1} g_2^{r2} \bmod p$

Figura 6.2. Notació

L'esquema de Brands utilitza un protocol del tipus Schnorr [S91] tant en el subprotocol de *reintegrament* (on el banc ha de calcular *signatures cegues restrictives*) com el protocol

de pagament, on el comerç demana al client una prova de possessió Schnorr com a resposta als reptes del comerç. A la figura 6.2 presentam diferents peces d'informació que ens ajudaran a entendre l'esquema de pagament amb diners electrònics proposta per Brands.

A la següent secció descriurem l'esquema de diners electrònics i, per això, cal tenir presents les equacions que hem descrit a la figura 6.2 i el seu significat. A més, en la descripció següent observarem que quan el comerç demana al client una prova de la possessió del diner, aleshores el client ha de mostrar que en coneix una *representació*. Per entendre el concepte de representació podem dir que una representació de z (en termes de g_1, g_2) és $\{u_1*x, x\}$ perquè $z = M^x \bmod p = (g_1^{u1} * g_2)^x \bmod p = g_1^{(u1*x)} * g_2^x \bmod p$. De la mateixa manera la representació de M és $\{u_1, 1\}$. Si un client coneix una representació d'A i B (vg. l'anterior definició de moneda) respecte a (g_1, g_2), aleshores el comerç acceptarà que l'actual propietari de la moneda és el client.

6.3.1 L'esquema de Brands

En aquesta secció descriurem la versió més bàsica del sistema de diners electrònics proposat per Brands a [B94]. Aquesta versió només inclou informació signada (monedes electròniques) d'un sol valor. Per descriure les nostres propostes utilitzarem la notació que habitualment hem fet servir en aquesta tesi però, per descriure la proposta de Brands farem servir la seva notació. Així denotarem el banc per **B**, un propietari genèric d'un compte per **U** (les operacions que aquí associam a aquest propietari, a nivell d'implementació, les faria el dispositiu de pagament, com per exemple una *smart card* o un ordinador personal) i un comerç qualsevol per **S**. El protocol bàsic original està format pels següents procediments o subprotocols:

1. Inicialització del sistema. El banc (**B**) inicialitza els paràmetres del sistema i defineix les primitives criptogràfiques: **B** genera aleatòriament el vector generador (g, g_1, g_2) de G_q ($G_q \subset Z_p^*$) i tria el seu secret $x \in_R Z_p^*$. **B** també tria H i H_0 dues funcions de *hash* lliures de col·lisions. La funció H s'utilitza per construir i verificar les signatures de **B** i la funció H_0 especifica la manera com s'han de computar els reptes en el subprotocol de *pagament*. La clau pública de **B** és $h = g^x$. Després el banc fa públiques aquestes funcions i els paràmetres anteriors.
   Aquí se suposa que cada comerç **S** té un únic identificador I_S. Aquest identificador serà un dels paràmetres d'entrada de la funció H_0, amb la qual cosa tendrem pràcticament assegurat que els reptes que generaran els comerços seran diferents. Per assegurar que un mateix comerç generarà reptes diferents a transaccions diferents l'entrada a la funció H_0 també haurà de comptar amb un paràmetre que representi la data i l'hora de la transacció.

B genera la base de dades dels comptes dels usuaris (on hi haurà la informació de cada un dels clients) i la base de dades de dipòsits de monedes gastades i la informació associada a aquestes.

2. Obertura d'un compte. Per obrir un compte l'usuari (**U**) presenta les seves credencials a **B** i aquest crea un compte al seu nom: **B** associa **U** amb $I = g_1^{u1}$ on $u_1 \in_R Z_p$ és un nombre aleatori escollit per **U** tal que $g_1^{u1} g_2 \neq 1$. **U** guarda en secret u_1 i **B** guarda la informació identificativa d'**U**. Ens referirem a I com el número de compte d'**U** que ha de ser únic per a tot el conjunt d'usuaris. Després **B** calcula $z = (Ig_2)^x$ i ho transmet a **U**.
3. Reintegrament. Quan **U** vol treure del seu compte una determinada quantitat de diners i guardar-los en un dispositiu seu ha de realitzar les següents passes:
    1- **U** prova a **B** que és el propietari d'un compte.
    2- **B** genera de forma aleatòria $w \in_R Z_p$, i envia $a = g^w$, $b = (Ig_2)^w$ a **U**.
    3- **U** selecciona aleatòriament els nombres: $x_1, x_2, u, v, s \in Z_p$; i calcula $A = (Ig_2)^s$, $B = g_1^{x1} g_2^{x2}$, $z' = z^s$, $a' = a^u g^v$, $b' = b^{su} A^v$; després calcula el repte $c' = H(A, B, z', a', b')$; i envia el repte cec $c = c'/u \bmod q$ a **B**.
    4- **B** respon amb $r = cx + w \bmod q$ a **U** i redueix el saldo del seu compte.
    5- **U** verifica que: $g^r = h^c a$, $(Ig_2)^r = z^c b$. Si la verificació és correcta després calcula $r' = ru + v \bmod q$. La moneda que té **U** i de la qual coneix una representació és: $\{A, B, \text{sign}(A, B) = (z', a', b', r')\}$.
4. Pagament. Quan **U** ha de pagar al comerç (**S**) una certa quantitat de diners s'ha d'executar el següent subprotocol:
    1- **U** envia a **S**: A, B, sign(A, B).
    2- Si $A \neq 1$, aleshores **S** calcula i envia el repte $d = H_0(A, B, I_S, \textit{date/time})$ a **U**.
    3- **U** calcula la resposta $r_1 = d(u_1 s) + x_1 \bmod q$, $r_2 = ds + x_2 \bmod q$ i ho transmet a **S**.
    4- **S** verifica la signatura de **B** sobre la moneda (sign(A, B)); i accepta el pagament si:
    $$g_1^{r1} g_2^{r2} = A^d B$$
5. Dipòsit. **S** fa un dipòsit d'una moneda electrònica en el seu compte i **B** augmenta el saldo del compte a través d'aquestes operacions:
    1- **S** envia a **B** una còpia del pagament: A,B,sign(A,B),(r_1,r_2) i (*date/time*).
    2- Si A = 1, aleshores **B** no accepta la transacció. En cas contrari, **B** calcula d i verifica que $g_1^{r1} g_2^{r2} = A^d B$ i que sign(A, B) és una signatura sobre A, B. Després **B** fa una recerca en la base de dades de dipòsits per veure si A ja hi és. Hi ha dues possibilitats:
        a) A no és a la base de dades; aleshores **B** guarda les dades de la transacció i augmenta el saldo del compte de **S**.
        b) A ja és a la base de dades; per tant hi ha hagut un frau. Si la còpia de la transacció guardada indica que qui va fer el dipòsit fou **S** i la

data i hora de la transacció (*date/time*) són els mateixos que la còpia rebuda de la nova transacció, aleshores **S** està dipositant la mateixa moneda per segona vegada. En cas contrari la moneda ha estat reutilitzada (gastada dues vegades), si suposam que (d, r_1, r_2) són dades de la transacció en curs i (d', r'_1, r'_2) de la transacció guardada, **B** pot calcular: $g_1^{(r1- r'1)/ (r2- r'2)}$; que identifica el número de compte de l'usuari que va reutilitzar la moneda.

Fins aquí hem descrit el sistema de pagament *off-line* amb diners electrònics irrastrejables proposat per Brands. Per veure més detalls sobre les seves propietats ens podem adreçar directament al document original on l'autor fa la proposta [B94]. Nosaltres en els següents apartats volem analitzar els serveis que el banc **B** ofereix als usuaris **U** i **S** per després introduir les modificacions necessàries perquè aquests serveis siguin verificables i, d'aquesta manera, augmentant la confiança de l'usuari amb el banc i, per extensió, amb tot el sistema de pagament.

6.3.2 Operacions del banc

A partir de l'especificació feta a l'anterior secció, ara descriurem les operacions o activitats de seguretat que realitza el banc **B** per donar servei als usuaris **U** i **S** en cada subprotocol del sistema de pagament amb diners electrònics. Presentarem aquesta segmentació de les operacions de la TTP com a una seqüència que ens permetrà poder seguir una transacció qualsevol a través de les operacions bancàries. A continuació presentarem el mapa d'activitats de la TTP en cada subprotocol, que no és res més que un esquema en pseudocodi de les operacions de la TTP ja que pensam que presentar les activitats de seguretat de forma algorísmica resulta bastant aclaridor. En el subprotocol d'*inicialització del sistema* el banc inicialitza els paràmetres del sistema de diners electrònics i defineix les primitives criptogràfiques. Així doncs, el banc no ofereix cap servei de forma directa als usuaris. En el subprotocol d'*obertura d'un compte* l'usuari presenta les seves credencials al banc i crea un compte al seu nom. A la figura 6.3 descrivim cada activitat del banc per donar el servei en aquest subprotocol.

- Subprotocol o*bertura d'un compte*:

Inici del subprotocol
► Activitat 1: Recepció i verificació de la petició de l'usuari
If (verificació correcta) **then**
► Activitat 2: Guardar la informació identificativa d'**U**
► Activitat 3: Generar i enviar $z = (Ig_2)^x$
Else
STOP
Fi del subprotocol /**obertura d'un compte*/*

Figura 6.3. Mapa d'activitats del subprotocol d'*obertura d'un compte*

En el subprotocol de *reintegrament* l'usuari treu del seu compte una certa quantitat de diners i ho guarda en el seu dispositiu. Les activitats que el banc dur a terme les explicam a la figura 6.4.

- Subprotocol de *reintegrament*:

Inici del subprotocol
► Activitat 1: Després de la recepció de la petició de l'usuari el banc verifica l'existència del compte i fa el que anomenam "detecció de sobredespesa"; és a dir, comprova que l'usuari només retiri monedes per un valor no superior al seu valor permès
If (verificació correcta) **then**
► Activitat 2: Generar i enviar la moneda electrònica
► Activitat 3: Reintegrament. El banc minva el saldo del compte de l'usuari
Else
STOP
Fi del subprotocol /**reintegrament*/*

Figura 6.4. Mapa d'activitats del subprotocol de *reintegrament*

Durant el subprotocol de *pagament* l'usuari paga al comerç una certa quantitat de diners que té guardat en el seu dispositiu. Encara que sigui un esquema de pagament *off-line*, el banc ofereix a **S** de forma indirecta [MFH02] el servei que descrivim a la figura 6.5.

- Subprotocol de *pagament*:

Inici del subprotocol
► Activitat 1: és una activitat que podem anomenar de validació ja que permet a **S** verificar el correcte format de la moneda enviada per **U**. És una activitat *off-line* perquè és una conseqüència de l'activitat 2 de la figura 6.4 que permet diferir la validació de la moneda
Fi del subprotocol /**pagament*/*

Figura 6.5. Mapa d'activitats del subprotocol de *pagament*

En el subprotocol de *dipòsit* el comerç ingressa una moneda electrònica en el banc, després l'entitat bancària augmenta el saldo del seu compte. En aquest subprotocol el banc, a més de donar el servei per fer el dipòsit també fa activitats relacionades en la detecció del frau que les hem especificades a la figura 6.6.

- Subprotocol de *dipòsit*:

Inici del subprotocol

► Activitat 1: Després de la recepció de la petició de l'usuari el banc verifica el format de la moneda

If (verificació correcta) **then**

If (moneda gastada) **then**

► Activitat 2: Dipòsit de la moneda que implica l'increment del saldo del compte de l'usuari

Else

If (**S** mateix usuari que ja va fer el dipòsit) **and** (les dues transaccions amb el mateix *date/time*) **then**

► Activitat 3: Detecció d'un frau de doble dipòsit; és a dir, detecció de l'ingrés de la mateixa moneda per part del mateix usuari

Else

► Activitat 4: Detecció d'un frau de reutilització; és a dir, detecció de l'ingrés de la mateixa moneda feta probablement per distints usuaris o pel mateix usuari, però provinent de distintes transaccions i la identificació de l'usuari que ha gastat la moneda més d'una vegada

Else

STOP

Fi del subprotocol /**dipòsit*/*

Figura 6.6. Mapa d'activitats del subprotocol de *dipòsit*

6.4 Notació general per a les noves propostes

A la següent secció analitzarem les diferents operacions que duu a terme el banc per donar servei als usuaris, dins l'esquema de Brands, des del punt de vista de la seva verificabilitat. L'objectiu és descriure nous subprotocols per tal d'aconseguir un servei verificable dins del sistema de pagament. Així quan les operacions del banc a l'esquema original siguin qualificades com a *no verificables* proposarem un subprotocol alternatiu per millorar aquesta qualificació i així el servei serà verificable.

A les nostres propostes empram la següent notació *nombre.*{*acció*}:{*descripció*} per descriure cada una de les accions individuals dutes a terme pels participants en el protocol, on *nombre* és el número de seqüència dins del protocol de l'acció concreta que descrivim, {*acció*} pot ser, per exemple, l'enviament d'un missatge de l'usuari X a l'usuari Y (designat per $X \rightarrow Y$) o una operació *get* de FTP [RFC959] designada per $X \leftrightarrow Y$) o l'execució d'algun càlcul d'un participant (designat pel seu nom). La {*descripció*} és una breu explicació del tipus de contingut del missatge intercanviat o del tipus d'acció executada localment. En concret, l'operació que detallam com a $PR_U(m)$ indica la

signatura del missatge *m* amb la clau privada de l'usuari U. Aquesta notació també serà la utilitzada per fer les nostres propostes en els protocols dels capítols 7, 8 i 9.

6.5 Classificació de les activitats de seguretat de la TTP

Un cop definides les operacions que el banc executa per donar servei als usuaris dins del sistema de diners electrònics, procedirem a la seva classificació. D'acord amb l'anterior descripció dels serveis del banc en el sistema de pagament, els usuaris del sistema (venedors i compradors) han de refiar-se del mode de funcionament del banc ja que el banc proporciona serveis de confiança (serveis de seguretat proporcionats per una TTP). Aquests serveis només poden afegir valor quan els seus usuaris estan segurs de la qualitat del funcionament de la TTP. Un punt important per aconseguir la qualitat dins un servei de confiança és que sigui possible comprovar i verificar l'operació de la TTP [OII98].

6.5.1 Classificació

Ara classificarem cada activitat de seguretat d'acord amb les definicions de la secció 5.2. És a dir, cada activitat de seguretat podrà ser catalogada com a no verificable (*nv*), verificable *on-line* (*v_on*) o verificable *off-line* (*v_off*). Començarem classificant les activitats del subprotocol d'obertura d'un compte, que podem veure a la figura 6.7.

- Subprotocol o*bertura d'un compte*:
  ► Activitat 1: Recepció i verificació de la petició de l'usuari
  If (verificació correcta) **then**
  Evidència Rebuda: $z = (Ig_2)^x$
  Classificació de l'Activitat 1: *v_on*
  Else
  Evidència Rebuda: L'usuari no rebrà evidència en aquest cas
  Classificació de l'Activitat 1: *nv*
  En aquesta classificació podem observar que una activitat pot ser classificada de forma diferent en funció del flux d'execució del protocol. No obstant això, en aquest cas haurem de dir que de forma general hem de classificar aquesta activitat com a no verificable

  ► Activitat 2: Guardar la informació identificativa d'**U**
  Evidència Rebuda: $z = (Ig_2)^x$
  Classificació de l'Activitat 1: *v_on*

  ► Activitat 3: Generar i enviar $z = (Ig_2)^x$
  Evidència Rebuda: $z = (Ig_2)^x$
  Classificació de l'Activitat 1: *v_on*

Figura 6.7. Classificació de les activitats del Banc en el subprotocol d'*obertura d'un compte*

A la figura 6.7 hem apuntat que a l'activitat 3 quan l'usuari obre un compte rep del banc aquesta fórmula $z = (Ig_2)^x$, on hi ha la clau secreta del banc juntament amb la identitat de l'usuari. Per tant, si un usuari declara davant d'un àrbitre que el banc no vol operar amb ell tot negant l'existència del seu compte; aleshores, si aquest àrbitre pot tenir accés a la clau secreta del banc, l'usuari estarà en disposició de demostrar que té un compte obert. Els missatges signats pel banc en els subprotocols de *reintegrament* o *dipòsit* de monedes sobre aquest compte, també seran una prova de l'existència del mateix. Per tant, el servei és verificable. No tenim en compte, com en la resta de serveis, que el banc no vulgui obrir el compte ja que aleshores el problema a resoldre seria un altre: la negació del servei. A la figura 6.8 classificam les activitats del banc dutes a terme en el subprotocol de *reintegrament* després de rebre una petició d'un client.

- Subprotocol de *reintegrament*:
  ► Activitat 1: Recepció de la petició i detecció de sobredespesa
  If (verificació correcta) **then**
  Evidència Rebuda: $r = cx + w \bmod q$
  Classificació de l'Activitat 1: *nv*
  Quan l'usuari executa el subprotocol de *reintegrament*, pot comprovar la correcció dels paràmetres enviats pel banc. En canvi, si aquests paràmetres no són correctes i l'usuari no pot generar la moneda, aleshores no pot provar que el banc li va enviar els paràmetres erronis
  Else
  Evidència Rebuda: L'usuari no rebrà evidència en aquest cas
  Classificació de l'Activitat 1: *nv*

  ► Activitat 2: Generar i enviar la moneda electrònica
  Evidència Rebuda: $r = cx + w \bmod q$
  Classificació de l'Activitat 1: *nv*
  El resultat d'aquesta classificació l'hem obtingut amb l'argument de l'anterior classificació

  ► Activitat 3: Reintegrament. El banc minva el saldo del compte de l'usuari
  Evidència Rebuda: L'usuari no rebrà evidència en aquest cas
  Classificació de l'Activitat 1: *nv*

Figura 6.8. Classificació de les activitats del Banc en el subprotocol de *reintegrament*

A la figura 6.9 classificam les activitats o unitats funcionals que executa la TTP durant el subprotocol de *pagament*.

- Subprotocol de *pagament*:
  - ► Activitat 1: Verificació de la moneda per part del comerç.
    Evidència Rebuda: A, B, sign(A, B), $r_1 = d(u_1 s) + x_1 \bmod q$, $r_2 = ds + x_2 \bmod q$
    Classificació de l'Activitat 1: *v_on*
    Durant el subprotocol de *pagament*, l'usuari *S* pot verificar la signatura del banc i també verifica que *U* coneix una representació de la moneda; és a dir que *U* és el propietari de la mateixa. Per tant, *S* pot demostrar si una moneda té la signatura correcta del banc o no, ja que qualsevol pot comprovar que:
    $$g^{r'} = h^{H(A, B, z', a', b')} \cdot a', \quad A^{r'} = z'^{H(A, B, z', a', b')} \cdot b', \quad g_1^{r1} g_2^{r2} = A^d B$$

Figura 6.9. Classificació de les activitats del Banc en el subprotocol de *pagament*

Classificarem les activitats del banc en el subprotocol de *dipòsit* a la figura 6.10.

- Subprotocol de *dipòsit*:
  - ► Activitat 1: El banc verifica el format de la moneda
    Evidència Rebuda: A, B, sign(A, B), $r_1 = d(u_1 s) + x_1 \bmod q$, $r_2 = ds + x_2 \bmod q$
    Classificació de l'Activitat 1: *v_on*
    Com ja hem vist a la figura anterior, qualsevol pot verificar el format i la signatura de la moneda, per tant *S* té elements suficients per demostrar la validesa de la moneda que vol ingressar i, d'aquesta manera, el banc ho haurà de reconèixer.
  - ► Activitat 2: Increment del saldo del compte de l'usuari
    Evidència Rebuda: L'usuari no rebrà evidència en aquest cas
    Classificació de l'Activitat 1: *nv*
  - ► Activitat 3: Detecció de doble dipòsit
    Evidència Rebuda: L'usuari no rebrà evidència en aquest cas
    Classificació de l'Activitat 1: *nv*
    El banc rep les dades referents a una moneda que haurà d'ingressar en un compte d'usuari i, aleshores, pot al·legar que ja tenia totes aquestes dades guardades en la seva base de dades de monedes utilitzades, sense que l'usuari *S*, que vol ingressar la moneda en el seu compte, tengui alguna evidència per poder rebatre-ho
  - ► Activitat 4: Detecció de reutilització
    Evidència: $g_1^{(r1 - r'1)/(r2 - r'2)} = g_1^{u1} = I$
    Classificació de l'Activitat 1: *v_off*
    El banc podria iniciar accions legals contra l'usuari que ha comès el frau i notificar-ho al comerç. El procediment per efectuar això ho deixam en funció del la política de seguretat del banc i del marc legal que permeti sancionar a l'infractor. En qualsevol cas, el protocol presenta elements que permeten verificar l'actuació del banc, però no mitjançant les evidències rebudes per l'usuari

Figura 6.10. Classificació de les activitats del Banc en el subprotocol de *dipòsit*

6.6 Protocol amb la TTP verificable

En aquesta secció proposarem nous subprotocols per a l'esquema de diners electrònics de Brands on comprovarem que la TTP involucrada, en aquest cas el banc, és verificable. Els nous subprotocols estan basats en els originals que acabam de veure amb la intenció que tenguin característiques semblants però afegint la propietat de verificabilitat de la tercera part. El nou subprotocol d'*obertura d'un compte* és a la figura 6.11.

1. $U \rightarrow B$: credencials = PR_U(*request identification*, credencials de l'usuari)
2. B: **if (**credencials correctes**) then**
   B: **guardar(**informació identificativa**)**
   $B \rightarrow U$: PR_B(*request identification*, I, $z = (Ig_2)^x$)
   else
   $B \rightarrow U$: PR_B(*request identification*, credencials, 'credencials no vàlides')

Figura 6.11. Subprotocol d'*obertura d'un compte*

L'operació indicada com a guardar significa que el banc emmagatzema les credencials de l'usuari amb les dades del seu compte en una base de dades que té per a aquesta funció. A la figura 6.12 especificam el nou subprotocol de *reintegrament* perquè les activitats de seguretat que hi dur a terme el banc siguin verificables.

1. $U \rightarrow B$: PR_U(*request identification*, I, 'withdrawal request')
2. B: **if (***balance* $\geq$ (amount of money of an e-coin)**) then**
   $B \rightarrow U$: PR_B(*request identification*, I, *balance*, a, b)
   else
   $B \rightarrow U$: PR_B(*request identification*, I, *balance*, 'overspending detection')
   STOP
3. $U \rightarrow B$: PR_U(*request identification*, I, *balance*, c)
4. $B \rightarrow U$: PR_B(*request identification*, I, *updated balance*, r)

Figura 6.12. Subprotocol de *reintegrament*

El nou subprotocol de la figura 6.12 s'atura després del segon pas si el saldo és més petit que la quantitat de diners que representa la moneda electrònica. No hem inclòs dins cap missatge la quantitat de diners que vol treure perquè en l'esquema original proposat a [B94] només es tenen en compte monedes d'un sol valor. Consegüentment, en el

subprotocol en qüestió, per treure una moneda electrònica no hi ha necessitat d'especificar el valor d'aquesta moneda ja que només n'hi haurà d'un tipus. Els paràmetres *I, a, b, c* i *r* tenen el mateix significat que l'especificat a l'apartat 6.3. Finalment a la figura 6.13 presentam la nostra proposta per al subprotocol de *dipòsit* amb les activitats del banc verificables.

1. $S \rightarrow B$: PR_S (*request identification*, *I*, 'deposit request', A)
2. *B*: **if (**A = 1**) then**
   El banc no accepta el dipòsit per un error de format de la moneda i així ho ha de comunicar a *S*
   else
   if (A no és a la base de dades de monedes utilitzades**) then**
   $B \rightarrow S$: PR_B (*request identification*, *I*, *balance*, 'acepted request')
   else
   $B \rightarrow S$: PR_B (*request identification*, *I*, *balance*, 'spent e-coin', *user_id*, *date/time´* -of the stored transaction-, r'_1)

On *user_id* és un paràmetre que indica si l'usuari que ingressa la moneda és el mateix usuari que la va ingressar per primera vegada (si *user_id* = 1). Amb aquestes modificacions, la informació que ha de guardar el banc per cada moneda gastada és: [A, r_1, r_2, *date/time* de la transacció, *I*].

3. *S*: **if (**la resposta del banc duu l'etiqueta: 'acepted request'**) then**
   $S \rightarrow B$: PR_S (*request identification*, *I*, *balance*, [A, B, sign(A,B), (r_1, r_2), *date/time*])
   else
   if [(*user_id* = 0**) or ((***user_id* = 1**) and (***date/time* de l'actual transacció ≠ *date/time´***) and (**$r'_1 \neq r'_1$**))] then**
   $S \rightarrow B$: PR_S (*request identification*, *I*, [A, B, sign(A,B), (r_1, r_2), *date/time*])

Si aquesta darrera condició no es compleix vol dir que el banc acaba de demostrar que *S* vol ingressar una mateixa moneda per segona vegada. En canvi, si es compleix indica que el comerç *S* no intenta dipositar la moneda per segona vegada. Encara que, en aquesta situació, podria passar que la moneda ja hagués estat dipositada per un altre usuari o pel mateix però amb distinta data de transacció (*date/time*). En aquests dos casos tendríem una situació de 'doble despesa' i no de 'doble dipòsit', la qual cosa significa que el banc podria identificar l'usuari infractor (qui ha gastat dues vegades la mateixa moneda).

Figura 6.13. Subprotocol de *dipòsit*

4. *B*: **if (**la petició de dipòsit havia estat acceptada**) then**
   if ($g_1^{r1}g_2^{r2} = A^dB$**) and (**sign(A,B) és una signatura sobre A, B**) then**
   $B \rightarrow S$: PR_B (*request identification*, *I*, *updated balance*, 'accepted e-coin')
   Després d'haver fet les pertinents verificacions, la moneda és dipositada al compte de *S*
   else
   $B \rightarrow S$: PR_B (*request identification*, *I*, 'invalid e-coin')
   else
   $B \rightarrow S$: PR_B (*request identification*, *I*, (d',r'_1,r'_2), 'double-spending detection')

   Els paràmetres *I*, A, B, sign(A,B), r_1, r_2 i r'_1 tenen el mateix significat que en la secció 6.3.

***Figura 6.13* (continuació).** Subprotocol de *dipòsit*

6.7 Resolució de disputes

En aquest apartat volem argumentar que, a les nostres propostes, les activitats de seguretat dutes a terme pel banc són ara verificables. En els subprotocols presentats a les figures 6.11, 6.12 i 6.13, el banc fa el mateix tipus operacions que a l'esquema inicial tot i que no es duen a terme de la mateixa forma, ja que les solucions estan basades en les originals. La intenció de la nostra proposta és que el banc sigui una TTP verificable tal i com enunciarem seguidament.

***Enunciat*: El banc, que és la tercera part de confiança involucrada en la nostra proposta de sistema de pagament amb diners electrònics, és verificable ja que totes les activitats que duu a terme són verificables *on-line*.**

A continuació, mitjançant les distintes proves, analitzarem cada una de les activitats de seguretat i comprovarem que la tercera part és verificable.

Prova 1*: L'activitat 1 del subprotocol d'*obertura d'un compte* és verificable *on-line
***Argumentació*:** A la proposta original la primera activitat no verificable és l'activitat 1 del subprotocol d'*obertura d'un compte*. La disputa podria sorgir si el banc considera que les credencial enviades per l'usuari no són correctes. Segons la nostra proposta l'usuari ara rebrà una notificació signada pel banc amb les dades sobre les quals s'han fetes les comprovacions pertinents (PR_B(*request identification*, credencials, 'credencials no vàlides')). Aquest missatge lligat a la petició de l'usuari feta al primer pas d'aquest subprotocol són

evidència suficient per verificar l'operació del banc. Així doncs, amb la nova proposta, classificam aquesta activitat de seguretat com a verificable *on-line*.

Prova 2*: Les activitats 1, 2 i 3 del subprotocol de *reintegrament* són verificables *on-line
***Argumentació*:** Les tres activitats que fa el banc en el subprotocol de *reintegrament* original han estat classificades com a no verificables. Aquestes activitats fan referència a la detecció de sobredespesa, la generació de la moneda electrònica i el decrement del saldo del compte.

En el segon pas del subprotocol que proposam a la figura 6.12 el banc comprova la petició de l'usuari i fa la detecció de sobredespesa (activitat 1). Aquesta entitat envia una evidència a l'usuari sobre el saldo del seu compte. Si el saldo és més gran que el valor d'una moneda, aleshores l'evidència enviada pel banc representa el seu compromís d'executar el subprotocol de *reintegrament* perquè l'usuari tregui una nova moneda del seu compte. Des d'aquest punt de vista, podem veure el subprotocol com un protocol optimista per a l'intercanvi equitatiu de valors [ASW97] on els missatges dels passos 1 i 3 autoritzen el banc a actualitzar (minvar, en aquest cas) el saldo del compte de l'usuari i en els passos 2 i 4 el banc col·labora amb l'usuari a generar la nova moneda. D'acord amb això, quan el banc envia el seu compromís en el pas 2, l'usuari pot aconseguir *weak fairness* [ASW97] si el banc no envia el missatge especificat en el pas 4, perquè l'usuari pot emprar l'evidència rebuda en el pas 2 per aconseguir l'equitat en un sistema de resolució de disputes extern. És a dir, qualssevol de les dues parts que intervenen el protocol poden acudir a àrbitre perquè pugui avaluar les evidències que han obtinguts de l'execució de tot o part del protocol i aconseguir equitat en la transacció (suposant que alguna d'elles considera que l'altra part no ha executat correctament el protocol). En qualsevol cas, l'usuari podrà verificar immediatament després de rebre el missatge del pas 2 l'activitat 1 del banc i en conseqüència aquesta activitat serà verificable de forma *on-line*.

En aquest mateix subprotocol l'usuari obté un evidència que inclou els paràmetres enviats pel banc. Per tant, si el banc minva el saldo però els paràmetres enviats a l'usuari són incorrectes, aleshores l'usuari té una evidència que pot ser utilitzada per aconseguir l'equitat en un sistema de resolució de disputes extern. D'aquesta manera l'activitat 2 és ja verificable *on-line*.

En el subprotocol de *reintegrament* especificat a [B94], l'usuari ha de provar ser el propietari del seu compte. Malgrat això, el banc no dóna cap prova a l'usuari de com ha abaixat correctament el saldo del seu compte. D'aquesta manera, podem dir que l'operació del banc és no verificable ja que l'usuari no té cap evidència sobre l'actualització del seu saldo. En canvi, en el subprotocol que hem presentat a la figura 6.12, el banc, en el pas 4,

envia un missatge signat amb el saldo actualitzat. En conseqüència, el subprotocol que hem proposat dóna a l'usuari l'evidència que necessita per aconseguir l'equitat en cas d'una actualització equivocada del saldo. Així, d'acord amb les especificacions d'aquest nou subprotocol, l'activitat de seguretat 3 serà ara verificable *on-line*.

Prova 3*: Les activitats 2, 3 i 4 del subprotocol de *dipòsit* són verificables *on-line
***Argumentació*:** No hem fet cap modificació que afecti a l'activitat 1 dels subprotocols de *pagament* i de *dipòsit*, amb la qual cosa continuaran essent operacions verificables. En canvi, resta per analitzar si amb les noves propostes fetes les activitats 2, 3 i 4 del subprotocol de *dipòsit* són ara verificables *on-line*.

Referent a l'activitat 2 a [B94] no s'especifica que el banc hagi de comunicar a l'usuari el seu saldo després d'ingressar una moneda en el seu compte per poder comprovar que s'ha incrementat de forma correcta. Per tant, l'usuari no només no té cap prova per poder demostrar que el seu saldo ha estat incrementat correctament o no, sinó que senzillament no se l'informa d'aquest fet. Amb el subprotocol proposat la figura 6.13, després dels dos intercanvis inicials, els passos 3 i 4 completen la transacció de manera que si el banc no realitza el seu servei de forma correcta, aleshores l'usuari *S* tendrà les evidències necessàries (PR_S (*request identification*, *I*, 'deposit request', A) i PR_B (*request identification*, *I*, *balance*, 'acepted request')) per equilibrar la situació amb l'ajut d'una altra TTP perquè el seu saldo sigui actualitzat correctament. Per tant, amb la nova proposta feta l'activitat de dipòsit és verificable *on-line*.

En el subprotocol de *dipòsit* el banc rep les dades referents a una moneda que haurà d'ingressar en un compte d'usuari i, aleshores, pot al·legar que ja tenia totes aquestes dades guardades en la seva base de dades de monedes utilitzades, sense que l'usuari *S*, que vol ingressar la moneda en el seu compte, tengui alguna evidència per poder rebatre-ho. A més, d'acord amb el protocol original, el banc no necessita aportar cap prova per no acceptar la moneda per aquest motiu. Així doncs, l'activitat 3 del protocol original ha estat classificada com a no verificable. Perquè l'operació del banc sigui verificable, el banc ha de demostrar que la moneda ja ha estat ingressada prèviament, abans que *S* reveli totes les dades referents a aquest dipòsit. Per fer que l'activitat de detecció de doble dipòsit (activitat 3) sigui verificable, el subprotocol de *dipòsit* ha de modificar-se de la manera especificada a la figura 6.13.

En el subprotocol de la figura 6.13 quan el banc emet el segon missatge especificat en el pas 2 d'aquest subprotocol vol dir que la moneda ja ha estat ingressada, indicant amb el paràmetre *user_id* si fa el dipòsit el mateix usuari o és un usuari diferent de qui va dipositar per primera vegada la moneda. Si *user_id* indica que es tracta del mateix usuari i el banc revela a *S* la mateixa data de transacció i el mateix valor del paràmetre r_1, entenem que li està demostrant que la moneda ja ha estat usada. De totes maneres, *S* pot continuar

amb el subprotocol perquè el banc pugui trobar la identitat de l'usuari que ha usat dues vegades la mateixa moneda.

Finalment, l'activitat 4 ja era verificable a l'esquema original. La verificabilitat però és *off-line*. El banc ha de calcular:

$$g_1^{(r1-\ r'1)/\ (r2-\ r'2)} = g_1^{u1} = I$$

el valor $(r_1 - r'_1)/(r_2 - r'_2)$ mod q li serveix com a prova de reutilització, ja que, suposant la irresolubilitat del problema del logaritme discret, el banc només pot arribar a aquesta conclusió quan un usuari gasta una mateixa moneda més d'una vegada.

***Resultat*:** D'acord amb les proves 1, 2 i 3, que acabam de presentar i les seves argumentacions, la tercera part de confiança involucrada en la nostra proposta de sistema de pagament amb diners electrònics és verificable ja que totes les activitats que duu a terme són verificables *on-line*.

6.8 Conclusions

En aquest capítol hem analitzat les operacions que duu a terme el banc dins del sistema de pagament amb diners electrònics proposat a [B94]. En aquest protocol, el banc actua com a tercera part de confiança, oferint serveis de seguretat als usuaris en distintes situacions, com per exemple, durant el reintegrament d'una moneda electrònica, en el moment de realitzar un pagament i, també, quan es fa un dipòsit de diners. En aquestes situacions els usuaris confien en l'actuació del banc per aconseguir monedes electròniques vàlides, que puguin ser utilitzades per fer un pagament o que puguin ser ingressades en el compte de l'usuari, segons sigui el cas. També s'ha de confiar en el banc perquè el sistema no sigui corrupte, és a dir, perquè els increments i les reduccions del saldo dels comptes dels usuaris siguin correctes i, a més, es puguin prevenir o detectar múltiples despeses d'una mateixa moneda.

Després d'analitzar les operacions fetes pel banc per donar servei als usuaris en aquest protocol, hem proposat una sèrie de modificacions sobre la proposta original perquè els usuaris del sistema puguin verificar les actuacions del banc i així obtenir més garanties de seguretat per a les seves transaccions, ja que podran tenir evidències sobre la seguretat que aporta el banc en el sistema de pagament. Ara totes les activitats de seguretat del banc són verificables *on-line* i, per tant, aquest protocol té la propietat de verificabilitat de la TTP.

D'aquesta manera, les evidències obtengudes emprant conceptes de no rebuig (definits a [X.813]) podran ser utilitzades per corregir una possible actuació errònia (intencionada o

no) del banc. Per corregir aquesta situació, on un mal servei del banc ha romput la seguretat del sistema, s'haurà d'iniciar un contenciós davant la instància pertinent i presentar les evidències que demostren l'error. Així doncs, podem dir que després de les propostes fetes aquí el sistema és més sòlid i apropa el control de la seguretat als usuaris. Hem obtingut, per tant, una alternativa al protocol original que ofereix unes característiques de seguretat addicionals (verificabilitat dels serveis de la tercera part); aleshores els usuaris podran escollir entre l'ús d'un protocol o un altre en funció de la seguretat que desitgin.

L'estudi fet en aquest capítol no només ha servit perquè un sistema de diners electrònics sigui més segur i no requereixi d'un dipòsit de confiança tan gran en la tercera part que hi intervé. També ens ha servit per poder veure l'actuació de la TTP des d'un punt de vista més genèric i detectar, en aquest punt de la recerca, sobre quin tipus d'operacions o situacions el servei de la tercera part no és típicament verificable i, d'aquesta manera, poder detectar i corregir amb més facilitat TTPs no verificables en altres protocols. Observant les situacions de no verificabilitat del banc en el protocol analitzat podem dir que les situacions no verificables provenen genèricament de dues fonts:

- Informació que internament manipula la TTP de la qual depenen algunes de les respostes de la TTP als usuaris del servei. Per exemple, el saldo del compte bancari és el causant que el servei de reintegrament no sigui verificable a la proposta original. Un cas semblant és la base de dades de monedes gastades que utilitza el banc per la detecció de possibles fraus.
- Els distints missatges d'una mateixa transacció no tenen cap punt de connexió que els lligui. Per exemple, els paràmetres emesos pel banc que ajudaran a l'usuari a generar la moneda no tenen cap lligam amb la petició de reintegrament de l'usuari. Aquest fet és el causant que el servei del banc en el reintegrament de la moneda electrònica sigui no verificable.

Abans d'acabar volem fer una observació que lliga amb el mètode de classificació dels serveis de les TTPs exposat en el capítol 4. Hem d'indicar que podria ser que per motius legals el banc no pogués enviar la informació especificada en el darrer enviament del subprotocol de *dipòsit* especificat a la figura 6.13, ja que amb aquests paràmetres el comerç pot saber qui és l'infractor d'una doble despesa. Això podria ser així perquè és pot considerar que el lloc adequat per fer aquest tipus de demostracions és, per exemple, davant d'un jutge. Això significaria que l'activitat 4 d'aquest protocol només seria verificable *off-line* i, així, no podrien classificar la TTP, que intervé en aquest protocol, com a verificable. Tot i que la resta d'operacions del banc ho serien. Aquest fet és un dels motius que ens ha fet indicar a l'apartat de conclusions del capítol 4 que una línia d'investigació futura podria intentar trobar una forma perquè els usuaris poguessin ponderar les avaluacions de cada propietat dels serveis de l'una TTP perquè, com és prou

evident, no es pot fer la mateixa consideració sobre l'actuació d'una TTP si sabem és no verificable perquè moltes de les seves activitats no ho són o, simplement, és no verificable perquè una de les seves activitats només és verificable *off-line*.

En el següent capítol analitzarem un altre tipus de protocol de seguretat. La intenció d'aquesta nova anàlisi, dins la recerca feta en aquesta tesi, serà la de confirmar i eixamplar els mètodes per introduir la propietat de terceres parts verificables en els protocols de seguretat i les situacions que provoquen que els serveis de confiança no siguin verificables.

Capítol 7

Verificabilitat en un sistema de votació electrònica

7.1 Introducció

La votació electrònica a través d'Internet és un tema d'actualitat. Els esforços que s'ha fent recentment per part de les administracions públiques han centrat l'atenció de molta gent cap a conceptes com són ara la democràcia digital o l'administració electrònica. Els defensors dels sistemes de votació a través d'Internet argumenten que l'adopció d'aquests sistemes incrementarà la participació i reduirà el cost de les eleccions. En canvi, el principal argument en contra són els problemes de seguretat que pot representar l'utilització d'aquests sistemes. Sense cap dubte, per poder implantar aquests sistemes de votació electrònica és necessari un equilibri entre seguretat i simplicitat [IPI, CIV00].

Per tal de donar confiança al votant i legitimitat als governants electes, tots els nivells del procés de votació a través d'Internet han de ser auditables. Per això pensam que un objectiu dels protocols de votació electrònica no és tan sols aconseguir unes eleccions netes sinó que aquestes eleccions siguin percebudes com a netes. Les solucions proposades en els articles científics utilitzen *Autoritats de Seguretat* que són les responsables de fer el recompte de les paperetes i de salvaguardar la integritat del procés. Aquestes *Autoritats* representen el paper d'allò que anomenam terceres parts de confiança (TTPs) [X.842] i poden tenir noms diferents depenent del protocol de votació en concret i dels serveis de seguretat que proporcionen (per exemple podem trobar noms com *Administrator*, *Counter*, *Central Tabulating Facility*, *Central Legitimisation Agency*, *Commissioner*…) [FOO93, CC97, SK95, RHOA, S96, RRN01, JZF03].

En aquest punt, nosaltres volem enllaçar l'estudi que fem en aquesta tesi sobre la propietat de verificabilitat de les terceres parts de confiança amb els protocols de votació electrònica. Es tracta d'aconseguir que les TTPs que intervenen en un determinat esquema de votació per Internet siguin verificables; d'aquesta manera aconseguirem acostar la seguretat als usuaris (obtendran evidències de les activitats de seguretat de les terceres

parts) i incrementar la seva confiança en el procés. Així ajudam a fer que les eleccions siguin més segures i també que siguin percebudes amb més transparència (recordem que, amb la introducció de la propietat de verificabilitat, els votants obtendran evidències sobre l'actuació de les TTPs, a través de les quals es podrà comprovar la correcció de les operacions fetes per les TTPs i, en cas d'incorrecció, podem emprar-les per corregir possibles errades d'aquestes entitats).

Com passa en altres tipus de procediments, quan hi ha un canvi entre el format convencional en paper i el format electrònic, els processos de votació per Internet canvien la percepció pública d'unes eleccions. Per tant, és pertinent intentar introduir elements de seguretat i confiança dins d'aquests nous procediments electrònics. No és estrany, doncs, que en alguns informes sobre la votació per Internet troben interrogants sobre si la tecnologia electrònica pot afectar la confiança de la gent en unes eleccions i si la manca de transparència dels sistemes automàtics afecta la confiança en el procés. Aleshores, la introducció de propietats com la verificabilitat pot donar un valor afegit a la seguretat d'un esquema de votació determinat.

En aquest capítol fem una passa més pel que fa a la verificabilitat en els protocols de seguretat. Volem incrementar la seguretat d'un conegut protocol de votació formulat per A. Fujioka et al. a [FOO93] a través de l'anàlisi de l'actuació de les TTPs durant el procés electoral. Després, si els serveis proporcionats als usuaris no són verificables (és a dir, les operacions de les TTPs no són verificables *on-line*), estudiarem la manera d'introduir la verificabilitat dins del protocol. Hem el protocol de votació proposat a [FOO93], ja que també és utilitzat com a model de referència bàsic per a altres investigadors [CC97, SK95, RHOA, RRN01, JZF03].

7.2 Actuació sobre el protocol de votació

En el capítol anterior hem analitzat el servei de seguretat que ofereix un banc, que actua com a tercera part de confiança, dins d'un conegut esquema de diners electrònics. Ara volem introduir la verificabilitat dins d'un esquema de votació electrònica. L'esquema de votació que hem escollit té dues entitats que actuen com a terceres parts de confiança entre els votants que participen en el procés de votació. Aquestes dues TTPs s'anomenen originalment *Administrator* i *Counter* i ofereixen serveis de seguretat als usuaris de l'esquema de votació.

Nosaltres volem determinar i posteriorment classificar cada una de les activitats de seguretat que duen a terme aquestes entitats. El nostre objectiu no ha estat tan sols introduir modificacions en el protocol original per tal d'obtenir un esquema alternatiu on els serveis de les TTPs siguin verificables, sinó que també volíem trobar similituds entre els distints tipus d'operacions que fan les TTPs en els protocols de diners electrònic de

l'anterior capítol i aquest de votació electrònica i les solucions que podem aportar perquè aquestes operacions siguin verificables [MFH04].

Com hem vist en el capítol anterior, des del punt de verificabilitat, les operacions relacionades amb la comprovació i actualització de dades, que la TTP guarda internament, presenten freqüentment problemes de verificabilitat. També hem vist que hem de tenir cura especial amb el contingut i el format dels missatges emesos per la TTP. Veurem en aquest capítol que podem detallar i ampliar aquesta casuística i comprovarem que l'ús que fem de les evidències i dels serveis de no rebuig serveixen igualment per presentar un protocol alternatiu on els serveis de les terceres parts siguin verificables.

Utilitzam els serveis de no rebuig per protegir els usuaris del protocol contra la falsa negació que un determinat fet o acció s'ha produït, ja que el seguiment del protocol genera evidències que permeten resoldre les disputes que puguin sorgir [ZDB99]. En relació als protocols que definirem, ens interessa que el concepte d'equitat hi estigui present, encara que només sigui de forma implícita. Un intercanvi equitatiu ha de garantir que al final de l'intercanvi, cada part ha d'haver rebut allò que esperava de l'altra i cap part ha rebut res més. Per tant, direm que una part comunicant actua amb equitat si segueix les regles del protocol i no abandona l'execució intencionadament [ZG96a]. En la secció número 5 d'aquest capítol definirem nous protocols amb serveis de seguretat verificables. Aquests protocols seran equitatius, en el sentit que, un cop acabat l'intercanvi, l'originador i el receptor tendran evidències vàlides i irrefutables de les accions dutes a terme durant l'execució del protocol, sense donar a cap part cap avantatge sobre qualsevol altra part [ZG96a]. A nosaltres ens interessaran especialment les evidències que fan referència a les operacions dutes a terme per una TTP quan dóna un servei a un usuari. Els nostres protocols proporcionaran evidències als votants; les evidències mostraran d'una forma no rebutjable com una TTP ha proporcionat el servei de seguretat. Les proves podran ser utilitzades per solucionar una disputa si el votant no ha rebut allò que esperava rebre de la TTP. D'aquesta manera, podem dir que, malgrat una TTP no actuï correctament, el protocol garanteix l'equitat de l'intercanvi.

7.3 Serveis de les TTPs en el protocol de votació electrònica

En aquesta secció descriurem el protocol de votació electrònica proposat per Fujioka et al a [FOO93]. En les seccions següents descriurem i classificarem els serveis de les TTPs involucrades en el protocol i després farem les nostres propostes perquè els serveis de seguretat siguin verificables. Abans d'especificar l'esquema de votació proposat per A. Fujioka et al., explicarem breument la notació que farem servir per a les primitives criptogràfiques emprades en la descripció del protocol. Aquesta notació està exposada a la taula 7.1.

Esquema de compromís de bits (*Bit Commitment*) per al missatge v_i usant la clau k_i	$\xi(v_i, k_i)$
Esquema de signatura del votant V_i	$\sigma_i(e_i)$
Esquema de signatura de l'Administrador	$\sigma_A(e_i)$
Signatura cega (*Blind Signature*) per al missatge x_i i el nombre aleatori r_i	$\chi(x_i, r_i)$
Tècnica de recuperació de signatura cega	$\delta(d_i, r_i)$

Figura 7.1. Notació

Les tècniques de *Bit Commitment* i *Blind Signatures* són dos algorismes crítics que utilitza aquest protocol. Els esquemes de compromís (*Bit Commitment*) de bits es poden utilitzar per mostrar una cadena de bits que va lligada i representa una determinada informació (per exemple, una predicció, un vot, etc.) sense revelar la informació que representa. Posteriorment, l'usuari pot destapar la cadena de bits i mostrar la informació que amagava aquesta cadena. La paraula *compromís* que s'utilitza per designar aquests esquemes prové de la característica d'aquesta tècnica que pretén assegurar que, un cop l'usuari ha revelat la cadena de bits, no podrà canviar la informació que hi amaga; és a dir, l'usuari queda compromès a la informació que hi ha sota la cadena de bits ja que només tendrà una manera de poder-la destapar. Podem trobar una descripció i una implementació d'un esquema de compromís de bits utilitzant funcions unidireccionals a [S96]. Referent a les signatures digitals cegues (*blind signatures*), hem de dir que generalment en els protocols de signatura digital l'entitat que signa un determinat document sempre coneix allò que està signant. La tècnica de signatura cega permet que una entitat signi un document electrònic sense que conèixer seu contingut. En el capítol anterior també hem utilitzat aquesta tècnica: el banc emissor del sistema de pagament realitza una signatura cega sobre els bitllets que els usuaris treuen dels seus comptes. David Chaum, que proposà inicialment aquest procediment, explica signatures cegues a [C82].

7.3.1 El protocol de votació proposat per Fujioka et al.

El sistema de votació proposat per Fujioka et al. compleix les principals característiques de seguretat que es poden exigir a un esquema de votació electrònica. Aquestes característiques són:

- *Anonimat*: Ningú ha de poder relacionar els vots amb els votants que el ha emès.
- *Eligibilitat*: Ningú que no tengui permès votar podrà votar.
- *No-reutilització*: Cap votant pot votar dues vegades.

- *Precisió*: Tots els vots vàlids són comptats correctament.
- *Incorruptibilitat*: Un votant deshonest no pot corrompre la votació (canviant els vots emesos o aturant el procés sencer).
- *Infalsificabilitat*: El recompte ha de ser infalsificable.
- *Imparcialitat*: El recompte de les paperetes no ha de poder afectar la votació.

No obstant això, hem de remarcar que els autors del protocol necessiten fer algunes suposicions, que nosaltres ens interessa destacar, per demostrar que l'esquema de votació té les anteriors propietats. Per exemple, per demostrar la propietat de *completeness* han de suposar que cap de les TTPs voldrà o podrà corrompre el resultat de la votació i, per tant, poden assegurar que tots els vots vàlids seran comptats correctament. Ara bé, com demostrarem més endavant, una TTP corrupta podria fer un recompte fraudulent de la votació (especialment si no voten tots els votants que podrien fer-ho). Aquesta manipulació podria no ser detectada i, en qualsevol cas, ningú no disposaria de cap evidència per demostrar que ha estat la TTP qui ha manipulat el procés. Amb la introducció de la propietat de verificabilitat de les terceres parts, nosaltres pretenem donar un protocol alternatiu on puguem assegurar als votants la detecció i la posterior rectificació d'un error en el procés produït per una operació no correcta d'una TTP.

L'esquema de votació té sis etapes diferents. Els actors que podem trobar en aquestes etapes són els votants (ID_i és l'identificador del votant V_i i v_i és el seu vot), l'*Administrator* (*A*) i el *Counter* (*C*). El protocol de votació és el següent:

1. Etapa de *preparació*
   - El votant V_i selecciona el vot v_i i completa la seva butlleta $x_i = \xi(v_i, k_i)$ utilitzant la clau k_i escollida aleatòriament
   - V_i calcula el missatge e_i usant una tècnica de signatura cega $e_i = \chi(x_i, r_i)$
   - V_i signa $s_i = \sigma_i(e_i)$ i envia $[ID_i, e_i, s_i]$ a l'*Administrator A*
2. Etapa d'*administració*
   - L'*Administrator A* processa les peticions dels votants:
     i. *A* comprova que V_i té dret a vot. Si V_i no té dret a vot, *A* rebutja la petició
     ii. *A* comprova que V_i no ha demanat abans una signatura sobre una butlleta cega. Si V_i ja ho ha fet, *A* rebutja la petició
     iii. *A* comprova la signatura s_i sobre e_i. Si la signatura és valida, aleshores *A* calcula $d_i = \sigma_A(e_i)$ i l'envia a V_i

     Al final d'aquesta etapa, *A* anuncia el nombre de votants que han rebut la signatura de l'*Administrator A* i també publica una llista que conté totes les peticions rebudes $[ID_i, e_i, s_i]$
3. Etapa de *votació*
   - V_i recupera la signatura desitjada y_i de la butlleta x_i calculant $y_i = \delta(d_i, r_i)$

- V_i comprova que y_i és la signatura de l'administrador sobre x_i. Si la comprovació falla, V_i ho reclama mostrant que la parella [x_i, y_i] és invàlida
- V_i envia [x_i, y_i] al *Counter C* per un canal de comunicació anònim

4. Etapa de *reunió*
   - El *Counter C* comprova que y_i és una signatura sobre x_i usant la clau de verificació de l'administrador. Si la comprovació és bona, *C* introdueix [l, x_i, y_i] dins d'una llista amb el nombre l
   - Després que tots els votants hagin votat, *C* publica la llista
5. Etapa d'*obertura*
   - V_i comprova que el nombre de butlletes a la llista és igual que el nombre de votants[10]. Si la comprovació falla, els votants poden reclamar demostrant que coneixen el factor d'emmascarament r_i usat per calcular e_i (missatge que conté la butlleta de cada votant) el qual ha estat signat posteriorment per *A* obtenint d_i. Només un votant pot conèixer el factor d'emmascarament del seu vot.
   - V_i comprova que és dins el llistat. Si el seu vot no hi és, aleshores ho pot reclamar obrint [x_i, y_i]
   - V_i envia la seva clau amb el nombre l a *C* mitjançant un canal de comunicació anònim
6. Etapa de *recompte*
   - *C* obre la butlleta cega x_i, recupera el vot v_i i comprova si v_i és un vot vàlid
   - *C* recompta tots els vots i anuncia els resultats de la votació (*C* publica una llista amb tots els [l, x_i, y_i, k_i, v_i] rebuts)

7.3.2 Operacions de les TTPs

Dos dels tres actors que hi ha a l'esquema de votació que acabam de descriure són terceres parts de confiança: l'*Administrator* i el *Counter*. El tercer actor és el votant genèric V_i que selecciona un vot v_i. Ara descriurem cada una de les operacions o activitats de seguretat que proporciona o bé l'*Administrator* o bé el *Counter* en cada una de les etapes o subprotocols del sistema de votació proposat a [FOO93]. Presentarem aquestes operacions de forma seqüencial de tal manera que podrem seguir el procés de votació a través de les activitats de seguretat o unitats funcionals executades per les TTPs.

En l'etapa de *Preparació* el votant omple una butlleta i l'envia a l'administrador. Prèviament a aquesta etapa hem de suposar que una Autoritat ha publicat un llistat amb tots els identificadors (ID_i) de tota la gent que té dret a votar: $sign_A$('list of voters', $\Sigma_i ID_i$).

[10] Els autors de l'esquema de votació suposen que cap votant que ha fet l'etapa de preparació s'abstè a l'etapa de votació perquè les terceres parts no puguin corrompre fàcilment el resultat de la votació inserint vots nous abans que C publiqui la llista de votants al final de l'etapa de reunió.

Amb aquesta notació volem expressar que aquest llistat ha estat signat per l'autoritat corresponent perquè tengui les propietats d'autenticitat i d'integritat (en la notació anterior, el subíndex *A* indica que la signatura l'ha feta una tercera part *A*utoritzada per dur a terme aquesta tasca, que podria coincidir amb alguna de les TTPs que ja intervenen en el protocol). $\Sigma_i ID_i$ denota la seqüència de tots els identificadors dels votants. També hem de suposar que hi ha un acord amb el format i el contingut dels vots. Aleshores això significa que hi haurà d'haver una autoritat que publiqui una llista autenticada amb tots els possibles vots vàlids: $sign_A$('possible votes', $\Sigma_j v_j$), on $\Sigma_j v_j$ denota la seqüència de tots els vots vàlids. La publicació d'aquestes dues llistes és prèvia al protocol de votació i no han estat especificades en el protocol original, per tant les utilitzarem però considerarem els serveis associats a la publicació d'aquestes dues llistes més enllà de l'àmbit estricte del protocol de votació. Així doncs, ni l'*Administrator* ni el *Counter* ofereixen directament cap servei als votants durant l'etapa de *preparació*.

Durant l'etapa d'*administració*, l'*Administrator* signa la butlleta dels votants i retorna la signatura cega sobre aquesta al votant. En aquesta etapa després de la recepció de la petició del votant l'*Administrator* fa les activitats descrites a la figura 7.2.

- Subprotocol d'*administració*:

Inici del subprotocol

► Activitat 1: Després de la recepció de la petició i abans de signar el vot l'*Administrator* comprova si el votant té el dret de votar o no, és a dir, verifica la identitat del votant

If (verificació correcta) **then**

► Activitat 2: Fa el que podem anomenar detecció de sobrevotació. Això vol dir que l'*Administrator* verifica que el votant no hagi demanat la seva signatura sobre la butlleta amb anterioritat

If (verificació correcta) **then**

► Activitat 3: L'*Administrator* comprova la signatura del votant sobre la butlleta cega

If (verificació correcta) **then**

► Activitat 4: Si totes les verificacions són correctes, l'*Administrator* signa el vot i emet la butlleta

► Activitat 5: Al final de l'etapa d'*administració*, l'*Administrator* publica un llistat de tots els votants que han demanat les seva signatura amb les butlletes emeses

Else

STOP

Else

STOP

Else

STOP

Fi del subprotocol /**administració*/*

Figura 7.2. Mapa d'activitats del subprotocol d'a*dministració*

Com en el capítol anterior, a la figura 7.2 hem presentat les operacions de la TTP de forma algorísmica que hem anomenat mapa d'activitats del subprotocol d'a*dministració*. En les etapes de *votació* i de *reunió* el votant recupera la butlleta signada per l'*Administrator* i l'envia al *Counter*. A continuació el *Counter* comprova la signatura sobre la butlleta rebuda a través d'un canal anònim emprant la clau de verificació de l'administrador. El *Counter* fa l'activitat de seguretat descrita a la figura 7.3.

- Subprotocol de *votació i reunió*:

Inici del subprotocol

► Activitat 1: El *Counter* publica un llistat de les butlletes rebudes amb la signatura de l'Administrator

Fi del subprotocol /**votació i reunió*/*

Figura 7.3. Mapa d'activitats dels subprotocols de *votació i reunió*

El votant en les etapes d'*obertura* i de *recompte* envia la seva clau de xifratge a través d'un canal anònim perquè es pugui destapar el seu vot. El *Counter* obre el compromís de cada butlleta i recupera els vots. Aleshores el *Counter* publica els resultats de la votació. Així doncs, podem veure a la figura 7.4 l'activitat de seguretat que fa el *Counter* en aquestes etapes.

- Subprotocol d'*obertura i recompte*:

Inici del subprotocol

► Activitat 1: Després d'obrir cada butlleta, el *Counter* comprova la correcció de cada vot. Llavors anuncia els resultats de la votació

Fi del subprotocol /**obertura i recompte*/*

Figura 7.4. Mapa d'activitats dels subprotocols d'*obertura i recompte*

7.4 Classificació de les activitats de seguretat

Hem segmentat i descrit les operacions que fan les terceres parts de confiança en cada un dels subprotocols o etapes de l'esquema de votació. Hem etiquetat cada una d'aquestes activitats que duen a terme les TTPs i ara volem analitzar-les. El nostre propòsit és descriure nous subprotocols (o introduir petites modificacions a l'esquema original) per poder obtenir uns serveis de seguretat verificables. La verificabilitat de les terceres parts representarà una millora en el sistema i ajudarà els usuaris a dipositar confiança en l'*Administrator* i amb el *Counter*. De fet reduïm la quantitat de confiança que un usuari ha

de posar en les TTPs, ja que si hi ha una disputa sobre una determinada operació de la TTP, aleshores l'usuari tendrà una evidència que podrà mostrar a un jutge i demostrar exactament allò que ha passat i obtenir algun tipus de compensació o rectificació pel greuge que s'ha pogut crear.

Classificarem cada activitat de la TTP com a *verificable* (*on-line* o *off-line*) o *no verificable*. En el cas d'una operació *no verificable*, especificarem un nou subprotocol on puguem tenir un servei verificable. Les noves propostes no modificaran el format original de la butlleta amb l'objectiu que el protocol conservi unes característiques el més semblant possible a l'esquema original (amb l'addició de la verificabilitat). Pel mateix motiu també utilitzarem un canal de comunicació anònim com l'utilitzat a la proposta original en les etapes de *votació* i *obertura*. També farem servir en aquestes etapes el canal de comunicació anònim per recuperar la informació publicada pel *Counter* en un directori públic. Aquesta operació és similar a un accés remot a un fitxer on un usuari es pot connectar a qualsevol estació de treball i accedir i baixar o pujar fitxers públics a través de la xarxa. Podem emprar com a referència de l'accés anònim a un fitxer localitzat en una màquina remota el model FTP descrit a [RFC959].

Per descriure les nostres propostes utilitzarem la notació que ja hem emprat en els anteriors capítols i que hem descrit a l'apartat 6.4. A més, per a aquest protocol que emprar l'enviament d'un missatge de l'usuari X a l'usuari Y mitjançant un canal anònim hem escollit aquesta notació $X \rightarrow_{\text{anonymous}} Y$ per analogia amb Fujioka et al. a [FOO93].

7.4.1 Classificació

Seguint la notació de l'anterior capítol cada activitat de seguretat podrà ser catalogada com a no verificable (*nv*), verificable *on-line* (*v_on*) o verificable *off-line* (*v_off*). Començarem classificant les activitats o unitats funcionals executades per la TTP en el subprotocol d'*administració,* que podem veure a la figura 7.5. A l'etapa d'*administració* la TTP comprova la identitat del votant per saber si té dret a vot o no. No obstant això, l'*Administrator* no enviarà sempre evidències a l'usuari referent a aquesta comprovació i quan rep d_i si el votant no està d'acord amb la decisió adoptada per aquesta entitat respecte del seu dret a vot haurà de revelar quin és el seu vot destapant la butlleta cega amb r_i i així perdrà la confidencialitat del seu vot. Per tant, l'activitat 1 (de la figura 7.5) la classificam globalment com a no verificable.

Referent a l'activitat 2 de la figura 7.5 en de tenir en compte que si l'usuari té el dret de votar, aleshores l'*Administrator* ha de comprovar si el votant ja ha fet anteriorment una petició per demanar la signatura de la TTP sobre una butlleta. Si aquest és el cas, llavors l'*Administrator* rebutjarà la petició. Per poder tenir un servei verificable, el votant ha de tenir alguna evidència sobre la provisió del servei, però a la proposta original la TTP no

envia cap informació sobre això. Per tant, hem de classificar el servei com a no verificable. Després de la petició del votant per aconseguir la signatura sobre el vot, l'*Administrator* comprova la signatura del votant s_i sobre la butlleta cega e_i (activitat 3 de la figura 7.5). La TTP rebutjarà la petició si la signatura no és vàlida. No obstant això, l'*Administrator* no envia cap informació sobre aquesta comprovació a l'usuari si el resultat no és correcte. Consegüentment, el votant no té cap evidència per poder reclamar si no està d'acord amb l'*Administrator*. Com a resultat d'això, hem de classificar aquesta activitat com a no verificable.

- Subprotocol *administració*:
  ► Activitat 1: Recepció de la petició i verificació de la identitat de l'usuari
  If (totes les verificacions són correctes) **then**
  Evidència Rebuda: $d_i = \sigma_A(e_i)$
  Classificació de l'Activitat 1: *v_on*
  Else
  Evidència Rebuda: L'usuari no rebrà evidència en aquest cas
  Classificació de l'Activitat 1: *nv*

  ► Activitat 2: Detecció de sobrevotació
  If (totes les verificacions són correctes) **then**
  Evidència Rebuda: $d_i = \sigma_A(e_i)$
  Classificació de l'Activitat 1: *v_on*
  Else
  Evidència Rebuda: L'usuari no rebrà evidència en aquest cas
  Classificació de l'Activitat 1: *nv*

  ► Activitat 3: Comprovació de la signatura del votant
  If (verificació correcta) **then**
  Evidència Rebuda: $d_i = \sigma_A(e_i)$
  Classificació de l'Activitat 1: *v_on*
  Else
  Evidència Rebuda: L'usuari no rebrà evidència en aquest cas
  Classificació de l'Activitat 1: *nv*

  ► Activitat 4: Signar i emetre la butlleta
  Evidència Rebuda: $d_i = \sigma_A(e_i)$
  Classificació de l'Activitat 1: *v_on*

  ► Activitat 5: Publicació del llistat de butlletes acceptades
  Evidència Rebuda: llistat amb [ID_i, e_i, s_i]
  Classificació de l'Activitat 1: *nv*

Figura 7.5. Classificació de les activitats de la TTP en el subprotocol d'*administració*

Pel que fa a la classificació de l'activitat 4 de la figura 7.5 podem comentar que l'*Administrator* signa el missatge dins del qual hi ha amagat el vot de l'usuari i l'hi envia. Aleshores el votant pot comprovar si la TTP ha donat el servei tal i com el protocol especifica o no. No obstant això i, com ja hem comentat, si utilitza aquest missatge com a evidència (l'ítem d'informació d_i) l'usuari hauria de demostrar que coneix el que s'amaga darrera e_i ja que d_i no està lligat a la seva transacció. Per tant, tot i que es podria arribar a comprovar la correcció d'aquesta activitat, significaria la pèrdua de la confidencialitat del vot, cosa que podríem evitar si lligam tots aquests missatges com a corresponents a una mateixa transacció.

Finalment, pel que fa a l'etapa d'*administració*, la TTP publica una llista que conté el nombre de votants i un llistat amb totes les peticions rebudes de cada votant que demanen la signatura de l'*Administrator* sobre el seu vot (activitat 5). No obstant això, per poder classificar aquest servei com a verificable, la llista publicada hauria de ser autenticable; en cas contrari, qualsevol votant podria manipular-la. Consegüentment, aquesta activitat, tal i com està especificada a la proposta original, no és verificable. A la figura 7.6 hem classificat la l'activitat feta per la TTP durant les etapes o subprotocols de *votació* i de *reunió*. En aquest subprotocols el *Counter* publica una llista que conté totes les butlletes rebudes amb la signatura corresponent de l'administrador. No obstant això, per tal de classificar aquesta activitat com a verificable el llistat ha de ser autenticat; d'altra manera, qualsevol votant podria manipular-lo i, per tant, no podrà ser emprat com a evidència. A més, els votants no tenen cap evidència de no rebuig de recepció del seu parell $[x_i, y_i]$. Així doncs, si un votant no troba la seva butlleta a la llista, no pot reclamar perquè no té cap evidència sobre la recepció de la butlleta per part del *Counter*. Podem concloure que aquesta activitat tal i com ha estat especificada a la proposta original no és verificable.

- Subprotocols de *votació* i *reunió*:
  ► Activitat 1: Verificació i posterior publicació en forma de llistat de les butlletes rebudes
  Evidència Rebuda: L'usuari no rebrà evidència en aquest cas
  Classificació de l'Activitat 1: *nv*

Figura 7.6. Classificació de les activitats de la TTP en el subprotocol de *votació i reunió*

La classificació de l'activitat de seguretat del *Counter* en els subprotocols d'*obertura* i de *recompte* l'hem feta a la figura 7.7.

- Subprotocols d'*obertura* i *recompte*:
  ► Activitat 1: Obertura de les butlletes i publicació de resultats
  Evidència Rebuda: L'usuari no rebrà evidència en aquest cas
  Classificació de l'Activitat 1: *nv*

Figura 7.7. Classificació de les activitats de la TTP en el subprotocol d'*obertura* i *recompte*

En els subprotocols d'*obertura* i *recompte*, després de comprovar que cada vot és correcte, el *Counter* fa públic el resultat de la votació. No obstant això, a l'etapa de *recompte*, la llista de butlletes no està autenticada i, com en el cas anterior, si un votant no troba la seva butlleta a la llista, no pot reclamar perquè no té cap evidència sobre la recepció de la clau de xifratge per part del *Counter*. Per això hem classificat l'activitat de la figura 7.7 com a no verificable.

7.5 Protocol amb la TTP verificable

Seguin la notació general que hem exposat a l'apartat 6.4, en aquesta apartat hi ha exposades les nostres propostes sobre com modificar les etapes de l'esquema de votació electrònica anterior perquè les terceres parts involucrades siguin verificables. En primer lloc, a la figura 7.8, hi hem exposat els nous subprotocols de *preparació* i d'*administració*.

1. V_i: **selecciona un vot (**v_i**)**, de la llista: PR_A('possible votes', $\Sigma_j v_j$).
2. V_i: $x_i = \xi(v_i, k_i)$; $e_i = \chi(x_i, r_i)$; $s_i = \sigma_i(e_i)$ on k_i és una clau escollida aleatòriament i r_i és un nombre aleatori
3. $V_i \rightarrow A$: PR_{Vi}(*tid*, ID_i, e_i, s_i). On *tid* és un identificador de la transacció
4. *A*: **if (**$ID_i \notin PR_A$('list of voters', $\Sigma_i ID_i$)**) then**
   $A \rightarrow V_i$: PR_A(*tid*, 'Reject: ID_i is not a voter')
   else if (ID_i has already voted**) then**
   $A \rightarrow V_i$: PR_A(*tid*, 'Reject: ID_i has already voted', e'_i, s'_i)
   A: **guarda(**PR_{Vi}(*tid*, ID_i, e_i, s_i)**)**
   else if (s_i is not a signature on e_i**) then**
   $A \rightarrow V_i$: PR_A(*tid*, 'Reject: s_i is not a signature on e_i')
   else
   A: $d_i = \sigma_A(e_i)$
   $A \rightarrow V_i$: PR_A (*tid*, d_i)

Al final de l'etapa d'*administració*:

5. *A* : **publishes (**PR_A('list of accepted voters', number of voters, $\Sigma_i(ID_i, e_i, s_i)$**)**

Figura 7.8. Subprotocols de *preparació* i *administració*

El votant V_i selecciona el seu vot de la llista de vots permesos que ha estat signada i publicada per una autoritat. La llista conté tots els possibles vots vàlids. El votant també genera l'identificador de transacció (*tid*) que lligarà tots els missatges relacionats amb el seu procés de votació. Aleshores, el votant construeix el missatge utilitzant la tècnica de signatures cegues i l'envia a l'*Administrator* per aconseguir la seva signatura sobre la butlleta. Al pas quatre l'*Administrator* comprova que el votant té dret a votar i, per això, comprova que la identitat del votant ID_i és a la llista dels votants admesos. Hem suposat

que una autoritat ha publicat prèviament aquest llistat. En el pas 4 de la nostra proposta, si finalment totes les comprovacions que es fan són positives, aleshores la TTP envia un missatge signat a l'usuari amb el mateix identificador de transacció (*tid*). Al final de l'etapa publica un llistat amb les peticions rebudes i signa aquesta informació.

A la figura 7.9 hem fet la nostra proposta per al subprotocols de *votació* i de *reunió*. Amb aquesta solució, com demostrarem més endavant, les operacions de la TTP són verificables. En aquesta figura podem veure que a l'etapa de *votació* cada votant envia el parell (x_i, y_i) al *Counter*. Aleshores, durant cada període de temps Δt, el *Counter* publica les butlletes rebudes durant aquest interval en un directori públic. Qualsevol pot aconseguir aquest llistat i, en cas de problemes de comunicació, qualsevol votant pot saber si el *Counter* ha rebut la seva butlleta o no.

Etapa de *votació*

1. V_i: **comprova la signatura(**d_i, e_i**)**
2. V_i: $y_i = \delta(d_i, r_i)$
3. $V_i \rightarrow_{anonymous}$ C: x_i, y_i
4. C: **cada Δt, publica(***PR_C*(‘received ballots between Δt’, $\Sigma_i(x_i, y_i)$)**)**
5. $V_i \leftarrow_{anonymous}$ C: *PR_C*(‘received ballots between Δt’, $\Sigma_i(x_i, y_i)$)
1. V_i: **if [**$(x_i, y_i) \notin$ *PR_C*(‘received ballots between Δt’, $\Sigma_i(x_i, y_i)$)**] and [**the voting stage isn’t finished**] then go to step 3**

Etapa de *reunió*

1. C: **comprova la signatura** Σ_i**(**y_i, x_i**)**
2. C: **publica(***PR_C*(‘list of accepted ballots’,$\Sigma_i(l_i, x_i, y_i)$)**)**

Figura 7.9. Subprotocols de *votació* i de *reunió*

Per acabar, especificam dues noves etapes de l'esquema de votació electrònica. A la figura 7.10 hi ha els nous subprotocols d'*obertura* i de *recompte*.

Etapa d'*obertura*

1. V_i: **if (**$(y_i, x_i) \in$ *PR_C*(‘list of accepted ballots’,$\Sigma_i(l_i, x_i, y_i)$)**) then**
   $V \rightarrow_{anonymous}$ C: l_i, k_i
2. C: **cada Δt, publica(***PR_C*(‘received keys between Δt’, $\Sigma_i(l_i, k_i)$)**)**
3. $V_i \leftarrow_{anonymous}$ C: *PR_C*(‘received keys between Δt’, $\Sigma_i(l_i, k_i)$)
4. V_i: **if [**$(l_i, k_i) \notin$ *PR_C*(‘received keys between Δt’, $\Sigma_i(l_i, k_i)$)**] and [**deadline**] then go to step 1**

Etapa de *recompte*

1. C: **obre les butlletes(**$\Sigma_i(l_i, x_i, y_i, k_i)$**)**
2. C: **comprova la validesa(**$\Sigma_i v_i$**) i calcula resultats**
3. C: **publica(***PR_C*(‘list of valid ballots’,$\Sigma_i(l_i, x_i, y_i, k_i, v_i)$, results)**)**

Figura 7.10. Subprotocols d'*obertura* i de *recompte*

En les etapes d'*obertura* i de *recompte* de la figura 7.10, cada votant obre el seu vot enviant la seva clau de xifratge k_i a la TTP. Aleshores, cada període de temps Δt, el Counter publica les claus rebudes durant aquest interval de temps en un lloc públic. Com a l'etapa de *votació*, els canals emprats són dels anomenats *resilient*, això significa que qualsevol pot aconseguir aquesta llista pública, fins i tot encara que hi hagi problemes temporals de comunicació i, per tant, qualsevol votant pot saber si la TTP ha rebut la seva clau o no.

7.6 Resolució de disputes

Els subprotocols presentats a l'apartat anterior modifiquen les activitats de seguretat de les TTPs de l'esquema original perquè ara siguin verificables de forma *on-line*. Així, fem el següent enunciat:

***Enunciat*: les terceres parts de confiança involucrades en la nostra proposta de sistema de votació electrònica són verificables perquè totes les activitats que duen a terme són verificables *on-line*.**

A continuació, provarem que efectivament és així per a cada activitat.

Prova 1*: L'activitat 1 dels subprotocols de *preparació* i *administració* és verificable *on-line
***Argumentació*:** El missatge enviat per l'*Administrator* "PR_A(*tid*, 'Reject: ID_i is not a voter')" en aquests subprotocols té la propietat de seguretat de no rebuig d'origen i pot ser utilitzat com a evidència en cas de disputa (per exemple si el votant no està d'acord amb la decisió de l'*Administrator*). D'aquesta manera podem afirmar que l'activitat 1 on la TTP verifica la identitat del votant és verificable de forma *on-line* perquè el votant té evidències suficients per comprovar el resultat de l'operació de la TTP i per aconseguir equitat en un sistema de resolució de disputes extern en cas de no estar-hi d'acord. El votant tendrà ara els següents missatges com a evidències: PR_{Vi}(*tid*, ID_i, e_i, s_i), PR_A(*tid*, 'Reject: ID_i is not a voter'), PR_A('list of voters', $\Sigma_i ID_i$).

Prova 2*: L'activitat 2 dels subprotocols de *preparació* i *administració* és verificable *on-line
***Argumentació*:** D'acord amb la solució proposada a la figura 7.8, l'*Administrator* ha de tenir una base de dades on guardi les peticions acceptades dels votants. Consegüentment, quan la TTP rebi una nova petició, podrà comprovar si el votant que la signa ja n'havia feta una anteriorment. En aquest cas, l'*Administrator* enviarà un missatge signat de rebuig al votant. Els paràmetres e'_i i s'_i del missatge de rebuig han estat localitzats per la TTP a la seva base de dades on hi havia guardada la primera petició del votant, que fou acceptada.

D'aquesta manera, e'_i i s'_i proven que el votant ja havia intentat aconseguir la signatura de la TTP amb anterioritat (s'_i és la signatura del votant sobre la butlleta cega e'_i). Amb aquest protocol, el votant obté evidències sobre l'activitat 2, on la TTP fa la detecció de sobrevotació, i així podem classificar l'actuació de la TTP com a verificable. Les evidències que l'usuari tendrà són: $PR_{Vi}(tid, ID_i, e_i, s_i)$, $PR_A(tid,$ 'Reject: ID_i has already voted', $e'_i, s'_i)$.

Prova 3*: L'activitat 3 dels subprotocols de *preparació* i *administració* és verificable *on-line

***Argumentació*:** De forma semblant a l'activitat 2, l'*Administrator* envia un missatge de rebuig signat per poder donar al votant una evidència sobre l'operació que ha feta (comprovació de la signatura del votant sobre la butlleta cega.). Per tant, l'activitat de la TTP serà ara verificable. Després del pas 4 d'aquest protocol, el votant tendrà les següent evidències sobre l'operació de la tercera part: $PR_A(tid,$ 'Reject: s_i is not a signature on e_i').

Prova 4*: L'activitat 4 dels subprotocols de *preparació* i *administració* és verificable *on-line

***Argumentació*:** Segons els subprotocols proposats a la figura 7.8, si totes les verificacions que fa l'*Administrator* han estat vàlides, llavors aquest ha d'enviar un missatge signat amb el paràmetre d_i. Per poder classificar l'activitat de signatura de la butlleta com a verificable no és suficient enviar d_i, com està especificat a la proposta original [FOO93], perquè el missatge no està lligat a la petició del votant. Per aquesta raó, a la nostra proposta, l'*Administrator* envia el missatge $PR_A(tid, d_i)$ al votant en lloc de d_i. Ara l'activitat és verificable perquè l'usuari té les següents evidències sobre l'operació de la tercera part: $PR_V(tid, ID_i, e_i, s_i)$, $PR_A(tid, d_i)$. Així si d_i no és una signatura bona sobre e_i, el votant té evidències suficients per resoldre la disputa. Hem d'observar que la recepció del missatge $PR_A(tid, d_i)$ significa que no s'haurà enviat cap missatge de rebuig en les anteriors activitats dutes a terme per l'*Administrator*.

Com hem explicat ja a la secció 7.3 d'aquest mateix capítol, el sistema de votació original proposa que el votant ha de comprovar que y_i (el votant recupera y_i de la signatura cega d_i) és una signatura de x_i a l'etapa de *votació*. Si aquesta comprovació falla, el votant haurà de reclamar aquesta falta mostrant que (x_i, y_i) és invàlid. Encara que amb aquestes evidències el votant pogués corregir el problema, perdria la privacitat del seu vot. Per això proposam la comprovació de la signatura cega d_i enlloc de y_i, com es proposa en el sistema original. Aleshores el votant pot reclamar que d_i no és una signatura sobre e_i mostrant les següents evidències: $PR_V(tid, ID_i, e_i, s_i)$, $PR_A(tid, d_i)$ i així l'usuari no perdrà la privacitat perquè ningú no pot lligar la butlleta x_i amb d_i. Consegüentment no serà necessari la comprovació de y_i en l'etapa de *votació* perquè, com a norma general, podem dir que si $S(m)$ és una signatura digital sobre el missatge m, $f()$ és una funció que ens permet ocultar unes dades (usualment basat en un nombre secret aleatori anomenat *blinding factor*) i $g()$ és la funció

inversa de $f()$. Aleshores, la signatura cega està basada en la següent equació: $g(S(f(m))) = S(m)$ (figura 7.11). El protocol de votació durant l'etapa d'*administració* té l'esquema de la figura 7.8.

i. $V \rightarrow A$: $f(m)$
ii. $A \rightarrow V$: $S(f(m))$
iii. V: $g(S(f(m))) = S(m)$

Figura 7.11. Signatura cega

D'aquí podem deduir fàcilment que si $S(f(m))$ és una signatura sobre $f(m)$ aleshores $g(S(f(m)))$ serà una signatura sobre m. Per tant, si l'activitat *Signatura de la Butlleta* s'ha realitzat correctament, significarà que d_i és una signatura sobre e_i i, aleshores podrem deduir que y_i serà una signatura sobre x_i. D'aquesta manera podem concloure que fent verificable aquesta activitat, permetem comprovar que y_i és una signatura sobre x_i i si la comprovació falla, no tendrem necessitat de revelar x_i per corregir la situació.

Prova 5*: L'activitat 5 dels subprotocols de *preparació* i *administració* és verificable *on-line

***Argumentació*:** La llista de butlletes acceptades publicada per l'*Administrator* té molta importància en l'activitat 1 dels subprotocols de *votació i reunió* on el *Counter* publica un llistat de les butlletes rebudes amb la signatura de l'Administrator i que analitzarem després. Per resoldre les queixes dels votants que tenen relació amb aquesta altra activitat, el llistat de votants acceptats ha d'estar autenticat. Per tant, en el pas 5 de l'etapa d'*administració* proposat, la TTP publica la llista signada de tots els votants acceptats. Ara l'activitat serà verificable. Hi ha dues possible reclamacions en relació amb aquest servei:

a) Si un votant, que ha demanat la signatura de la TTP sobre el seu vot, no apareix a la llista, les evidències que té per corregir aquest error en un sistema de resolució de disputes extern són: $PR_V(tid, ID_i, e_i, s_i)$, $PR_A(tid, d_i)$, PR_A('list of accepted voters', number of voters, $\Sigma_i(ID_i, e_i, s_i)$).

b) Si un votant reclama que apareix a la llista, però que ell no ha demanat votar, aleshores, l'evidència que tendrà serà: PR_A('list of accepted voters', number of voters, $\Sigma_i(ID_i, e_i, s_i)$). Certament, qualsevol pot queixar-se que un s_i no és una signatura de ID_i sobre e_i.

Prova 6*: L'activitat 1 dels subprotocols de *votació i reunió* és verificable *on-line

***Argumentació*:** Si seguim la proposta que hem fet a la figura 7.9, qualsevol que tengui una butlleta vàlida (y_i és la signatura sobre x_i) pot reclamar que no és a la llista de butlletes admeses. També, qualsevol pot reclamar que una butlleta no vàlida és en aquesta llista. Per realitzar aquesta queixa els votants no necessitem revelar cap informació

privada, perquè per solucionar la disputa cada votant pot presentar les següents evidències: PR_C('received ballots between Δt', $\Sigma_i(x_i, y_i)$), PR_C('list of accepted ballots',$\Sigma_i(l_i, x_i, y_i)$).

Hi ha alguns problemes de seguretat en aquest servei: el llistat de butlletes acceptades pot tenir més butlletes que votants en el llistat PR_A('list of accepted voters', number of voters, $\Sigma_i(ID_i, e_i, s_i)$). En aquesta situació podem dir que el llistat de butlletes acceptades té un *overflow*. És possible trobar parells duplicats de (x_i, y_i) ja que qualsevol votant pot enviar la seva butlleta dues o més vegades al *Counter*. Fins i tot el mateix *Counter* pot duplicar algun dels vots que ha rebut al final de l'etapa de *reunió*, especialment si ha observat que alguns votants no han enviat el seu vot. Es pot donar el cas que alguns votants no enviïn el seu vot al *Counter* i malgrat tenir alguns vots duplicats la llista no tengui un *overflow*. També hem de tenir en compte la possibilitat que existeix de tenir parells duplicats de forma aleatòria. L'*Administrator* pot generar butlletes vàlides al *Counter* i pot corrompre el procés de votació. Per ventura alguns votants no han enviat el seu vot al Counter i malgrat tenir alguns vots de l'administrador (que no corresponen a cap votant) la llista pot no presentar *overflow*.

Proposam que el *Counter* hagi de publicar el llistat de butlletes acceptades sense cap dels parells (x_i, y_i) que estiguin duplicats. Si un votant no troba el seu vot a la llista perquè el *Counter* l'ha eliminat a causa d'una repetició de la seva butlleta, aleshores pot corregir la situació emprant les evidències que hem concretat per a aquesta activitat. Així doncs, si tots els votants llistats a la llista de votants acceptats envien la seva butlleta al *Counter*, no pot ocórrer cap d'aquests tipus de frau.

Prova 7*: L'activitat 1 dels subprotocols d'*obertura* i de *recompte* és verificable *on-line
***Argumentació*:** Aquest activitat fa referència a la publicació per part del *Counter* del llistat amb les butlletes vàlides juntament amb els resultats de la votació. Segons la proposta de la figura 7.10 qualsevol pot reclamar que la clau rebuda (l_i, k_i) i que apareix al llistat PR_C('received keys between Δt' ,$\Sigma_i(l_i, k_i)$) no apareix en el llistat de butlletes vàlides juntament amb el seu parell (x_i, y_i). Naturalment el parell (x_i, y_i) ha d'estar en el llistat PR_C('list of accepted ballots',$\Sigma_i(l_i, x_i, y_i)$). És clar que qualsevol àrbitre podrà avaluar aquests resultats i podem dir, per tant, que l'activitat de la TTP és verificable. Les evidències que qualsevol votant ha de tenir per resoldre una queixa en relació amb aquesta activitat de seguretat són: PR_C('list of accepted ballots',$\Sigma_i(l_i, x_i, y_i)$), PR_C('received keys between Δt',$\Sigma_i(l_i, k_i)$), PR_C('list of valid ballots',$\Sigma_i(l_i, x_i, y_i, k_i, v_i)$, results), $sign_A$('possible votes', $\Sigma_j v_j$).

Com ja hem dit abans, el canal de comunicació entre la TTP i els votants és *resilient*; això significa que, si la clau d'un votant no apareix a cap de les llistes publicades del tipus

PR_C('received keys between Δt', $\Sigma_i(l_i, k_i)$) després d'haver-la enviat a la TTP repetides vegades, podrem dir que el *Counter* nega aquest servei al votant. Ara bé, hem de dir que la negació de servei és un tema que està fora de l'estudi d'aquesta tesi.

***Resultat*:** D'acord amb les proves 1, 2, 3, 4, 5, 6 i 7 que acabam de presentar i les seves argumentacions, les terceres parts de confiança involucrades en el sistema de votació electrònica que hem proposat són verificables ja que totes les activitats que duen a terme són verificables *on-line*.

Independentment d'això, volem indicar que abans hem suposat que l'*Administrator* i els usuaris tenen dos esquemes de signatura diferents. En realitat només necessiten un criptosistema però n'hem emprat dos perquè no hem volgut modificar cap dels missatges proposats a l'esquema de votació original. Ara bé, a mode d'exemple, si només utilitzàssim un sol criptosistema, el pas 4 de la proposta feta a la secció 7.8 (subprotocols de *preparació* i *administració*) quedaria com mostra la figura 7.12.

4. A: **if (**$ID_i \notin PR_A$('list of voters', $\Sigma_i ID_i$)**) then**
   A $\rightarrow V_i$: PR_A(tid, 'Reject: ID_i is not a voter')
   else
   if (ID_i has already voted**) then**
   A $\rightarrow V_i$: PR_A(tid, 'Reject: ID_i has already voted', e'_i, s'_i)
   A: **guarda(**PR_{Vi}(tid, ID_i, e_i, s_i)**)**
   else
   if (s_i is not a signature on e_i**) then**
   A $\rightarrow V_i$: PR_A(tid, 'Reject: s_i is not a signature on e_i')
   else
   A: $d_i = \sigma_A(e_i)$
   A $\rightarrow V_i$: σ_A (tid, d_i)

Figura 7.12. Modificació del subprotocol d'*administració*

7.6 Conclusions

En aquest capítol hem vist com podem convertir uns serveis proporcionats per TTPs *no verificables* en serveis *verificables on-line*. L'objectiu de l'obtenció de serveis d'aquest tipus és proporcionar evidències als usuaris del sistema sobre el funcionament de la TTP en el protocol. Per això hem seguit l'esquema del capítol anterior i hem descrit i classificat cada una de les accions dutes a terme per les TTP per proveir els serveis als usuaris (en aquest cas, els votants). Ens sembla que és una manera prou exhaustiva de presentar les operacions que fan les terceres parts de cara a l'usuari i d'aquesta manera assegurar la verificabilitat de cada una d'elles i per extensió de les terceres parts de confiança.

Hem identificat tots els serveis de les TTPs en un esquema de votació electrònica. Després, hem modificat la proposta original augmentant la seguretat del sistema de tal manera que els usuaris han vist millorada la seva confiança en les TTPs perquè obtenen evidències de cada una de les operacions que es fan per donar-li el servei. Les evidències demostren allò que realment ha passat durant l'execució del protocol.

En el capítol anterior veiem que el problema de la verificabilitat de les TTP provenia especialment de dues fonts: la informació que internament manipula la TTP i de la qual depèn alguna de les respostes que rep l'usuari i la manca de lligam entre els distints missatges d'una mateixa transacció. A continuació concretarem més les fonts d'aquest problema. Analitzant les activitats que duen a terme les TTPs vèiem que hi ha tres tipus d'operacions genèriques que provoquen les situacions de no verificabilitat:

- L'enviament de missatges o peticions de l'usuari a la TTP i que el protocol no assegura que quedarà constància d'aquest fet. Aleshores la TTP pot actuar de forma incorrecta al·legant la no recepció de les dades, sense que es pugui provar si això és cert o no ho és. Aquests tipus de problemes, els podem veure tant en el subprotocol de *votació* analitzat en aquest capítol com en el protocol diners electrònics del capítol anterior. Aquest és el cas de l'activitat de recepció de butlletes (activitat 1 de la figura 7.6) feta pel *Counter* en el subprotocol de *votació* o l'operació de reintegrament feta pel banc en el sistema de diners electrònics (activitat 3 de la figura 6.8) que no dóna constància de l'actualització del saldo a l'usuari.
- L'emissió de missatges per part de la TTP dels quals el protocol no assegura el no rebuig d'origen o que no estan enllaçats amb els altres missatges de la mateixa transacció. Un cas clar d'aquest tipus de situacions és l'operació de signatura de la butlleta que realitza l'*Administrator* en l'etapa d'*administració* del protocol de votació (activitat 4 de la figura 7.5). De forma semblant l'activitat de generació feta pel banc emissor al protocol analitzat en el capítol anterior (activitat 2 de la figura 6.8) no és tampoc verificable.
- La dificultat que tenen els usuaris per comprovar algunes de les respostes de la TTP que estan en funció de dades que aquesta entitat té emmagatzemades. Per exemple, la detecció de sobrevotació (activitat 2 de la figura 7.5) és representada en forma de resposta de l'*Administrator* en funció d'anteriors peticions dels usuaris que la TTP ha guardat a la seva base de dades. En el sistema de diners electrònics analitzat al capítol anterior podem veure aquest tipus d'operacions en activitats com la detecció de doble dipòsit (activitat 3 de la figura 6.10) i la detecció de reutilització (activitat 4 de la figura 6.10).

En el següent capítol aplicarem d'una forma sistemàtica les solucions trobades per a cada un d'aquests tipus d'operacions dins l'àmbit d'un altre tipus de protocol de seguretat. D'aquesta manera explicarem com podem trobar i comprovar una pauta general per convertir un tercera part no verificable en verificable a través de la descripció de les operacions que realitza de cara a l'usuari per donar-li servei.

Capítol 8

Verificabilitat en un protocol d'intercanvi equitatiu

8.1 Introducció

En aquest capítol, millorarem la confiança dels usuaris sobre el fet d'invocar una TTP durant l'execució d'un protocol d'intercanvi equitatiu de valors. La recerca s'ha centrat a veure quines són les situacions en les quals un error de la tercera part (intencionat o no) romp la seguretat de l'intercanvi sense que els usuaris tenguin cap eina per arreglar aquesta possible falla en la seguretat del protocol.

Estudiarem aquest punt en un protocol d'intercanvi equitatiu concret i posteriorment veurem com podem introduir la propietat de verificabilitat de la TTP en el protocol, tal com hem fet per altres tipus de protocols en anteriors capítols. Així doncs, modificarem el protocol originalment proposat de tal manera que els usuaris tenguin evidència de les accions de la TTP. Així, les activitats de seguretat seran verificables *on-line* i, en cas de disputa, les evidències podran usar-se per aconseguir l'equitat de l'intercanvi a través d'un sistema de resolució de disputes (per exemple en un tribunal de justícia).

Les noves propostes introduiran relativament pocs canvis respecte a l'esquema original perquè la TTP faci les mateixes activitats de seguretat per donar servei als usuaris. No obstant això, les activitats de seguretat seran dutes a terme de forma diferent per tal d'aconseguir la verificabilitat de la TTP.

En aquest capítol estudiam un conegut protocol de correu electrònic certificat [ZDB99], on l'intercanvi d'un missatge i una evidència de no rebuig d'origen per una evidència de no rebuig de recepció han de ser equitatius. La solució més eficient per a aquests tipus de protocols és l'anomenat enfocament *optimista,* on una tercera part de confiança només intervé en el protocol en cas d'excepció per garantir l'equitat de l'intercanvi. Cal destacar que els serveis de no rebuig són usats fonamentalment en els sistemes de transmissió de

missatges (com és el cas dels protocols de correu electrònic certificat) i en el comerç electrònic.

Volem destacar especialment l'ús de dos serveis de no rebuig:

- *No rebuig d'origen*: proporciona al receptor d'un missatge l'evidència de l'origen del mateix que el protegirà contra qualsevol intent de l'emissor de negar en fals haver emès el missatge.
- *No rebuig de recepció*: proporciona a l'emissor d'un missatge l'evidència de recepció del mateix que el protegirà contra qualsevol intent del receptor de negar en fals haver rebut el missatge.

Utilitzam també aquest serveis per aconseguir la verificabilitat de la tercera part. Així doncs, els protocols hauran de generar evidències per garantir aquests serveis i, en cas de disputa, un àrbitre (per exemple un jutge) ha de poder avaluar les evidències i prendre una decisió a favor d'una o altra part sense cap tipus d'ambigüitat.

8.2 Propietats

La introducció de la propietat de verificabilitat en un protocol d'intercanvi equitatiu de valors tendrà com a conseqüència que les activitats de seguretat de la TTP seran verificables, això vol dir que els usuaris tendran evidència de l'operació duta a terme per la TTP quan dóna servei a la petició que ells han fet. En el cas que l'usuari pensi que l'intercanvi no ha estat equitatiu (això és, no ha rebut de l'altra part els ítems d'informació que li correspondrien), pot utilitzar les evidències per demostrar l'incompliment dels serveis de seguretat.

Incorporarem en el protocol el concepte de *verificabilitat on-line* i *off-line* com hem definit i explicat en el capítol 5. Així doncs, quan analitzem les operacions de la TTP dins el protocol, podrem classificar cada activitat de seguretat com a no verificable, verificable *on-line* o verificable *off-line*. Tal i com es desprèn de les definicions aportades en el capítol 5, el nostre objectiu, com en els dos capítols anteriors, serà la introducció en el protocol de les modificacions necessàries perquè la verificabilitat de les operacions de la TTP sigui *on-line*.

Aquest objectiu ens obligarà a definir protocols on les terceres parts emeten evidències sobre les activitats que duen a terme. No obstant això, si un usuari no rep les evidències relacionades amb algun servei, és difícil determinar la raó per la qual no les ha rebut. L'usuari pot pensar que no ho ha rebut perquè la TTP no ha actuat correctament, però potser el motiu és que la TTP i/o l'usuari són víctimes d'un atac de negació del servei

(DoS - *Denial of Service*). A causa de la naturalesa dels atacs DoS, és difícil trobar-li una solució; per tant continuarà probablement havent-hi atractives i efectives formes de realitzar atacs que intenten deteriorar o prevenir l'ús legítim d'un ordinador o dels recursos d'una xarxa.

Independentment de la diligència, esforços o recursos utilitzats en contra dels intrusos, els sistemes interconnectats estan davant d'una consistent i real amenaça d'atac DoS a causa bàsicament a dues característiques d'Internet [HW01]:

- Internet està formada per un conjunt de recursos limitats i consumibles.
- La seguretat a Internet és altament interdependent.

En definitiva, les nostres propostes no van encaminades a prevenir el deteriorament o els problemes d'ús de qualsevol dels recursos d'una xarxa, sinó que exclusivament pretén donar més confiança als usuaris sobre l'ús de terceres parts de confiança en els protocols de seguretat. Això significa la inclusió d'una nova propietat de seguretat en els protocols, cosa que donarà la possibilitat als usuaris de verificar l'actuació de la TTP emmarcada dins d'una correcta execució del protocol esmentat.

Missatge de l'usuari A enviat a l'usuari B	M
Xifrat simètric de m amb la clau k	$c = E_K(m)$
Etiqueta per identificar l'execució d'un protocol	$l = h(m, k)$
Etiqueta que identifica el propòsit del missatge	F
Evidència d'origen de c	$EOO = PR_A(f_{EOO}, B, TTP, l, h(c))$
Evidència de recepció de c	$EOR = PR_B(f_{EOR}, B, TTP, l, h(c))$
Evidència d'origen de k	$EOO_k = PR_A(f_{EOOk}, B, l, k)$
Evidència de recepció de k	$EOR_k = PR_B(f_{EORk}, A, l, k)$
Evidència de transmissió de k a la TTP	$Sub = PR_A(f_{Sub}, B, l, E_{TTP}(k))$
Sol·licitud de cancel·lació del protocol	$Abort = PR_A(f_{Abort}, B, l)$
Evidència de cancel·lació del protocol	$Con_a = PR_{TTP}(f_{Con\text{-}a}, A, B, l)$
Evidència de confirmació de k	$Con_k = PR_{TTP}(f_{Con\text{-}k}, A, B, l, k)$
Reconeixement de X de la seva participació en l'intercanvi d'informació amb Y	$Rec_X = PR_X(f_{Rec\text{-}X}, Y, l)$

Figura 8.1. Notació

8.3 Protocol d'intercanvi equitatiu

Un dels protocols més complets d'intercanvi equitatiu va ser proposat simultàniament per Zhou et al. en [ZDB99] i Kremer et al. en [KM00]. És un protocol optimista que compleix la propietat d'*equitat*[11] i *timeliness*[12] sense haver de comptar amb un canal que els autors defineixen a [KM00] com a *operacional*; és a dir, que assegura al receptor l'arribada de les dades emeses en un interval de temps determinat i conegut. És suficient per la seguretat del protocol tenir un canal *resilient*: la informació es pot retardar però sempre arriba al seu receptor després d'un interval finit de temps. Tot i mantenir elements de la notació de les propostes originals dels protocols, tant per descriure el protocol original com les nostres propostes utilitzarem la notació que ja hem emprat en els anteriors capítols i que vàrem descriure a l'apartat 6.4. A la figura 8.1 presentam la notació específica emprada en la definició dels diferents subprotocols que conformen aquesta proposta. En la descripció dels protocols hem utilitzat X i Y per indicar que tant l'usuari A com B poden realitzar l'operació especificada; és a dir, X i Y tant poden representar a A com a B. El subprotocol *bàsic* proposat en [ZDB99] i [KM00] té la forma de la figura 8.2.

1. A→ B: f_{EOO}, f_{Sub}, B, TTP, l, c, $E_{TTP}(k)$, EOO, *Sub*
2. B→ A: f_{EOR}, A, TTP, l, EOR
3. A→ B: f_{EOOk}, B, l, k, EOO_k
4. B→ A: f_{EORk}, A, l, EOR_k

Figura 8.2. Subprotocol *bàsic*

En cas de problemes, A té la possibilitat d'executar el subprotocol *abort* si no rep el missatge 2. El subprotocol *abort* és el de la figura 8.3.

1. A→ TTP: f_{Abort}, l, B, *Abort*

if *aborted* **or** *recovered* **then STOP**
else *aborted* = *true*

2. TTP→ A: $f_{Con\text{-}a}$, A, B, l, Con_a
3. TTP→ B: $f_{Con\text{-}a}$, A, B, l, Con_a

Figura 8.3. Subprotocol *abort*

[11] *Equitat* és la propietat que assegura que al final del protocol o l'emissor del missatge *m* ha obtengut l'evidència de no rebuig del missatge i el receptor té el corresponent missatge *m* així com l'evidència de no rebuig d'origen d'aquest missatge, o cap d'ells ha aconseguit cap informació de vàlua durant l'intercanvi.

[12] Un protocol de no rebuig proporciona *timeliness* si i només si totes les parts honestes sempre poden arribar, en un període finit de temps, a un punt del protocol on el poden aturar i preservar la propietat d'*equitat* de l'intercanvi.

En cas d'excepció A i B tenen l'opció d'executar el subprotocol *recovery* de la figura 8.4.

1. X→ TTP: $f_{Rec\text{-}X}$, f_{Sub}, Y, l, $h(c)$, $E_{TTP}(k)$, Rec_X, *Sub*, EOR, EOO
if *aborted* **or** *recovered* **then STOP**
else *recovered* = *true*
    2. TTP→ A: $f_{Con\text{-}k}$, A, B, l, k, Con_k, EOR
    3. TTP→ B: $f_{Con\text{-}k}$, A, B, l, k, Con_k

Figura 8.4. Subprotocol *recovery*

El protocol és equitatiu ja que si A no rep el missatge del segon pas del subprotocol *bàsic* i B no ha executat el subprotocol *recovery*, l'usuari A només podrà obtenir la cancel·lació de l'intercanvi a través del subprotocol *abort* (que també serà notificada a B). Els altres recorreguts possibles del protocol acaben amb l'obtenció d'una evidència de no rebuig de recepció (EOR, EOR_k o Con_k) i una de no rebuig d'origen (EOO, EOO_k o Con_k) ja sigui a través del subprotocol *bàsic* o del subprotocol *recovery*.

8.4 Operacions de la TTP

Ara descriurem quines són les activitats que duu a terme la TTP per donar servei a les peticions que rep dels usuaris. Un cop haguem fet això podrem classificar-les i després veurem quines són les modificacions que proposam sobre el protocol original per aconseguir que aquestes activitats siguin *verificables on-line*.

- Subprotocol *abort*:

Inici del subprotocol
    ► Activitat 1: Recepció i verificació de la informació de la petició de l'usuari (e.g. verificació de la signatura en el missatge *Abort*)
    If (verificació correcta) **then**
        ► Activitat 2: Comprovar l'estat de l'intercanvi (*aborted* o *recovered*)
        If (*aborted* **or** *recovered*) **then**
            STOP
        Else
            ► Activitat 3: Actualitzar l'estat de l'intercanvi (*aborted* = *true*)
            ► Activitat 4: Generar i enviar el *token* de cancel·lació (Con_a)
    Else
        STOP
Fi del subprotocol /**abort*/

Figura 8.5. Mapa d'activitats del subprotocol *abort*

8.4.1 Mapa d'activitats de seguretat

Les accions que duu a terme la TTP en el protocol dependran del tipus de petició rebuda i de l'estat de cada transacció en particular. Aleshores, com en els capítols anteriors, presentarem les operacions de la TTP de forma algorísmica. Així doncs, les dues figures següents descriuen el mapa d'activitats de seguretat de la TTP. A l'esquema enumeram cada activitat i la descrivim amb una breu frase. És important veure que determinades activitats només s'executaran en funció del resultat de determinades comprovacions. Les activitats de seguretat que pot dur a terme una TTP en el subprotocol *abort* són les de la figura 8.5. Les del subprotocol *recovery* estan descrites a la figura 8.6.

- Subprotocol *recovery*:

Inici del subprotocol
► Activitat 1: Verificació de la informació de la petició de l'usuari
If (verificació correcta) **then**
► Activitat 2: Comprovar l'estat de l'intercanvi
If (*aborted* **or** *recovered*) **then**
STOP
Else
► Activitat 3: Actualitzar l'estat de l'intercanvi (*recovered* = *true*)
► Activitat 4: Generar i enviar el *token* de no rebuig (Con_k).
Else
STOP
Fi del subprotocol /**recovery*/*

Figura 8.6. Mapa d'activitats del subprotocol *recovery*

8.4.2 Classificació de les activitats de seguretat

Com acabam de veure, la TTP pot realitzar fins a vuit activitats. Les activitats de seguretat que dugui a terme la TTP estaran en funció del tipus de petició rebuda (si una petició és per al subprotocol *abort* o per al *recovery*) i de l'estat en què es trobi cada intercanvi en particular. Ara classificarem les activitats en funció de les evidències que pot rebre l'usuari relatives a aquesta operació. Cada activitat de seguretat la classificam entre els tres valors diferents: no verificable (*nv*), verificable *on-line* (*v_on*) i verificable *off-line* (*v_off*). Així, a les figures 8.7 i 8.8 indicam la classificació de les diferents activitats; aprofitam els esquemes de la secció anterior per mostrar les evidències que els usuaris poden obtenir de la TTP en cada una de les activitats, depenent de cada possible execució del protocol. La classificació de cada activitat està feta en funció d'aquestes evidències. A la figura 8.7 exposam aquesta informació ordenada per activitats; les diferents classificacions de cada activitat s'expressen dins l'algorisme (fet en pseudocodi), que indica les possibles execucions del protocol i les evidències rebudes sobre una determinada activitat.

- Subprotocol *abort*:

► Activitat 1: Verificació de la informació de la petició de l'usuari

If (verificació correcta) **then**

If (*aborted* **or** *recovered*) **then**

Evidència rebuda: L'usuari no rebrà evidència en aquest cas

Classificació de l'Activitat 1: *nv*

Else

Evidència rebuda: Con_a

Classificació de l'Activitat 1: *v_on*

Else

Evidència rebuda: L'usuari no rebrà evidència en aquest cas

Classificació de l'Activitat 1: *nv*

► Activitat 2: Comprovar l'estat del protocol

If (*aborted* **or** *recovered*) **then**

Evidència rebuda: L'usuari no rebrà evidència en aquest cas

Classificació de l'Activitat 2: *nv*

Else

Evidència rebuda: Con_a

Classificació de l'Activitat 2: *v_on*

En la classificació de l'activitat 2 cal indicar que, si la transacció no es troba en estat *aborted* o *recovered*, hem considerat que si l'usuari A rep Con_a sabrà amb tota seguretat si la TTP ha actuat correctament o no (classificam l'activitat com a verificable *on-line*). Si el protocol estàs en estat *aborted* o *recovered*, l'usuari A ja tendria en el seu poder un *token* Con_a o Con_k. Amb la qual cosa podria demostrar que l'actuació de la TTP no ha estat correcta. Si la transacció ja estava en estat *aborted*, l'actuació incorrecta de la TTP no tendria cap conseqüència. En la mateixa situació es troba l'Activitat 2 del subprotocol *recovery*.

► Activitat 3: Actualitzar l'estat de la transacció

Evidència rebuda: Con_a

Classificació de l'Activitat 3: *v_off*

► Activitat 4: L'activitat de generar i enviar el *token* de cancel·lació va dirigida als dos usuaris, per tant podrà tenir una classificació per a A i una altra per a B

- Classificació per a A:
  - Evidència rebuda: Con_a
  - Classificació de l'Activitat 4: *v_on*
- Classificació per a B:
  - Evidència rebuda: Con_a
  - Classificació de l'Activitat 4: *v_off*

L'activitat número 4 és *verificable off-line* per a B ja que disposarà d'una evidència i en cas de disputa podrà provar que la TTP el va informar que la transacció que tenia amb A es va cancel·lar. En canvi, quan B rep aquesta evidència no pot estar segur que la TTP ha actuat correctament ja que no té evidència que l'emissió de l'ítem Con_a respongui a una petició de l'usuari A. La classificació de l'activitat 4 del subprotocol *recovery* respon al mateix criteri.

Figura 8.7. Classificació de les activitats de la TTP en el subprotocol *abort*

A la figura 8.8 classificam les activitats de seguretat de la TTP en el subprotocol *recovery*.

- Subprotocol *recovery*:
  - ► Activitat 1: Verificació de la informació de la petició de l'usuari
    If (verificació correcta) **then**
    If (*aborted* **or** *recovered*) **then**
    Evidència rebuda: L'usuari no rebrà evidència en aquest cas
    Classificació de l'Activitat 1: *nv*
    Else
    Evidència rebuda: Con_k
    Classificació de l'Activitat 1: *v_on*
    Else
    Evidència rebuda: L'usuari no rebrà evidència en aquest cas
    Classificació de l'Activitat 1: *nv*
  - ► Activitat 2: Comprovar l'estat del protocol per a una transacció
    If (*aborted* **or** *recovered*) **then**
    Evidència rebuda: L'usuari no rebrà evidència en aquest cas
    Classificació de l'Activitat 2: *nv*
    Else
    Evidència rebuda: Con_k
    Classificació de l'Activitat 2: *v_on*
  - ► Activitat 3: Actualitzar l'estat de la transacció (recovered = true)
    Evidència rebuda: Con_k
    Classificació de l'Activitat 3: *v_off*
  - ► Activitat 4: Generar i enviar el *token* de no rebuig (Con_k)
    - Classificació per a X:
      Evidència rebuda: Con_a
      Classificació de l'Activitat 4: *v_on*
    - Classificació per a Y:
      Evidència rebuda: Con_a
      Classificació de l'Activitat 4: *v_off*

  Essent X l'usuari que ha iniciat el subprotocol *recovery* i Y l'altre usuari.

Figura 8.8. Classificació de les activitats de la TTP en el subprotocol *recovery*

Queda clar que algunes activitats no poden classificar-se de forma única, sinó que la seva classificació depèn de cada execució del protocol. Per exemple, l'Activitat 2 del subprotocol *abort* la classifiquem com a *no verificable* si la transacció es troba en estat *aborted* o *recovered*, ja que l'usuari A no obtendrà cap evidència de l'operació de la TTP. En canvi, la mateixa activitat pot classificar-se com a *verificable on-line* si la transacció

no es troba en cap d'aquests dos estats, ja que obtendrà Con_a i sabrà immediatament si l'operació de la TTP ha estat correcta o no.

8.5 Protocol amb la TTP verificable

Dedicam aquesta secció a la proposta de dos nous subprotocols *abort* i *recovery* on podrem comprovar que la TTP involucrada és verificable. Els nous subprotocols estan basats en els subprotocols originals que acabam de veure amb la intenció que tenguin característiques semblants però afegint la propietat de verificabilitat de la tercera part. Els subprotocols són els de la figura 8.9.

- Subprotocol *abort*:
  1. A→ TTP: f_{Abort}, l, B, *Abort*
  if (dades de la petició incorrectes**) then**
  2. TTP→ A: f_{error}, PR_{TTP}(*Abort*, 'dades incorrectes')
  else
  if *recovered* **then**
  2. TTP→ A: f_{error}, PR_{TTP}(A, B, l, 'estat del protocol: *recovered*')
  else
  2. TTP: ***publicar*****(**$f_{Con\text{-}a}$, A, B, l, Con_a**)**
  3. TTP→ A, B: f_{notf}, PR_{TTP}(A, B, l, 'estat del protocol: *aborted*')
  4. TTP↔ A, B: $f_{Con\text{-}a}$, A, B, l, Con_a

- Subprotocol *recovery*:
  1. X→ TTP: $f_{Rec\text{-}X}$, f_{Sub}, Y, l, $h(c)$, $E_{TTP}(k)$, Rec_X, *Sub*, EOR, EOO
  if (dades de la petició incorrectes**) then**
  2. TTP→ X: f_{error}, $PR_{TTP}(E_{TTP}(k), Rec_X, Sub, EOR, EOO,$ 'dades incorrectes')
  else
  if *aborted* **then**
  2. TTP→ X: f_{error}, PR_{TTP}(A, B, l, 'estat del protocol: *aborted*')
  else
  2. TTP: ***publicar*****(**$f_{Con\text{-}k}$, A, B, l, k, Con_k, EOR**)**
  3. TTP→ A, B: f_{notf}, PR_{TTP}(A, B, l, 'estat del protocol: *recovered*')
  4. TTP↔ A, B: $f_{Con\text{-}k}$, A, B, l, k, Con_k, EOR

Figura 8.9. Subprotocols *abort* i *recovery* amb TTP verificable

Per a aquests nous subprotocols, hem modificat l'especificació de la figura 8.1 dels missatges Con_a i Con_k, ara tenen el format següent:

- $Con_a = PR_{TTP}(f_{Con\text{-}a}, A, B, l, Abort)$

- $Con_k = PR_{TTP}(f_{Con\text{-}k}, A, B, l, k, Rec_X)$

Cada un dels elements que conformen aquests dos missatges són els mateixos que hem descrit a la figura 8.1. L'operació ***publicar*()** significa posar les evidències a disposició dels usuaris en un directori públic en què només es permet l'operació de lectura. La notificació realitzada per la TTP en el pas 3 de cada subprotocol és opcional ja que podríem suposar que passat un cert interval de temps els usuaris poden consultar si l'evidència s'ha publicat i després descarregar-la.

8.6 Resolució de disputes

Enunciat*: La tercera part de confiança involucrada en els subprotocols *abort* i *recovery* definits a l'anterior secció és verificable ja que les evidències que proporciona donen a totes les seves activitats la propietat de *verificabilitat on-line

Per provar que la TTP és verificable, demostrarem que els participants (tant A com B), en cas de disputa, obtenen evidències a través del protocol que poden presentar a un àrbitre i provar com ha estat l'actuació de la TTP. El primer cas de disputa ocorre si B es queixa d'haver-se compromès a rebre la clau *k* del criptograma *c* juntament amb una evidència de no rebuig d'origen i la TTP no li dóna una resposta satisfactòria. El segon cas succeeix si A es queixa d'haver enviat la petició pertinent a la TTP, però no ha pogut completar correctament l'evidència de no rebuig de recepció. Les disputes poden ser resoltes per un àrbitre independent que avaluarà les evidències proporcionades pels participants.

Inicialment, l'àrbitre comprovarà que les parts volen fer l'intercanvi mitjançant la verificació que EOO és una signatura d'A sobre aquesta evidència, fet que indica la seva intenció de realitzar l'intercanvi, i també comprovarà el compromís de B (comprovant la signatura sobre l'evidència EOR). Després, podrà verificar cada una de les activitats de la TTP i determinar el resultat de la disputa. Provarem, en funció de cada una de les dues disputes possibles, que aquestes activitats de la TTP són verificables *on-line*.

El primer cas de disputa ocorre si B es queixa que no ha pogut completar l'intercanvi; aleshores l'àrbitre li requereix que proporcioni les següents evidències:

- $f_{Rec\text{-}X}$, f_{Sub}, A, l, $h(c)$, $E_{TTP}(k)$, Rec_X, *Sub*, EOR, EOO i, a més, alguna de les evidències següents:
- $PR_{TTP}(E_{TTP}(k), Rec_X, Sub, EOR, EOO,$ 'dades incorrectes') o bé
- $PR_{TTP}(A, B, l,$ 'estat del protocol: *aborted*') i Con_a o bé
- $PR_{TTP}(A, B, l,$ 'estat del protocol: *recovered*') i Con_k

Prova 1*: L'activitat 1 del subprotocol *recovery*, quan B és l'usuari implicat, és verificable *on-line
***Argumentació*:** L'activitat 1 consisteix en la verificació de la informació de la petició de l'usuari. Si B aporta $PR_{TTP}(E_{TTP}(k), Rec_X, Sub$, EOR, EOO, 'dades incorrectes') el jutge podrà saber si la TTP ha actuat correctament o no ja que es poden verificar totes les informacions. Si la TTP no ha respost correctament a la petició de B, aleshores el jutge ha d'obligar a la TTP a processar aquesta petició correctament. Hem d'observar que aquesta activitat de seguretat és verificable *on-line* ja que B ha pogut comprovar abans la resposta de la TTP i, en cas de no estar-hi d'acord, ha pogut anar a un àrbitre perquè resolgui la disputa.

Prova 2*: L'activitat 2 del subprotocol de *recovery*, quan B és l'usuari implicat, és verificable *on-line
***Argumentació*:** Mitjançant l'activitat 2 la TTP comprova l'estat del protocol per a una determinada transacció. Aleshores, B pot rebre dos missatges de la TTP relatius a aquesta activitat. Si rep PR_{TTP}(A, B, *l*, 'estat del protocol: *aborted'*), aleshores la TTP ha d'haver publicat un Con_a correcte. Si no és així, l'àrbitre ha d'obligar la TTP a actuar correctament. En canvi, si B rep PR_{TTP}(A, B, *l*, 'estat del protocol: *recovered'*) però no pot obtenir un Con_k correcte; aleshores també serà evident per a l'àrbitre que la TTP no ha actuat bé i, conseqüentment ha de rectificar. Està clar que la publicació de Con_a i Con_k comporta que l'activitat 2 relativa a l'estat en què es troba el protocol és verificable *on-line* ja que l'usuari pot verificar la resposta de la TTP i contrastar-la amb l'estat de la transacció publicat.

Prova 3*: Les activitats 3 i 4 del subprotocol de *recovery*, quan B és l'usuari implicat, són verificables *on-line
***Argumentació*:** En aquestes activitat la TTP actualitza l'estat i envia el *token* de no rebuig. Amb les evidències aportades per l'usuari, el jutge pot comprovar si està publicat de forma correcta l'estat d'*aborted* o *recovered* de la transacció (Con_a o Con_k publicats i que tenguin el format correcte). En cas contrari la TTP haurà de rectificar.

El segon cas de disputa ocorre si A es queixa que no ha pogut cancel·lar o completar l'intercanvi; en cas de cancel·lació A ha de presentar les següents evidències a l'àrbitre:

- *Abort* EOO i a més alguna de les evidències següents:
  - PR_{TTP}(*Abort*, 'dades incorrectes') o bé
  - PR_{TTP}(A, B, *l*, 'estat del protocol: *aborted'*) i Con_a

En cas de voler completar l'evidència de no rebuig de recepció presentarà:

- $f_{Rec\text{-}X}$, f_{Sub}, A, l, $h(c)$, $E_{TTP}(k)$, Rec_X, *Sub*, EOR, EOO i a més alguna de les evidències següents:
  - $PR_{TTP}(E_{TTP}(k), Rec_X, Sub$, EOR, EOO, 'dades incorrectes') o bé
  - PR_{TTP}(A, B, l, 'estat del protocol: *recovered'*) i Con_k

Els passos o comprovacions que ha de fer l'àrbitre són els següents:

Prova 4*: L'activitat 1 dels subprotocols *abort* i *recovery*, quan A és l'usuari implicat, és verificable *on-line
***Argumentació*:** L'activitat 1 és la verificació de la petició de l'usuari en qualsevol dels subprotocols. Si A aporta tant PR_{TTP}(*Abort*, 'dades incorrectes') com $PR_{TTP}(E_{TTP}(k), Rec_X, Sub$, EOR, EOO, 'dades incorrectes') l'àrbitre òbviament podrà saber si la TTP va actuar correctament. Amb aquestes proves, si la TTP no ha seguit correctament el protocol, l'àrbitre l'haurà d'obligar la tercera part a corregir la seva actuació.

Prova 5*: L'activitat 2 dels subprotocols *abort* i *recovery*, quan A és l'usuari implicat, és verificable *on-line
***Argumentació*:** Durant l'activitat 2, tant en el subprotocol *abort* com *recovery*, la TTP comprova l'estat d'una transacció particular. En funció del resultat de la verificació de l'estat de la transacció, A rebrà PR_{TTP}(A, B, l, 'estat del protocol: *aborted'*) o PR_{TTP}(A, B, l, 'estat del protocol: *recovered'*), per tant, la TTP es veurà obligada a actuar correctament davant d'aquestes evidències.

Prova 6*: Les activitats 3 i 4 dels subprotocols *abort* i *recovery*, quan A és l'usuari implicat, són verificables *on-line
***Argumentació*:** Les Activitats 3 i 4 d'aquests subprotocols són l'actualització de l'estat de la transacció i l'enviament del *token* corresponent. L'àrbitre pot comprovar si s'ha publicat de forma correcta l'estat d'*aborted* o *recovered* de la transacció en qüestió (Con_a o Con_k publicats i amb el format correcte). En cas contrari, la TTP haurà de rectificar. Aquestes activitats són verificables *on-line* ja que l'actualització de l'estat de la transacció és pública i les evidències emeses per la TTP tenen la propietat de no rebuig d'origen. Si la tercera part no ha actuat correctament, aleshores l'usuari pot iniciar la fase de resolució de disputes on podrà restablir l'equitat de l'intercanvi, com acabam de veure.

Cal observar que, en el cas de la disputa iniciada per l'usuari A, hem aprofitat la simetria de les activitats de seguretat de la TTP en els dos subprotocols per comprovar-les simultàniament. Per això, pràcticament no hem distingit entre una activitat del subprotocol *abort* i el seu corresponent en el subprotocol *recovery*.

***Resultat*:** D'acord amb les proves 1, 2, 3, 4, 5, i 6 que acabam de presentar, i les seves argumentacions, podem afirmar que la TTP involucrada en els subprotocols *abort* i

recovery definits a l'anterior secció és verificable ja que les evidències que proporciona donen a totes les seves activitats la propietat de *verificabilitat on-line* i, per tant, qualsevol usuari podrà comprovar immediatament si la conducta o les operacions de la TTP estan d'acord o no amb les especificacions del protocol. En cas de disfunció de la TTP, l'usuari afectat pot iniciar un contenciós (en un jutjat si fos el cas) on podrà restablir l'equitat de l'intercanvi.

8.7 Conclusions

Com hem anat veient en aquests darrers capítols, les TTPs són entitats definides en el context dels protocols de seguretat i que pretenen donar solució a alguns problemes plantejats en aquest tipus de protocols. Les solucions serien probablement més complicades sense la seva intervenció. L'inconvenient que hem indicat és que els usuaris han de dipositar un cert grau de confiança en aquestes entitats.

En concret, el que hem aconseguit en aquest capítol és obtenir un nou protocol d'intercanvi equitatiu de valors on hem reduït la quantitat de confiança que els usuaris han de dipositar en la TTP respecte a la proposta original. Hem fet les modificacions necessàries perquè la tercera part sigui verificable. D'aquesta manera, els usuaris del protocol, no sols tenen la mateixa seguretat que els del protocol original, sinó que obtenen evidències irrefutables sobre les activitats de seguretat de la TTP. Aquestes evidències es poden utilitzar per resoldre els problemes que es puguin derivar d'una mala actuació de la TTP. Això significa que hem rebaixat l'exigència del protocol inicial sobre l'usuari relativa al dipòsit de confiança en una entitat remota (com és la TTP) ja que l'usuari disposarà d'eines per corregir possibles errors de la TTP, amb la qual cosa podem considerar que el sistema és ara més robust i més susceptible de ser utilitzat per un nombre més gran d'usuaris.

Si observam els problemes de verificabilitat que ha tengut la TTP en les diferents activitats de seguretat que pot dur a terme durant l'execució del protocol *abort* o *recovery*, ens adonarem que:

- L'activitat de seguretat 1 que fa la TTP, relativa a la recepció de la petició de l'usuari, dóna problemes de verificabilitat perquè en segons quins casos la TTP no notifica a l'usuari el resultat de la comprovació sobre la correcció de les dades de la petició.
- Les activitat de seguretat 2 i 3 relatives a la comprovació i actualització de l'estat d'una transacció tenen problemes de verificabilitat perquè l'usuari no pot consultar i obtenir evidències sobre l'estat d'una determinada transacció ja que la tercera part guarda aquesta informació internament.

- L'activitat de seguretat 4, que consisteix en la generació i enviament de missatges als usuaris, presenta a vegades problemes de verificabilitat quan no es pot distingir entre la informació emesa per la TTP o la emesa pels usuaris. També té problemes quan el receptor d'aquests missatges no pot saber el motiu de l'acció de la TTP; és a dir, si l'emissió dels missatges respon a una petició d'un usuari o es tracta d'una iniciativa pròpia de la TTP.
- Com és lògic, qualsevol de les anteriors activitats també tendrà problemes de verificabilitat si les informacions emeses per la TTP no tenen la propietat de no rebuig d'origen i no estan lligades d'alguna manera a la transacció a la qual fan referència.

En el següent capítol, veurem com hem recopilat les conclusions anteriors, d'una banda, per definir les característiques que haurien de tenir les accions de la tercera part involucrada en un protocol de seguretat i, d'altra banda, per poder-la classificar com a verificable. Hem aplicat aquestes conclusions al disseny d'un nou protocol de seguretat i hem comprovat que la tercera part que hi està involucrada és verificable.

Capítol 9

Protocol de seguretat amb tercera part verificable

9.1 Introducció

En anteriors capítols hem vist que hi ha nombroses referències que parlen de la necessitat de dur a terme una avaluació i una identificació del nivell de risc associat als serveis proporcionats per les terceres parts i, al mateix temps, desenvolupar algunes eines que puguin ajudar els usuaris a dipositar la confiança necessària en aquestes entitats. També hem vist les dificultats que tenen les solucions més tradicionals en aquest problema com són l'intercanvi alternatiu de petites porcions d'informació o la multiplicitat de terceres parts en un protocol de tal forma que una minoria de terceres parts malicioses i/o corruptes no pugui comprometre la seguretat de l'intercanvi.

Nosaltres hem optat per investigar una propietat de seguretat de les terceres parts en els protocols de seguretat per tal de facilitar la confiança dels usuaris en aquestes entitats. Volem aprofitar l'experiència descrita en capítols anteriors sobre la introducció de la verificabilitat de les TTPs en els protocols de seguretat per mostrar quines han de ser les característiques que, a priori, han de tenir les operacions d'una tercera part per tal de poder definir un nou protocol de seguretat amb una TTP verificable.

Així doncs, en el pròxim apartat, descrivim un conjunt de recomanacions que ha de facilitar el disseny de protocols de seguretat amb terceres parts verificables. Hem posat en pràctica aquestes recomanacions i hem dissenyat un nou protocol de seguretat [MFH05] amb la TTP verificable, cosa que descrivim i comprovam en aquest mateix capítol. Per a aquesta aplicació vàrem escollir definir un nou protocol de correu electrònic certificat per ser un dels tipus de protocols que hem discutit més durant la tesi al voltant del qual s'ha fet una recerca considerable que inclou el tema de la fiabilitat de les terceres parts.

9.2 Operacions de les TTP verificables

A l'apartat de conclusions dels capítols anteriors, hem descrit alguns detalls del disseny dels protocols que fan que les TTPs que hi estan implicades no siguin verificables. Evidentment aquests detalls fan referència a la manera d'actuar de la tercera part i a les anomenades activitats de seguretat que duu a terme. Esquemàticament podem dividir els problemes de verificabilitat de les TTPs en tres gran tipus de problemes:

- Problemes de comprovació de l'activitat de la TTP: si la TTP guarda informacions relatives a les transaccions que puguin dur a terme els usuaris, aleshores és probable que algunes de les activitats que dugui a terme estiguin en funció d'aquestes dades. Aquestes activitats de seguretat seran difícilment verificables per als usuaris si aquests no poden consultar ni obtenir evidències sobre l'estat de les seves transaccions.
- Problemes de resposta de la TTP: de vegades el problema de la no verificabilitat de la tercera part ve causat perquè la seva resposta no permet comprovar les activitats que ha dut a terme. Com hem vist en els capítols anteriors, els motius d'això poden ser múltiples:
  - No està prevista resposta de la TTP en qualsevol de les situacions que puguin passar en la recepció de la petició de l'usuari.
  - No hi ha un punt de connexió entre la resposta de la TTP i els missatges d'una mateixa transacció.
  - Quan hi ha més d'un usuari involucrat en una transacció, pot passar que un usuari no pugui estar segur si els missatges que rep de la TTP són causats per una petició de l'altre usuari o són fets a iniciativa pròpia de la TTP.
  - També, en cas de múltiples usuaris, és motiu de no verificabilitat el fet que la TTP, dins del mateix protocol, pugui emetre informacions idèntiques a les emeses pels usuaris. En aquesta situació hi haurà missatges que podran haver estat publicats tant per la TTP com per algun usuari. Això determina la no verificabilitat de la TTP.
- Problemes en les propietats de seguretat del missatge: naturalment la TTP no serà verificable si els missatges que emet no tenen la propietat de no rebuig d'origen [X.813].

Ens interessa extreure dels problemes que acabam d'exposar unes recomanacions molt concretes que ens puguin servir de referència en el moment de dissenyar un protocol de seguretat, en el sentit que ens siguin útils per definir com han de ser les activitats de seguretat dutes a terme per una TTP si volem que aquesta sigui verificable. Per això, hem dividit les activitats de seguretat que pot efectuar una TTP en tres tipus:

- *Recepció*: activitats de seguretat relatives a la recepció de la petició de l'usuari i la resposta que la TTP li donarà.
- *Emissió*: activitats de seguretat relacionades amb la generació i emissió de missatges de la TTP cap als usuaris.
- *Comprovació*: activitats de seguretat que tenen relació amb comprovacions i actualitzacions d'informació que guarda la TTP sobre l'estat d'una determinada transacció, juntament amb les accions que es puguin desencadenar en funció del resultat d'aquestes comprovacions.

Les recomanacions que hauríem de tenir en compte per a cada tipus d'activitat si volem dissenyar un protocol amb una TTP verificables estan descrites a la figura 9.1.

Tipus d'activitat de seguretat	**Recomanacions**
Recepció	La petició de l'usuari ha de tenir sempre una resposta de la TTP. La resposta de la TTP ha de funcionar com una evidència de no rebuig de recepció de la petició de l'usuari i confirmar la seva correcta recepció. Aquesta evidència ha de mostrar que ha estat generada com a resposta a la petició d'un usuari i ha d'estar-hi lligada d'alguna manera (per exemple, dins la resposta de la TTP pot haver-hi la petició de l'usuari o una empremta digital d'aquesta).
Emissió	Els missatges generats i emesos per la TTP han de tenir la propietat de no rebuig d'origen i han d'estar lligats d'alguna manera al tipus de transacció o intercanvi al qual fan referència (per exemple, mitjançant un mateix identificador). Com en el cas de l'anterior operació, les evidències emeses han de mostrar que han estat generades com a resposta a una petició d'un usuari; és a dir, s'ha de poder comprovar que la TTP no ha emès un determinat missatge per iniciativa pròpia sinó que respon a les especificacions del protocol. La TTP no ha de poder emetre ítems d'informació en el mateix format que qualsevol dels usuaris; això és, qualsevol àrbitre ha de poder distingir entre els ítems generats per un usuari i els generats per la TTP.

Figura 9.1. Recomanacions per al disseny de protocols amb TTP verificable

Comprovació	Si volem que les operacions de comprovació i actualització que fa la TTP siguin verificables, aquestes hauran de ser, d'alguna manera, públiques. Per exemple, els usuaris hauran de tenir accés a les informacions que guarda la TTP sobre les seves transaccions i que, en funció de les verificacions de les quals poden ser objecte, la TTP pot actuar d'una manera o d'una altra. D'aquesta manera, els usuaris poden saber per quins motius la TTP ha actuat d'una determinada manera. Pot ser una bona pràctica la publicació de l'estat de les transaccions a través de missatges amb la propietat de no rebuig d'origen (el generador d'aquests missatges és la TTP) col·locats en un directori públic només amb drets de lectura per als usuaris i administrat per la TTP.

***Figura 9.1* (continuació).** Recomanacions per al disseny de protocols amb TTP verificable

9.3 Protocol de correu electrònic certificat

En aquesta secció proposam un nou protocol de correu electrònic certificat. A diferència de la resta de propostes, hem dissenyat aquest protocol tenint com a referència les recomanacions que acabam d'exposar. El resultat d'aquesta nova proposta demostra que podem dissenyar nous protocols seguint les recomanacions anteriors i obtenir unes solucions que poden tenir característiques semblants a les millors propostes que ja puguin existir però, a més a més, la tercera part involucrada en el protocol és verificable.

Així doncs, ens centrarem en el disseny del nou protocol de correu electrònic certificat i la seva problemàtica. Tal i com s'explica a [ZDB99], i d'acord amb l'estructura dels estàndards internacionals com el servei de lliurament de missatges X.400, va a càrrec del receptor reconèixer la recepció dels missatges. El receptor pot emetre reconeixements de recepció de missatges selectivament i això és indesitjable en algun procediment de comerç electrònic o en protocols de seguretat com el de correu electrònic certificat que tractam ara. Aquest problema també existeix en els estàndards de l'ISO/IEC 13888 [ISO13888-1, ISO13888-2, ISO13888-3]. En els protocols proposats en els articles científics sovint s'hi veuen involucrades TTPs per solucionar el problema del no rebuig. Consegüentment, podem dir que les TTPs representen un paper important en la provisió dels serveis de no rebuig i, de la seva fiabilitat, en depèn la seguretat del sistema. En canvi, per distintes raons, les terceres parts poden fallar, poden cometre errades, poden tenir una avaria i, fins i tot, poden cometre accions deshonestes (tots aquests aspectes poden causar les reticències dels usuaris a utilitzar aquests procediments). Per solucionar el problema del reconeixement selectiu del receptor presentarem aquí un nou protocol de correu electrònic certificat amb una TTP involucrada però, per incrementar la seva fiabilitat i la confiança

dels usuaris, seguirem les directrius que acabam de descriure a l'anterior paràgraf a fi i efecte que el disseny del nou protocol ens asseguri que la TTP que hi està involucrada és verificable.

Missatge	M
Xifratge simètric del missatge amb la clau K produint el criptograma *c*	$c = E_K(M)$
Missatge per lliurar de la clau a la TTP (clau K xifrada amb la clau pública de la TTP)	$k_T = PU_T(K)$
Missatge de la TTP per lliurar la clau a B (s_B per identificar la transacció i per mostrar que aquest ítem és en resposta de la petició d'un usuari. La clau K és xifrada amb la clau privada de la TTP)	$k'_T = PR_T(s_B, K)$
Missatge d'A per lliurar la clau a B (identificació de la transacció i la clau K estan xifrades amb la clau privada de l'usuari A)	$k_A = PR_A(A, B, h(c), K)$
Missatge de confirmació de recepció de la clau (identificació de la transacció i la clau K estan xifrades amb la clau privada de B)	$k_B = PR_B(A, B, h(c), K)$
Compromís d'A d'acabar l'intercanvi (identificació de la transacció i k_T xifrats amb la clau privada d'A)	$h_A = PR_A(A, B, h(c), k_T)$
Compromís de l'usuari B d'acabar l'intercanvi (identificació de la transacció i k_T xifrats amb la clau privada de B)	$h_B = PR_B(A, B, h(c), k_T)$
Cancel·lació de la transacció per a A (etiqueta '*cancel*' i s_A xifrats amb la clau privada de la TTP)	$h'_A = PR_T(\text{'}cancel\text{'}, s_A)$
Cancel·lació de la transacció per a B (etiqueta '*cancel*' i s_B xifrats amb la clau privada de la TTP)	$h'_B = PR_T(\text{'}cancel\text{'}, s_B)$
Petició de l'usuari A (informació de la transacció xifrada amb la clau privada d'A). Si A vol cancel·lar la transacció, aleshores h_B no ha de ser a s_A	$s_A = PR_A(c, A, B, h_A, h_B, k_T)$
Petició de l'usuari B (informació de la transacció xifrada amb la clau privada de B)	$s_B = PR_B(c, A, B, h_A, h_B, k_T)$
Evidència que prova que l'usuari A ha lliurat tota la informació de l'actual transacció (informació de la transacció xifrada amb la clau privada de la TTP)	$d_A = PR_T(\text{'}delivery\text{'}, s_A)$
Evidència que prova que l'usuari B pot tenir la clau per completar el protocol (informació de la transacció xifrada amb la clau privada de la TTP)	$d'_A = PR_T(\text{'}delivery\text{'}, s_A, k'_T)$

Figura 9.2. Notació

El correu electrònic certificat és un cas especial d'intercanvi equitatiu de valors; per tant, el protocol que es proposarà haurà de tenir el mateix tipus de propietats d'aquest tipus d'intercanvis com les que trobam en els documents [FPH00, ASW98, KMZ02]. En la descripció de la nostra proposta utilitzarem la mateixa notació que hem emprat en els capítols anteriors i que hem detallat a l'apartat 6.4. Els elements usats en la descripció del protocol són els descrits a la figura 9.2.

El protocol de correu electrònic certificat consisteix en un intercanvi d'un missatge i d'un *token* de no rebuig d'origen a canvi d'un *token* de no rebuig de recepció. El *protocol bàsic* que presentam és el de la figura 9.3.

1. A→ B: c, k_T, h_A
2. B→ A: h_B
3. A→ B: k_A
4. B→ A: k_B

Figura 9.3. Protocol bàsic

Després de l'execució d'aquest protocol, si no ha ocorregut cap excepció, el receptor tendrà el missatge (c i M) amb una prova de no rebuig d'origen (h_A, k_A), i l'emissor tendrà una prova de no rebuig de recepció (h_B, k_B). La TTP només s'involucrarà en el protocol quan ocorri alguna excepció i només a petició dels usuaris, això és: si el tercer o el quart missatge no arriba, aleshores A o B poden llançar els respectius protocols per a casos d'excepció.

El protocol per a l'usuari A per a situacions d'excepció és el descrit a la figura 9.4. En aquest protocol, l'usuari A intenta aconseguir l'ítem k'_T en el primer pas. Aquest ítem només haurà estat publicat per la TTP en el seu directori públic si B ja s'ha posat en contacte prèviament amb aquesta entitat per resoldre la transacció en qüestió. En funció de l'èxit del primer pas, l'usuari A fa la petició a la TTP. La resposta que obtendrà serà un missatge d'error si la petició no és correcta i, en cas contrari, la TTP respondrà amb una prova de lliurament de les dades de la transacció en curs o una evidència de cancel·lació (en funció de l'estat de la transacció). El protocol per a casos d'excepció per a un receptor (B) del protocol de correu electrònic certificat l'hem especificat a la figura 9.5.

1. T↔ A: k'_T
IF (step 1 is successful**) THEN**
  2. A→ T: s_A, k'_T
  3. T↔ A: d'_A
ELSE
  2. A→ T: s_A
  IF ($h_B \subset s_A$**) THEN**
    IF ($h'_A \not\subset$ Public Directory**) THEN**
      3. T↔ A: d_A
    ELSE
      3. T→ A: error_message
  ELSE
    IF (k'_T or $d_A \not\subset$ Public Directory**) THEN**
      3. T↔ A: h'_A
    ELSE
      3. T→ A: error_message

Figura 9.4. Protocol per a situacions d'excepció per a l'usuari *A*

En el protocol de la figura 9.5, l'usuari *B* envia la seva petició s_B a la TTP per poder obtenir la clau o un *token* de cancel·lació de la transacció depenent de l'estat de la mateixa. Abans i després de l'execució del protocol per a casos d'excepció, l'estat de la transacció pot ser comprovat per qualsevol usuari en el directori públic administrat per la TTP. En aquests protocols nosaltres suposam que la TTP comprovarà la correcció, el format i la signatura de cada un dels missatges que rep. En cas que el resultat de la comprovació sigui negatiu, la TTP enviarà el corresponent missatge d'error a l'usuari.

1. B→ T: s_B
IF ($h'_A \subset$ Public Directory**) THEN**
  2. T↔ B, A: h'_B
ELSE
  2. T↔ B, A: k'_T

Figura 9.5. Protocol per a situacions d'excepció per a l'usuari *B*

9.3.1 Resolució de disputes

Després d'haver completat una execució del protocol (amb o sense la participació de la TTP), poden sorgir disputes entre els participants que hi estan involucrats. Podem abordar dos tipus de disputes:

- Rebuig d'origen: l'usuari *B* diu haver rebut el missatge *M* de l'usuari *A* i *A* nega haver-lo enviat
- Rebuig de recepció: l'usuari *A* diu haver enviat el missatge *M* a l'usuari *B* i *B* nega haver-lo rebut

Un àrbitre extern (per exemple un jutge) ha d'avaluar les evidències que aporten els usuaris per resoldre la disputa. Com a resultat d'aquesta avaluació, l'àrbitre determinarà qui té raó.

En cas de no rebuig d'origen, *B* ha de proporcionar les següents informacions a l'àrbitre: *M, c,* h_A i k_A o k'_T. Primer de tot, l'àrbitre comprovarà que h_A i k_A o k'_T estan lligats al missatge mitjançant el mateix identificador de transacció i el missatge *M* és el desxifratge de *c* utilitzant la clau *K*, aleshores podrà comprovar la correcció de la signatura de l'usuari *A* sobre els missatges h_A i k_A o la signatura de la TTP sobre k'_T. Si totes les verificacions són correctes llavors l'àrbitre donarà la raó a *B*, però si una o més de les comprovacions prèvies han fallat, l'àrbitre rebutjarà la demanda de *B*. No obstant això, si totes les verificacions són correctes però *A* té un missatge de cancel·lació h'_A, això significa que *B* ha actuat correctament, mentre que la TTP o *A* no ho han fet. Gràcies al fet que l'operació de la TTP és verificable, l'àrbitre pot descobrir qui és el culpable d'aquesta inconsistència. Per tal de verificar l'operació de la TTP, l'àrbitre ha de comprovar els següents elements:

- La petició de *A* (s_A) ha de ser dins de h'_A
- h_B no ha de ser dins de s_A
- La signatura de la TTP sobre h'_A ha de ser vàlida
- *B* ha enviat k_A en la seva queixa en lloc d'un k'_T vàlid.

Si totes les verificacions són positives, significa que la TTP ha actuat correctament i aleshores *A* és el culpable de l'existència de proves d'haver completat exitosament una transacció i, al mateix temps, d'haver-hi proves de la cancel·lació de la mateixa. En qualsevol altre cas, la TTP és la culpable d'aquest fet (si la signatura de la TTP sobre h'_A és vàlida).

En cas de rebuig de recepció l'usuari *A* diu que *B* ha rebut el missatge *M*. Ha de proporcionar la següent informació a l'àrbitre: *M, c,* h_B i k_B o d_A o d'_A. Inicialment l'àrbitre comprovarà que h_B i k_B o d_A o d'_A estan lligats al missatge amb el mateix identificador de transacció i que el missatge *M* és el desxifratge del criptograma *c* usant la clau *K* i aleshores comprovarà la correcció de la signatura de *B* sobre els missatges h_B i k_B o la signatura de la TTP sobre d_A or d'_A. Si totes les verificacions són correctes aleshores l'àrbitre donarà la raó a *A*, però si una o més de les comprovacions prèvies ha fallat, l'àrbitre rebutjarà la demanda d'*A*.

9.3.2 Prova de la verificabilitat de la tercera part

***Enunciat*: La tercera part involucrada en el protocol de correu electrònic certificat és verificable ja que les activitats de seguretat que descriurem a les figures 9.6 i 9.7 són verificables i la seva verificabilitat és *on-line*.**

Inicialment segmentarem l'activitat de la TTP quan dóna servei a la petició de l'usuari i, per això, dividirem la seva operativitat en unitats funcionals que nosaltres anomenam activitats de seguretat (vegeu les definicions del tema 5). Després comprovarem que aquestes unitats o activitats de seguretat tenen una verificabilitat *on-line* i, si és així, aleshores podrem concloure que la TTP és verificable.

Servei de la TTP a l'emissor

A la figura 9.6 podem veure totes les activitats de seguretat utilitzades per la TTP per proporcionar el servei a un emissor de protocol de correu electrònic certificat proposat.

- **Activitat 1**: recepció i verificació de la informació de la petició de l'usuari: s_A

IF (verificació és correcta**) THEN**
  IF (la TTP rep k'_T**) THEN**
    - **Activitat 1(extensió)**: verificació de la correcció de k'_T i que h_B és a s_A

    IF (verificació és correcta**) THEN**
      - **Activitat 2**: generació i emissió de l'evidència de no rebuig d'_A

        ELSE
    - **Activitat 1(extensió)**: enviament d'un missatge d'error

  ELSE
    - **Activitat 1(extensió)**: comprovació que h_B és a s_A i que és correcta

    IF (verificació és correcta**) THEN**
      - **Activitat 3**: comprovació que h'_A no és al directori públic

      IF (verificació és correcta**) THEN**
        - **Activitat 4**: generació i emissió de l'evidència de lliurament d_A

      ELSE
        - **Activitat 3(extensió)**: enviament d'un missatge d'error

    ELSE
      - **Activitat 5**: comprovació que k'_T i d_A no són en el directori públic

      IF (verificació és correcta**) THEN**
        - **Activitat 6**: generació i emissió de l'evidència de cancel·lació h'_A

      ELSE
        - **Activitat 5(extensió)**: enviament d'un missatge d'error

ELSE
  - **Activitat 1(extensió)**: enviament d'un missatge d'error

Figura 9.6. Activitats funcionals utilitzades per la TTP per proporcionar el servei a un emissor

Hem agrupat alguns tipus d'activitats de seguretat que tenen el mateix tipus d'operació per fer més senzilla la demostració sobre la seva verificabilitat. D'aquesta manera, les activitats de seguretat relatives a les operacions de *recepció* (vegeu l'apartat 9.2) estan agrupades a l'activitat 1.

Prova 1*: L'activitat 1 que comprèn les operacions de la tercera part relacionades amb les operacions de *recepció* de la petició de l'usuari té una verificabilitat *on-line
***Argumentació*:** Aquesta activitat és verificable perquè l'usuari sempre rebrà una resposta de la TTP a la seva petició. La resposta pot ser una evidència de no rebuig, de lliurament o de cancel·lació o també pot rebre un missatge d'error. Tots aquests diferents tipus de respostes estan signades per la TTP i han de tenir el mateix identificador de transacció que la petició de l'usuari i que, a més, inclouen la petició de l'usuari s_A; per tant, qualsevol àrbitre pot avaluar la correcció de l'operació de la TTP i saber que l'emissió del *token* resposta per part de la TTP és a causa d'una petició de l'usuari.

Prova 2*: Les activitats de seguretat que fan referència al tipus d'operació anomenat d'*emissió* són verificables *on-line
***Argumentació*:** Les activitats de seguretat que són dels tipus d'operació *emissió* són les número 2, 4 i 6. Aquestes activitats són verificables ja que tots els missatges generats per la TTP en el protocol (d'_A, d_A i h'_A) s'han construït emprant criptografia de clau pública i tenen la propietat de no rebuig d'origen. A més, estan lligades a la petició de l'usuari a través del mateix identificador de transacció, tal i com especifiquen les recomanacions detallades a l'apartat 9.2 d'aquest capítol. Quan l'usuari rep qualsevol dels ítems emesos per la TTP pot comprovar immediatament la correcció de la resposta. Consegüentment podem afirmar que aquestes activitats tenen una verificabilitat *on-line*. És important observar que la TTP no pot generar i emetre cap missatge correcte que no es pugui distingir dels emesos per qualsevol dels usuaris (exceptuant, com és natural, que retransmeti un missatge de l'usuari tal i com l'ha rebut).

Prova 3*: Les activitats de seguretat relatives a les operacions de *comprovació* són verificables *on-line
***Argumentació*:** Les activitats de seguretat que representen operacions del tipus *comprovació* són les activitats que a la figura 9.6 estan marcades amb els números 3 i 5. Aquestes activitats són verificables ja que qualsevol d'aquestes operacions descrites en el protocol són públiques i, d'aquesta manera, els usuaris, mitjançant la resposta que reben de la TTP, poden saber que la TTP ha guardat, actualitzat o comprovat les dades correctament. En el protocol, l'estat de qualsevol transacció és a un directori públic i està representat per evidències verificables generades per la TTP (h'_A, k'_T i d_A mostren d'una manera pública i verificable per a qualsevol usuari l'estat de cada una de les transaccions); per tant, com ja hem avançat, les activitats 3 i 5 són verificables *on-line*.

Servei de la TTP al receptor

A la figura 9.7 podem veure totes les unitats funcionals o activitats de seguretat utilitzades per la TTP per donar servei a un receptor del protocol de correu electrònic certificat proposat.

- **Activitat 1**: recepció i verificació de la informació de la petició de l'usuari: s_B
  IF (verificació és correcta**) THEN**
  - **Activitat 2**: comprovació que h'_A és al directori públic

  IF (verificació és correcta**) THEN**
  - **Activitat 3**: generació i emissió de l'evidència de cancel·lació h'_B

  ELSE
  - **Activitat 4**: generació i emissió de l'evidència de submissió de la clau k'_T

ELSE
- **Activitat 1(extensió)**: enviament d'un missatge d'error

Figura 9.7. Activitats de seguretat utilitzades per la TTP per proporcionar el servei a un receptor

Com en el cas anterior, hem agrupat les activitats de seguretat relatives a les operacions de *recepció* a l'activitat 1; per això, hem etiquetat com una extensió de l'activitat 1 les successives operacions de la TTP directament relacionades amb la recepció i verificació de la petició de l'usuari.

Prova 4*: L'activitat 1 que comprèn les activitats de seguretat que executa la tercera part quan dóna servei a un usuari receptor del protocol i que estan relacionades amb les operacions de *recepció* de la petició de l'usuari té una verificabilitat *on-line
***Argumentació*:** D'acord amb el protocol, la TTP sempre enviarà un missatge després de la recepció de la petició de l'usuari. Si aquesta petició és correcta, aleshores la TTP enviarà una evidència de cancel·lació o de submissió. De la mateixa manera, si la petició no és correcta, l'usuari també rebrà una resposta de la TTP, aquesta vegada en forma de missatge d'error. En conseqüència l'usuari sempre rebrà un missatge signat de la TTP com a resposta a la seva petició i, complint amb les especificacions del protocol, aquesta resposta funcionarà com a evidència de no rebuig de recepció de la seva petició. Podem afirmar, doncs, que aquesta activitat de seguretat és verificable *on-line*, perquè la comprovació de la correcció de qualsevol d'aquestes evidències és immediata per part de l'usuari. En cas d'error de la TTP, l'usuari podrà anar a un sistema de resolució de disputes i les evidències que podrà aportar demostraran que les accions de la TTP no han estat correctes.

Prova 5*: Les activitats de seguretat que fan referència al tipus d'operació anomenat d'*emissió* i que són executades per la TTP quan dóna servei a l'usuari receptor del protocol són verificables *on-line
***Argumentació*:** Les activitats de seguretat que són del tipus d'operació *emissió* són les número 3 i 4. Aquestes activitats generen les evidències h'_B i k'_T, que tenen la propietat de no rebuig d'origen i també demostren que han estat generades com a resposta a una petició d'usuari (inclouen s_B) i la TTP no té en cap moment suficient informació per generar cap ítem que sigui indistingible dels emesos pels usuaris en el protocol. Quan l'usuari rep les evidències que acabam d'esmentar pot verificar-les immediatament i així comprovarà que l'activitat de la TTP s'ha dut a terme tal i com el protocol especifica. Així, doncs, podem afirmar que aquestes activitats són verificables *on-line*.

Prova 6*: L'activitat de seguretat relativa a les operacions de *comprovació* fetes per la TTP quan dóna servei a l'usuari receptor del protocol de correu electrònic certificat són verificables *on-line
***Argumentació*:** L'activitat 2 va lligada al tipus d'operació que hem anomenat de *comprovació*. Com en el protocol d'excepció per a l'usuari emissor, qualsevol usuari receptor també pot comprovar l'estat de la seva transacció comprovant h'_A que està situat en el directori públic administrat per la TTP. L'ítem h'_A és una prova de l'estat d'una determinada transacció i, si la resposta de la TTP no està d'acord amb aquesta evidència publicada, aleshores l'usuari estarà en disposició de provar que l'actuació de la TTP no ha estat correcta. Consegüentment podem afirmar que l'activitat 2 té una verificabilitat *on-line*.

***Resultat*:** Després de les sis proves anteriors i d'acord amb les definicions donades en el tema 5 d'aquesta tesi sobre la propietat de verificabilitat, les activitats de seguretat que hem descrit a les figures 9.6 i 9.7 són verificables i la seva verificabilitat és *on-line*. Per tant, podem assegurar que la tercera part involucrada en el protocol és verificable.

9.4 Conclusions

En aquest capítol hem descrit un petit conjunt de recomanacions sobre com ha de dur a terme una TTP cada tipus d'activitat de seguretat. Aquestes activitats de seguretat són les unitats funcionals que segmenten i descriuen les operacions de la tercera part quan rep una petició d'un usuari dins l'entorn d'un protocol de seguretat. El seguiment de les recomanacions esmentades anteriorment ha de tenir com a conseqüència que la TTP sigui verificable. D'aquesta manera, els dissenyadors de protocols tenen un punt de referència si pretenen implantar aquesta propietat a nous protocols de seguretat.

Com ja hem explicat, la introducció de la propietat de verificabilitat de la TTP en els protocols de seguretat significa que qualsevol operació no correcta de la TTP podrà ser immediatament detectada per l'usuari que sol·licità el servei. A més, aquest usuari estarà en disposició de demostrar a un àrbitre extern que la tercera part no va donar el servei correctament i, per tant, podrà demanar la rectificació per part de la TTP perquè es pugui conservar la seguretat de la transacció que s'estava executant.

En l'apartat 9.3 d'aquest capítol hem presentat un nou protocol de correu electrònic certificat on hem demostrat que és possible resoldre qualsevol disputa que pugui sorgir entre els participants d'un intercanvi (preservant en qualsevol cas l'equitat de l'intercanvi). Addicionalment i gràcies al compliment de les recomanacions presentades a l'apartat anterior, hem vist com també qualsevol mala actuació de la TTP pot ser immediatament detectada i els usuaris tendran les evidències que provaran aquest fet. Les proves es poden utilitzar en un sistema de resolució de disputes extern per restablir l'equitat de l'intercanvi que la tercera part podria haver romput.

Juntament amb el conjunt de recomanacions sobre com implantar la propietat de verificabilitat, en aquest capítol fem una segona aportació que no és només un nou protocol de correu electrònic certificat sinó que per a nosaltres representa la constatació que les recomanacions anteriorment esmentades són vàlides i que de forma efectiva ens han conduït a elaborar un protocol que presenta la verificabilitat de la TTP (verificabilitat *on-line* de cada activitat de la TTP) com a tret diferenciador i nou respecte a les propostes d'altres autors [AGH02, ASW98, FPH00, KM00, MK01, ZDB99]. D'aquesta manera veiem com una debilitat potencial dels protocols de seguretat pot ser eliminada millorant la seguretat global del sistema.

Capítol 10

Conclusions

El principal objectiu d'aquesta tesi ha estat l'estudi de les terceres parts de confiança que intervenen en els protocols d'intercanvi electrònic d'informació com a factor clau per a la salvaguarda de la seguretat. Enteníem abans de començar la recerca i, entenem més ara, que aquestes entitats són un punt crític dels sistemes d'intercanvi electrònic que compten amb la seva participació, ja que qualsevol errada seva pot malmetre la seguretat del protocol. Per això, inicialment, hem començat exposant les distintes formes com les TTPs poden intervenir en els protocols i com, en qualsevol dels casos, donen un servei als usuaris en relació amb la seguretat de l'intercanvi que duen a terme entre ells.

Mitjançant la introducció de les terceres parts en els protocols, hem vist com es pretén trobar solucions més pràctiques als problemes d'intercanvi electrònic plantejats. A canvi, els protocols arbitrats tenen un requeriment inicial que obliga els usuaris a dipositar un cert grau de confiança en les TTPs, ja que, a priori, la seguretat de les transaccions queda en mans de la conducta d'aquestes entitats. El problema que hem abordat en aquesta tesi rau en el dipòsit de confiança que han de fer els usuaris de la xarxa en les TTPs, fet que provoca un sentiment de seguretat relativa que no ajuda a vèncer les reticències que puguin tenir sobre la seguretat de les seves transaccions electròniques i les accions que es poden dur a terme si aquesta es perd.

Després de fer aquest plantejament i vistes les alternatives que fins ara s'havien presentat, podem concloure que una via per solucionar el problema és la inclusió de múltiples terceres parts que ofereixin un servei col·legiat als usuaris en els protocols de seguretat. Per això hem plantejat una solució al problema exposat, en el capítol 3 de la tesi, en forma de protocol de seguretat que inclou múltiples terceres parts de confiança i que és resistent a una minoria de terceres parts corruptes: això significa que les característiques de seguretat del protocol estan garantides sempre i quan una majoria de les TTPs que hi intervenen actuïn d'acord amb les especificacions del protocol. Els protocols que apliquen

aquesta tècnica distribueixen la confiança que s'hauria de dipositar en una sola TTP entre el conjunt de TTPs que es veuen involucrades en el protocol. La proposta que hem fet té una característica que li dóna un valor afegit i representa un tret diferencial respecte a altres propostes i és que utilitza esquemes de criptografia simètrica i de clau pública en lloc dels habituals esquemes criptogràfics llindar emprats en aquests tipus de propostes. Això significa que la nostra formulació és més eficient, tant des del punt de vista d'estalvi computacional com des del punt de vista d'estalvi en comunicacions. Així, podem afirmar que en el capítol 3 hem fet una proposta capaç de fer augmentar la confiança dels usuaris en les seves transaccions electròniques si fan servir aquest protocol, ja que per rompre la seguretat de l'intercanvi (des del punt de vista de l'estudi d'aquesta tesi) no bastaria que una TTP actuàs de forma improcedent sinó que caldria que una majoria d'aquestes fos corrupta, cosa que, òbviament, és més difícil que es produeixi.

No obstant la reducció de la sobrecàrrega en les comunicacions i càlcul que representa la nostra proposta respecte a plantejaments semblants fets per altres autors, hem obert una nova via en la resolució del problema de la relativa seguretat que provoca la intervenció de TTPs en els protocols, ja que vàrem poder observar que el tipus de solució presentada té un inconvenient que és el cost i la infrastructura que comporta tenir i mantenir un servei col·legiat de TTPs. Per això s'han analitzat les característiques del rol de les terceres parts en els intercanvis electrònics i hem presentat un sistema de classificació dels serveis oferts per les TTPs als usuaris. És una classificació de l'actuació de les TTPs en els protocols des de set punts de vista diferents. Hem d'assenyalar que per fer aquesta classificació no hem fet cap consideració sobre criteris institucionals i legals de les terceres parts, que poden canviar amb independència del protocol. És a dir, la nostra classificació està relacionada amb els intercanvis de dades definits en el protocol entre els usuaris i les TTPs, però no es relaciona amb l'administració de la TTP ni amb les lleis i regulacions nacionals i internacionals.

L'anàlisi de la intervenció de la TTP des de distints enfocaments no només és una contribució d'aquesta tesi per poder entendre les característiques de les TTPs en els protocols, sinó que ens ha permès trobar aquella propietat de seguretat que ens ofereix una alternativa a les solucions aportades fins ara per al control de les possibles errades (intencionades o no) de les TTPs durant l'execució d'un determinat protocol de seguretat, cosa que va motivar aquest estudi. La conclusió d'aquest ens ha portat a oferir una alternativa consistent en la inclusió en els protocols de la propietat de verificabilitat de les terceres parts, característica que representa una bona solució al problema.

La propietat de verificabilitat de les TTPs havia estat inicialment formulada per N. Asokan et al. a [ASW98] i l'hem utilitzada com un punt de vista més dins del mètode de classificació de les TTPs esmentat en els anteriors paràgrafs. Ara bé, per introduir aquesta propietat de forma sistemàtica en els protocols, com hem pogut veure en els capítols

anteriors, hem hagut de dissenyar prèviament el que hem anomenat entorn de verificabilitat, és a dir, un conjunt de definicions de tots els conceptes relatius a la propietat estudiada que pensam que són cabdals per entendre, aplicar i comprovar la verificabilitat de les terceres parts involucrades en els diferents protocols. És en aquest punt on volem destacar l'aportació de la divisió per primera vegada del concepte de verificabilitat, distingint entre el que hem anomenat verificabilitat *on-line* i *off-line*. La importància de la distinció rau en el fet de poder definir amb més rigor què és una tercera part de confiança verificable en un protocol de seguretat: a partir d'aquí hem considerat que només podrem anomenar la TTP com a verificable si la verificabilitat és del tipus *on-line*, és a dir, si els usuaris poden comprovar de forma immediata que l'actuació d'aquesta entitat està d'acord amb les especificacions del protocol.

Els capítols 6, 7 i 8 de la tesi detallen l'estudi d'aplicació de la verificabilitat en distints tipus de protocols, a través del qual mostram com es poden oferir alternatives a coneguts protocols de seguretat on la tercera part no era inicialment verificable. És a dir, sense menystenir la proposta de l'esquema original i, sobretot, preservant les característiques de seguretat, hem presentat en aquests capítols unes modificacions sobre els protocols mitjançant les quals convertim en verificables les TTPs que hi intervenen. Així doncs, hem formulat una alternativa per als protocols estudiats i presentam uns nous protocols derivats de les propostes inicials però que inclouen la propietat de verificabilitat de la TTP per donar seguretat al sistema i confiança als usuaris. Això significa que després de la feina feta hem obtingut una nova definició d'una propietat de seguretat (propietat de *verificabilitat de la tercera part de confiança*) que, mitjançant l'experiència, hem vist com pot ser inclosa en els nous procediments electrònics sense que això comporti cap sobrecàrrega afegida en els protocols.

Finalment hem conclòs la nostra recerca treballant per sintetitzar les experiències anteriorment esmentades i així poder aportar un conjunt d'orientacions per al disseny de protocols en els quals es facilita la introducció de TTPs verificables. En aquestes orientacions hem ressenyat com és convenient que es defineixi la conducta de la TTP en un protocol perquè sigui verificable. Per això, hem especificat les característiques desitjables de cada una de les operacions de la TTP en el protocol perquè les seves accions siguin verificables per als usuaris. Hem demostrat la utilitat i l'efectivitat d'aquestes recomanacions en el capítol 9, on les hem posat en pràctica per definir un nou protocol de seguretat d'intercanvi equitatiu de valors que, de bon començament, no només garanteix les característiques de seguretat i eficiència dels millors protocols d'aquests tipus, sinó que assegura als usuaris la verificabilitat de la TTP que hi intervé. Així doncs, amb el conjunt d'orientacions que hem aportat, tenim a l'abast un punt de partida a l'hora de posar-nos a dissenyar un nou protocol de seguretat amb una TTP verificable.

En definitiva, pensam que hem ofert una nova opció per al disseny de protocols de seguretat amb terceres parts de confiança. L'alternativa, com ja hem dit, pretén respondre a la sensació de relativa seguretat que tenen els usuaris sobre l'ús dels nous procediments electrònics. La manca de tradició de les terceres parts de confiança i la seva naturalesa com a noves entitats virtuals i remotes són motius que serveixen per provocar certes reticències en l'ús dels protocols que necessiten de la seva intervenció per complir amb els requeriments de seguretat de l'intercanvi d'informació que es duu a terme. Així doncs, la noves recomanacions ens permeten dissenyar protocols de seguretat amb TTPs verificables, una nova resposta, pel que fa a l'actuació de la TTP, a les incerteses dels usuaris sobre la seguretat de les seves transaccions que actualment dificulten l'expansió de les noves aplicacions electròniques, entre les qual podem citar els nous procediments de l'administració digital o els de comerç electrònic.

És important ressenyar que les alternatives que tenim perquè els protocols siguin resistents a possibles errades de les terceres parts no són excloents, en el sentit que un tipus de solució no n'invalida un altre. És a dir, pensam que, depenent del tipus de transacció, els usuaris haurien de poder escollir un determinat nivell de seguretat que podria conduir-los a diferents alternatives, o bé a l'ús d'un protocol amb múltiples TTPs, o bé a utilitzar-ne un amb una TTP però verificable o, fins i tot, no tenir cap element de seguretat pel que fa a l'actuació de la TTP.

També volem remarcar que hem proposat un tipus de solució que consisteix en la introducció de la propietat de verificabilitat en coneguts protocols de seguretat. Això significa que podem emprar, en cas de procediments electrònics que ja estiguin implementats i en ús, aquesta propietat sense renunciar al valor de la tradició del seu ús pel que fa a la confiança que això pugui generar. En canvi, amb la introducció d'aquesta nova propietat, podem corregir-ne les debilitats potencials. No obstant això, pensam que, si s'observen les normes de disseny que hem presentat, es poden obtenir noves solucions amb terceres parts verificables que no resten seguretat ni eficiència respecte a una solució equivalent però sense verificabilitat. Així doncs, en aquestes condicions, amb un cost negligible, la seguretat del sistema es veu augmentada gràcies a la propietat de verificabilitat de les terceres parts.

Per acabar, volem apuntar dues línies de futur del nostre treball. D'una banda, l'anàlisi dels serveis de seguretat de les TTPs que hem fet en el capítol 4 ens ajuda a considerar distints aspectes de la intervenció de les terceres parts en els protocols de seguretat: podem considerar una característica en particular i intentar canviar el protocol perquè també canviï el tipus de servei de la TTP si ens interessa aconseguir una propietat en particular. No obstant això, queda una línia oberta per poder aconseguir un sistema que sigui capaç d'unir els distints tipus de servei i poder-los ponderar en funció de les necessitats de cada usuari, d'aquesta manera obtendrem un sistema íntegra d'avaluar el

servei d'una TTP en un protocol de seguretat. D'altra banda, la segona línia de futur que apuntam és la implementació dels protocols de seguretat que hem proposat amb la intenció d'estudiar els problemes que a partir d'aquí es puguin plantejar referents a la verificabilitat de les TTPs. Mitjançant aquestes implementacions s'haurà d'investigar, entre altres coses, la compatibilitat de la verificabilitat de la TTP amb aspectes pràctics com és el tipus de canal de comunicació establert entre usuaris i TTP o amb qüestions temporals com, per exemple, el temps que la tercera part ha de mantenir les dades en els directoris públics que hem descrit en els protocols presentats a la tesi.

Bibliografia

[AGH02] M. Abadi, N. Glew, B. Horne, B. Pinkas: “Certifies Email with a Light On-line Trusted Third Party: Design and Implementation,” 11th International World Wide Web Conference, pp. 387-395, Hawaii 2002.

[AMG01] G. Ateniese, B. de Medeiros, M. T. Goodrich: “TRICERT: Distributed Certified E-mail Schemes,” ISOC 2001, Network and Distributed System Security Symposium (NDSS'01), San Diego 2001.

[ASW97] N. Asokan, M. Schunter, M. Waidner: “Optimistic protocols for fair exchange,” 4th ACM Conference on Computer and Communications Security, pp. 7-17, ACM Press, Zurich 1997.

[ASW98] N. Asokan, V. Shoup, M. Waidner: “Asyncronous Protocols for Optimistic Fair Exchange,” IEEE Symposium on Research in Security and Privacy, pp. 86-99, Oakland 1998.

[AT94] J. Alireza Bahreman, J.D. Tygar: “Certified electronic mail,” Symposium on Network and Distributed Systems Security, Internet Society, pp. 3-19, San Diego 1994.

[B79] G.R. Blakley: “Safeguarding Cryptographic Keys,” National Computer Conference, American Federation of Information Processing Societies, v.48, pp. 242-268, New York 1979.

[B83] M. Blum: “How to exchange (secret) keys,” STOC’83 Symposium on Theory of Computing, pp. 440-447, Boston 1983.

[B94] S. Brands: “Untraceable off-line cash in wallet with observers,” Advances in Cryptology-CRYPTO’93, LNCS 773, pp. 302-318, Springer Verlag 1994.

[BBC94] J. Boly, A. Bosselaers, R. Cramer, R. Michelsen, S. Mjølsnes, F. Muller, T. Pedersen, B. Pfitzmann, P. de Rooij, B. Schoenmakers, M. Schunter, L. Vallée, M. Waidner: “The ESPRIT Project CAFE - High Security Digital Payment Systems-,” ESORICS’94, LNCS 875, pp. 217-230, Springer Verlag 1994.

[BGM90] M. Ben-Or, O. Goldreich, S. Micali, R. L. Rivest: “A fair protocol for signing contracts,” IEEE Transactions on Information Theory, v. 36, n.1, pp. 40-46, IEEE Press 1990.

[C82] D. Chaum: “Blind Signatures for Untraceable Payments,” Advances in Cryptology, Proceedings of Crypto’82, pp. 199-203, Plenum Press 1982.

[C94] D. Chaum: “Designated Confirmer Signatures,” Advances in Cryptology-EUROCRYPT’94, LNCS 950, pp. 86-91, Springer Verlag 1994.

[C04] P. Cofta: “Computing Recommendations to Trust,” 2nd International Conference iTrust 2004, LNCS 2995, pp. 340-346, Springer Verlag 2004.

[CC03] P. Cofta, S. Crane: “Toward the Intimate Trust Advisor,” 1st International Conference iTrust 2003, LNCS 2692, pp. 123-135, Springer Verlag 2003.

[CC97] L. Cranor, R. Cryton: “Sensus: A Security-Conscious Electronic Polling System,” Hawaii International Conference on System Sciences, Hawaii 1997.

[CEF03] B. Crispo, S. Etalle, W.J. Fokkink: “Accountability in Electronic Commerce Protocol,” Research Proposal. Computer Science Competition 2003. Universiteit Twente, Neederland 2003.

[CFN89] D. Chaum, A. Fiat, M. Naor: “Untraceable Electronic Cash,” Advances in Cryptology-CRYPTO’88, LNCS 403, pp. 319-327, Springer-Verlag 1989.

[CG04] J. Carracedo Gallardo: *Seguridad en Redes Telemáticas*. Ed. McGraw-Hill/Interamericana, Madrid 2004.

[CIV00] California Internet Voting Task Force: *A Report on the Feasibility of Internet Voting*, January 2000. Disponible electrònicament a l’URL: http://www.electioncenter.org/voting/voting_report.html

[CLM00] B. Crispo, P. Landrock, V. Matyas Jr.: “WWW Security and Trusted Third Party Services,” Future Generation Computer Systems, v. 4, n. 16, pp. 331-341, Elsevier Science 2000.

[CPS96] J. Camenish, J.M. Piveteau, M. Stadler: “An Efficient Fair Payment System,” 3rd ACM Conference on Computer and Communications Security, pp. 88-94, ACM Press 1996.

[CR96] B. Crispo, G. Ruffo: “Reasoning about Accountability within Delegation,” 1st Security Protocols Workshop, LNCS 1189, pp. 19-32, Spinger Verlag 1996.

[CS96] T. Coffey, P. Saidha: “Non-repudiation with mandatory proof of receipt,” ACM SIGCOMM: Computer Communication Review, v. 26, n. 1, pp. 6-17, ACM Portal 1996.

[D93] I.B. Damgard: “Practical and provably secure release of a secret and exchange of signatures,” Advances in Criptology-EUROCRYPT’93, LNCS 765, pp. 200-217, Spinger Verlag 1993.

[D95] D.E. Denning: “The Key Escrow Encryption Technology,” recollit a Hoffman E.J., editor; *Building in Big Brother, The Cryptographic Policy Debate*. Springer Verlag 1995.

[DF93] J. Domingo Ferrer: “Unstransferable rights in a client-independent server environment,” Advances in Criptology-EUROCRYPT’93, LNCS 765, pp. 260-266, Spinger Verlag 1993.

[DFT97] G. Davida, Y. Frankel, Y. Tsiounis, M. Yung : “Anonymity Control in e-cash Systems,” Financial Cryptography’97, LNCS 1318, pp. 1-16, Springer Verlag 1997.

[DGL96] R.H. Deng, Li Gong, A.A. Lazar, W. Wang: “Practical protocols for certified electronic mail,” Journal on Network and Systems Management: Special Issue on Network Security Management, v. 4, n. 3, pp. 279-297, 1996.

[DH99] J. Domingo Ferrer, J. Herrera Joancomartí: *Criptografia per als serveis telemàtics i el comerç electrònic*. Publicacions de la Universitat Oberta de Catalunya SL., Barcelona 1999.

[E82] S. Even: "A protocol for signing contracts," Computer Science Departament, Technion, Technical Report 231, Haifa 1982.

[EGL85] S. Even, O. Goldreich, A. Lempel: "A Randomized Protocol for Signing Contracts," Communications of the ACM, v. 28, n. 6, pp. 637-647, Association for Computing Machinery 1985.

[ETS97] European Commission Information Society DG XIII/C.4. European Trusted Services (ETS) Studies, Final Report: *Standardisation Issues for the European Trust Services*, Quercus Information Ltd., May 1997. Disponible electrònicament a l'URL: http://www.cordis.lu/infosec/src/ets.htm

[ETSI97] European Telecommunications Standards Institute. ETSI EG/SEC-003000, *Requirements for Trusted Third Party Services* (Edition 1), Version 7.0, July 1997.

[EY80] S. Even, Y. Yacobi: "Relations among public key signature systems," Computer Science Departament, Technion, Technical Report 175, Haifa 1980.

[F93] N. Ferguson: "Single term off-line coins," CWI (Centre for Mathematics and Computer Science), Technical Report CS-R9318, Amsterdam 1993.

[F94] W. Ford: *Computer Communications Security - Principles, Standard Protocols and Techniques*. PTR Prentice Hall, Englewood Cliffs, New Jersey 1994.

[FKK96] A.O. Freier, P. Karlton, P.C. Kocher: "The SSL Protocol Version 3.0," INTERNET-DRAFT, November 1996. Disponible electrònicament a l'URL: http://wp.netscape.com/eng/ssl3/ssl-toc-html

[FHM98] J.Ll. Ferrer Gomila, Ll. Huguet i Rotger, M. Mut Puigserver: "Protocolo de correo electrónico certificado," V Reunión Española de Criptología, pp. 383-395, Málaga 1998.

[FMH00] J.Ll. Ferrer Gomila, M. Mut Puigserver, Ll. Huguet i Rotger: "Un protocolo eficiente para el intercambio equitativo de valores," VI Reunión Española de Criptología, pp. 233-242, Islas Canarias 2000.

[FNMT] Autoridad Pública de Certificación de la Fábrica Nacional de Moneda y Timbre, *Certificación electrónica X.509 v3 para uso en el ámbito tributario*. Disponible electrònicament a l'URL: http://www.cert.fnmt.es/

[FOO93] A. Fujioka, T. Okamoto, K. Ohta: "A Practical Secret Voting Scheme for Large Scale Elections," Advances in Cryptology-AUSCRYPT'92, LNCS 718, pp. 244-251, Springer Verlag 1993.

[FPH00] J.L. Ferrer Gomila, M. Payeras Capellà, Ll. Huguet i Rotger: "An Efficient Protocol for Certified Electronic e-mail," International Security Conference ISC2000, LNCS 1975, pp. 237-248, Spinger Verlag 2000.

[FR95] M.K. Franklin, M.K. Reiter: “The design and implementation of a secure auction service,” IEEE Symposium on Security and Privacy, pp. 2-14, Oakland 1995.

[FRH94] J.L. Ferrer Gomila, À. Rotger, Ll. Huguet i Rotger: “Firma electrónica de contratos,” III Reunión Española de Criptología, pp. 139-144, Barcelona 1994.

[G84] O. Goldreich: “A simple protocol for signing contracts,” Advances in Cryptology-CRYPTO’83, pp. 133-136, Plenum Press 1984.

[G93] Li Gong: “Increasing Availability and Security of an Authentication Service,” IEEE Journal on Selected Areas in Communications, v. 11, n. 5, IEEE Press 1993.

[G00] D. Gambetta: “Can We Trust Trust?,” Trust: Making and Breaking Cooperative Relations, pp. 213-237, Departament of Sociology, University of Oxford 2000.

[GKM97] R. Gennaro, P. Kerger, S. Matyas, M. Peyravian, A. Roginsky, D. Safford, M. Willett, N. Zunic: “Two-Phase Cryptographic Key Recovery System,” Computers & Security, v. 16, n.6, pp. 481-506, Elsevier Ltd.1997.

[GJM99] J.A. Garay, M. Jakobsson, P. MacKenzie: “Abuse-free Optimistic Contract Signing,” 19th Annual International Cryptology Conference on Advances in Cryptology-CRYPTO’99, LNCS 1666, pp. 449-466, Springer Verlag 1999.

[GSM] GSM Security Standards. Disponibles electrònicament a l’URL: http://www.gsm-security.net/gsm-security-standards

[H96] Y. Han: “Investigation of non-repudiation Protocols,” ACISP’96: Information Security and Privacy: Australasian Conference, LNCS 1172, pp. 38-47, Springer Verlag 1996.

[IEC] Institut d’Estudis Catalans: *Diccionari de la llengua catalana.* Enciclopèdia Catalana, Barcelona 1998.

[IM04] T. Ihaya, D. P. Mundy: “Trust Developement and Management in Virtual Communities,” 2nd International Conference iTrust 2004, LNCS 2995, pp. 266-276, Springer Verlag 2004.

[IPI] Internet Policy Institute. *Report of the National Workshop on Internet Voting: Issues and Research Agenda*. March 2001. Disponible electrònicament a l’URL: http://www.internetpolicy.org

[ISO7498] ISO/IEC 7498: “Basic Reference Model for Open Systems Interconnection,” 1994.

[ISO7498-2] ISO/IEC 7498-2: “Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture,” 1989.

[ISO11770-1] ISO/IEC 11770-1: “Information technology – Security techniques – Key Management – Part 1: Framework,” 1996.

[ISO13335-1] ISO/IEC 13335-1: “Information technology – Security techniques – Management of information and communications technology security – Part

1: Concepts and models for information and communications technology security management," 2004.

[ISO13335-3] ISO/IEC TR 13335-3: "Information technology – Guidelines for the management of IT Security – Part 3: Technics for the management of IT Security," 1998.

[ISO13335-4] ISO/IEC TR 13335-4: "Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards," 2000.

[ISO13335-5] ISO/IEC TR 13335-5: "Information technology – Guidelines for the management of IT Security – Part 5: Management guidance on network security," 2001.

[ISO13888-1] ISO/IEC 13888-1: "Information technology – Security techniques – Non-repudiation - Part 1: General," 2004.

[ISO13888-2] ISO/IEC 13888-2: "Information technology – Security techniques – Non-repudiation - Part 2: Mechanisms using symmetric techniques," 1998.

[ISO13888-3] ISO/IEC 13888-3: "Information technology – Security techniques – Non-repudiation – Part 3: Using asymmetric techniques," 1997.

[ISO18014-2] ISO/IEC 18014-2: "Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens," 2002.

[JL04] A. Josang, S. Lo Presti: "Analysing the Relationship Between Riesk and Trust," 2nd International Conference iTrust 2004, LNCS 2995, pp. 135-145, Springer Verlag 2004.

[JZF03] R. Joaquim, A. Zuquete, P. Ferreira: "REVS A Robust Electronic Voting System," IADIS International Conference e-Society, Lisbon 2003.

[KM00] S. Kremer, O. Markowitch: "Optimistic non-repudiable information exchange," J. Biemond (Ed.), 21st Symposium On Information Theory in the Benelux, Werkgemeenschap Informatie en Communicatietheorie, pp. 139-146, Wassenaar 2000.

[KMZ02] S. Kremer, O. Markowitch, J. Zhou: " An Intensive Survey of Non-repudiation Protocols," *Computer Communication Journal*, v. 25, n. 17, pp. 1606-1621, Elsevier Science 2002.

[KNT94] J.T. Kohl, B Neuman, T. Ts'o: "The Evolution of the Kerberos Authentication Service," in F. Brazier and D. Johansen, editors: *Distributed Open Systems*. pp. 78-94, IEEE Computer Society Press 1994.

[KR03] M. Kinateder, K. Rothermel: "Architecture and Algorithms for a Distributed Reputation System," 1st International Conference iTrust 2003, LNCS 2692, pp. 1-17, Springer Verlag 2003.

[LAK02] M. Lee, G. Ahn, J. Kim, J. Park, B. Lee, K. Kim, H. Lee: "Design and Implementation of an Efficient Fair Off-line E-Cash System based on Elliptic Curve Discrete Logarithm Problem," Journal of Communication and Networks, v. 4, n. 2, KICS and IEEE ComSoc 2002.

[MFH00] M. Mut Puigserver, J.Ll. Ferrer Gomila, Ll. Huguet i Rotger: “Certified Electronic Mail Protocol Resistant to a Minority of Malicious Third Parties,” IEEE INFOCOM 2000, pp. 1401-1405, Tel Aviv 2000.

[MFH02] M. Mut Puigserver, J.Ll. Ferrer Gomila, Ll. Huguet i Rotger: “Terceras partes de confianza. Clasificación de los servicios de seguridad,” VII Reunión Española sobre Criptologia y Seguridad de la Información, pp. 657-669, Oviedo 2002.

[MFH03] M. Mut Puigserver, J.Ll. Ferrer Gomila, Ll. Huguet i Rotger: “Trusted Verifiable Services,” Workshop on Security of Information Technology, pp. 43-52, Alger 2003.

[MFH04] M. Mut Puigserver, J.Ll. Ferrer Gomila, Ll. Huguet i Rotger: “A Voting System with Trusted Verifiable Services,” The 2004 International Conference on Computational Science and Its Applications ICCSA 2004, LNCS 3043, pp. 924-937 , Springer Verlag 2004.

[MFH05] M. Mut Puigserver, J.Ll. Ferrer Gomila, Ll. Huguet i Rotger: “Certified e-mail Protocol with Verifiable Third Party,” IEEE International Conference on e-Technology, e-Commerce and e-Service EEE’05, pp. 548-551, Hong Kong 2005.

[MK01] O. Markowitch, S. Kremer: “An Optimistic Non-repudiation Protocol with Transparent Trusted Third Party,” International Conference on Information Security, LNCS 2200, pp. 363-378, Springer Verlag 2001.

[MMH02] L. Mui, M. Mohtashemi, A. Halberstadt: “A Computational Model of Trust and Reputation,” 35th Hawaii International Conference on System Sciences, Hawaii 2002.

[MR99] O. Markowitch, Y. Roggeman: “Probabilistic non-repudiation without Trusted Third Party,” 2nd Conference on Security in Communication Networks’99, Amalfi 1999.

[MW97] J.K. Mackie-Mason, K. White: “Evaluating and Selecting Digital Payment Mechanisms,” Interconnection and the Internet, pp: 113-134, G. Rosston and D. Waterman, eds. Lawrence Erlbaum, 1997. Selected papers from the 1996 Telecommunications Policy Research Conference.

[MOV97] A. Menezes, P. Oorshcot, S. Vanstone: *Handbook of Applied Cryptography*. FL: CRC Press 1997.

[N97] Å. Nilson: “European Trusted Services(ETS)- Results of 1995 TTPs Projects,” Marinade Ltd., London SE1 2NE, U.K., 1997.

[NS78] R. Needam, M. Shroeder: “Using Encripition for Authentication in Large Networks of Computers,” Communications of the ACM, v. 12, n. 21, pp. 993-999, Association for Computing Machinery 1978.

[NSS91] H. Nurmi, A. Salomaa, L. Santean: “Secret Ballot Elections in Computer Networks,” Computer & Security, vol. 10, pp. 553-560, Elsevier Ltd. 1991.

[OII98] European Commission Information Society EC DGXIII/E. Open Information Interchange (OII) service: "OII Guide to Trust Services," 1998. Disponible electrònicament a l'URL: http://www.diffuse.org/oii/en/trust.html

[OO94] T. Okamoto, K. Ohta: "How to simultaneuosly exchange secrets by general assumptions," IEEE Symposium on Research in Security and Privacy, pp. 14-28, November 1994.

[OP98] European Commission DGXIII: "ETS preparatory actions. Project OPARATE (OPerational and ARchitectural Aspects of TTPs for Europe)," 1998.

[PFH02] M. Payeras Capellà, J.L. Ferrer Gomila, Ll. Huguet i Rotger: "Moneda Electrónica Totalmente Anónima e Indetectable," VII Reunión Española sobre Criptología y Seguridad de la Información, pp. 699-711, Oviedo 2002.

[PP97] H. Petersen and G. Poupard: "Efficient scalable fair cash with off-line extortion prevention," International Conference on Information and Communication Security (ICICS'97), LNCS 1334, pp. 463-477, Springer Verlag 1997.

[RBP91] J. Rumbaugh, M. Blaha, W. Premerlani, F. Eddy, W. Lorensen: *Object-Oriented Modeling and Design*, Prentice-Hall, Inc. 1991.

[RFC959] RFC 959, *File Transfer Protocol* (*FTP*), The Internet Society 1995.

[RFC2527] RFC 2527, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, The Internet Society 1999.

[RFC3161] RFC 3161, *Internet X.509 Public Key Infrastructure Time-Stamp Protocol* (*TSP*), The Internet Society 2001.

[RH91] J. Rifà i Coma, Ll. Huguet i Rotger: *Comunicación Digital. Teoria matemática de la información. Codificación algebraica. Criptologia.* Ed. Masson, S. A., Barcelona 1991.

[RHOA] R. Rivest, M. Herschberg, K. Ohta, B. Adida, B. Durette, R. Greenstadt and K. Mcald. *Cryptography and Information Security Group Research. Project Electronic Voting: eVox*. Disponible electrònicament a l'URL: http://theory.lcs.mit.edu/~cis/voting/voting.html

[RRN01] I. Ray, I. Ray, N. Narasimhamurthi: "An Anonymous Electronic Voting Protocol for Voting Over The Internet," IEEE 3rd International Workshop on Advanced Issues of E-Commerce and Web-Based Information System, San Juan 2001.

[RSA78] R. Rivest, A. Shamir, L. Adleman: "A method for obtaining digital signatures and public key cryptosystems," Communications of the ACM, v.21, n. 2, pp. 120-126, Association for Computing Machinery 1978.

[S79] A. Shamir: "How to Share a Secret," Communications of the ACM, v. 24, n. 11, pp. 612-613, Association for Computing Machinery 1979.

[S91] Schnorr, C.P.: "Efficient Signature Generation by Smart Cards," Journal of Criptology, v. 4, n. 3, pp. 161-174. Springer Verlag 1991.

[S95] W. Stallings: *Network and internetwork security: principles and practice*. Prentice Hall, Englewood Cliffs, New Jersey. IEEE Press 1995.

[S96] B. Schneier: *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Ed. John Wiley & Sons, Inc. 1996.

[S02] D. Stinson: *Cryptography: Theory and Practice*. FL: CRC Press 2002.

[SET97] Visa International and Mastercard International: *SET Secure Electronic Transaction* (*TM*) *Specification*. Version 1.0, 1997.

[SK95] K. Sako, J. Kilian: "Receipt-free mix-type voting scheme – a practical solution to the implementation of a voting both–," Advances in Cryptology-EUROCRYPT'95, LNCS 921, pp. 393-403, Springer Verlag 1995.

[SM02] V. Shmatikov and J.C. Mitchell: "Finite-State Analysis of Two Contract Signing Protocols," Theoretical Computer Science (TCS), special issue on Theoretical Foundations of Security Analysis and Design (ed. R. Gorrieri), v. 283, n.2, pp. 419-450, Elsevier Ltd. 2002.

[S/MIME] Secure/Multipart Internet Mail Extensions (S/MIME): series of Proposed Standards by The Internet Engineering Task Force S/MIME Mail Security Working Group. Disponible electrònicament a l'URL: http://www.imc.org/ietf-smime/

[TEDIS94] TEDIS II: "Security in open environtments," TEDIS II, B7, ver. 15, July 1994.

[TM03] P. Nixon, S. Terzis (Eds): *Proceedings of Trust Management, 1st International Conference, iTrust 2003*. LNCS 2692, Springer-Verlag 2003.

[TM04] C. Jensen, S. Poslad, T. Dimitrakos (Eds.): *Proceedings of Trust Management, 2nd International Conference, iTrust 2004*. LNCS 2995, Springer-Verlag 2004.

[VITS] Verisign Internet Trust Services. Disponible electrònicament a l'URL: http://www.verisign.com/

[X.400] ITU-T Recommendation X.400 (1996), Message Handling System and service overview.

[X.500] ITU-T Recommendation X.500 (1997), Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services.

[X.509] ITU-T Recommendation X.509 (2001) | ISO/IEC 9594-8:2001, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

[X.800] ITU-T Recommendation X.800 (1991), Security Architecture for Open Systems Interconnection for CCITT applications.

[X.810] ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, Information technology – Open Systems Interconnection – Security Frameworks for Open Systems: Overview.

[X.813] ITU-T Recommendation X.813 (1996) | ISO/IEC 10181-4:1997, Information technology – Open Systems Interconnection – Security Frameworks for Open Systems: Non-repudiation framework.

[X.842] ITU-T Recommendation X.842 (2000) | ISO/IEC TR 14516, Information technology – Security Techniques – Guidelines for the Use and Management of Trusted Third Party Sevices.

[Z03] J. Zhou: “A fair non-repudiation protocol,” ACNS'2003 International Conference on Applied Cryptography and Network Security. Tutorial disponible electrònicament a l’URL: http://acns2003.i2r.a-star.edu.sg/ACNS03-program.html

[ZDB99] J. Zhou, R. H. Deng, F. Bao: “Evolution of Fair Non-repudiation with TTP,” ACISP’99: Information Security and Privacy: Australasian Conference, LNCS 1587, pp. 258-269, Springer Verlag 1999.

[ZG96a] J. Zhou, D. Gollmann: “A fair non-repudiation protocol,” IEEE Symposium on Research in Security and Privacy, pp. 55-61, Oakland 1996.

[ZG96b] J. Zhou. D. Gollmann: “Observations on non-repudiation,” Advances in Cryptology-ASIACRYPT’96, LNCS 1163, pp. 133-144, Springer Verlag 1996.

[ZG97] J. Zhou, D. Gollmann: “An Efficient Non-repudiation Protocol,” 10th IEEE Computer Security Foundation Workshop, pp. 126-132, Rockport 1997.

Publicacions Pròpies Relacionades

[FHM98] J.Ll. Ferrer Gomila, Ll. Huguet i Rotger, M. Mut Puigserver: “Protocolo de correo electrónico certificado,” V Reunión Española de Criptología, pp. 383-395, Málaga 1998.

[MFH00] M. Mut Puigserver, J. Ll. Ferrer Gomila, Ll. Huguet i Rotger: “Certified Electronic Mail Protocol Resistant to a Minority of Malicious Third Parties,” IEEE INFOCOM 2000, pp. 1401-1405, Tel Aviv 2000.

[FMH00] J.Ll. Ferrer Gomila, M. Mut Puigserver, Ll. Huguet i Rotger: “Un protocolo eficiente para el intercambio equitativo de valores,” VI Reunión Española de Criptología, pp. 233-242, Islas Canarias 2000.

[MFH02] M. Mut Puigserver, J.L. Ferrer Gomila, Ll. Huguet i Rotger: “Terceras partes de confianza. Clasificación de los servicios de seguridad,” VII Reunión Española sobre Criptologia y Seguridad de la Información, pp. 657-669, Oviedo 2002.

[MFHP03] M. Mut Puigserver, J.L. Ferrer Gomila, Ll. Huguet i Rotger, M. Payeras Capellà: “Análisis de los sistemas de dinero electrónico. Mejoras al esquema de Brands,” II Simposio Español de Comercio Electrónico, pp. 109-116, Barcelona 2003.

[MFH03] M. Mut Puigserver, J.L. Ferrer Gomila, Ll. Huguet i Rotger: “Trusted Verifiable Services,” Workshop on Security of Information Technology, pp. 43-52, Alger 2003.

[MFH04] M. Mut Puigserver, J.L. Ferrer Gomila, Ll. Huguet i Rotger: “A Voting System with Trusted Verifiable Services,” The 2004 International Conference on Computational Science and Its Applications ICCSA 2004, LNCS 3043, pp. 924-937 , Springer Verlag 2004.

[MFHP04] M. Mut Puigserver, J.L. Ferrer Gomila, Ll. Huguet i Rotger, M. Payeras Capellà: “Verificabilidad en Protocolos de Intercambio Equitativo,” VIII Reunión Española sobre Criptologia y Seguridad de la Información, pp. 279-289, Madrid 2004.

[MFH05] M. Mut Puigserver, J.L. Ferrer Gomila, Ll. Huguet i Rotger: “Certified e-mail Protocol with Verifiable Third Party,” IEEE Iternational Conference on e-Technology, e-Commerce and e-Service EEE’05, pp. 548-551, Hong Kong 2005.

[MFH05b] M. Mut Puigserver, J.L. Ferrer Gomila, Ll. Huguet i Rotger: “Protocolos de seguridad con TTP verificable,” III Simposio Español de Comercio Electrónico, pp. 83-94, Palma de Mallorca 2005.