Correu electrònic certificat

Josep Lluís Ferrer Gomila
Llorenç Huguet Rotger
M. Magdalena Payeras Capellà

PID_00199772

UOC
Universitat Oberta de Catalunya

Índex

Introducció

El correu electrònic és un dels serveis més utilitzats de la xarxa Internet. Malgrat el caràcter asíncron que té (no cal que remitent i destinatari estiguin connectats simultàniament), la immediatesa, facilitat d'ús, etc. han fet que substitueixi sovint el correu convencional en paper.

En els orígens el correu electrònic d'Internet presentava dos greus inconvenients. D'una banda, només es podien transmetre informacions que es corresponguessin amb caràcters ASCII de 7 bits. No era possible enviar arxius, imatges, etc., de manera còmoda. D'altra banda, el correu no incorporava cap servei de seguretat.

El primer problema va quedar resolt amb l'adveniment de l'estàndard MIME (*multi-purpose Internet mail extensions*). El segon problema es va resoldre amb l'estàndard S/MIME (*secure/MIME*). Però aquest darrer estàndard només resolia els problemes bàsics de seguretat: confidencialitat, autenticitat, integritat i no-repudi en origen. Però un dels serveis de què disposem en el món en paper, el correu electrònic certificat, no va quedar resolt amb S/MIME.

Com la signatura electrònica de contractes, el correu electrònic certificat forma part del conjunt de problemes que de manera genèrica rep el nom d'*intercanvi equitatiu de valors*. En aquest cas els objectes que s'intercanvien són un missatge (i probablement un element que permeti garantir el no-repudi en origen) per un acusament de recepció del destinatari.

El requisit que ha de complir qualsevol protocol per al correu electrònic certificat és l'equitat. És a dir, que o remitent i destinatari reben el que esperen al final de l'intercanvi, o cap d'ells estarà en una posició avantatjosa al final d'aquest intercanvi.

> La propietat fonamental dels protocols de correu electrònic certificat és l'equitat: que cap de les parts no es trobi en una situació de desavantatge després de finalitzar l'execució del protocol de correu certificat.

La solució en el món en paper es basa en l'existència d'entitats (com poden ser els agents de correus o els agents judicials) que, amb el lliurament de manera presencial, permet garantir que cada part obtingui el que està esperant, sense assumir el risc de proporcionar la seva sense rebre la de la contrapart. Òbviament, en el món electrònic no podem fer l'intercanvi cara a cara, però sí que podem disposar d'entitats electròniques de confiança. Com en el cas de

la signatura electrònica de contractes, hem de proporcionar solucions alternatives però que permetin mantenir (o millorar) els nivells de seguretat del món en paper.

Les solucions per al correu electrònic certificat, com passava amb la signatura electrònica de contractes, se solen classificar en funció de si intervé o no una tercera part de confiança (TTP, de l'anglès *trusted third party*), i si hi intervé, com ho fa (en tots els correus, si sorgeixen problemes, etc.). Per això, exposarem solucions amb la implicació diferent d'una TTP i solucions sense TTP.

En aquest mòdul s'observarà que es repeteixen moltes explicacions que ja s'han fet en el de signatura electrònica de contractes. Això és perquè, com hem dit, tots dos problemes formen part de la mateixa família: l'intercanvi equitatiu de valors. S'ha optat per mantenir les repeticions, en lloc de fer contínues referències al mòdul de signatura electrònica de contractes, per permetre'n una lectura independent (només en la solució sense TTP s'ha obviat la repetició del protocol "cara o creu").

1. Solucions per al correu electrònic certificat amb TTP

La classificació feta en la introducció respecte de les TTP es pot refinar més, segons el grau d'intervenció de la TTP en l'execució dels protocols per al correu electrònic certificat. Així, parlem de protocols per al correu electrònic certificat amb:

- TTP *in-line*, quan la TTP intervé en tots els passos de l'execució del protocol.
- TTP *on-line*, quan la TTP intervé en totes les execucions del protocol de correu electrònic certificat, però no en tots els passos d'aquest.
- TTP *off-line*, quan la TTP només intervé en cas que hi hagi conflictes o problemes entre les parts, és a dir, sota demanda d'una o més d'aquestes; per tant, en aquest tipus de protocols la TTP no intervé de manera genèrica, i també reben el nom de *protocols optimistes*.

Ara ens centrarem en el correu electrònic certificat entre dues parts, és a dir, un remitent i un destinatari que volen intercanviar un missatge per un acusament de recepció.

Abans de començar amb la descripció dels protocols, procedirem a descriure la notació per a designar els actors que usarem. Els actors que hi intervindran són, d'una banda, el remitent i el destinatari, que denominarem A(lice) i B(ob), respectivament, i d'altra banda tenim la tercera part de confiança, que denominarem T. En alguna ocasió etiquetarem el remitent com a R(emitent).

Solucions amb TTP *in-line* i *on-line*

Començarem amb la que es pot considerar com la solució més senzilla possible, utilitzant una TTP *in-line*. A i B han d'enviar el missatge i l'acusament de recepció a la TTP. Una vegada la TTP disposa dels dos elements, procedeix a verificar que són correctes i, si és el cas, retransmet l'element de A a B, i el de B a A. En primer lloc, el remitent A envia el missatge a la TTP:

$$\mathrm{A} \rightarrow \mathrm{T}: M, Sign_A(M)$$

A continuació la TTP ha d'indicar a B que té un correu certificat pendent de ser rebut. No li pot enviar directament aquest missatge, ja que estaríem assumint el risc que, un cop llegit, B es negui a enviar l'acusament de recepció. Per això la TTP envia el missatge xifrat amb una clau que només ella coneix:

$$\mathrm{T} \rightarrow \mathrm{B}: c = E_k(M)$$

Ara B ha de procedir a enviar l'acusament de recepció:

$$\text{B} \rightarrow \text{T: } AR_B = Sign_B(c)$$

En aquest moment la TTP disposa del missatge que li ha proporcionat A i de l'acusament de recepció que li ha proporcionat B. A continuació, una vegada garantida la possible equitat de l'intercanvi, procedeix a retransmetre la informació que estan esperant cada una de les parts:

$\text{T} \rightarrow \text{A: } AR_B$
$\text{T} \rightarrow \text{B: } k, Sign_T(k)$

Un cop que B hagi rebut la clau k, podrà procedir a desxifrar el criptograma c que havia rebut anteriorment:

$$\text{B: } D_k(c) = M$$

Noteu que en aquest senzill protocol la TTP és la que proporciona les garanties que l'intercanvi sigui equitatiu. Fins que no disposa dels objectes de les dues parts, no els retransmet. Per tant, es compleix la propietat d'equitat.

Vegem ara una variació del protocol anterior, per observar com seria un protocol per al correu electrònic certificat amb TTP *on-line*. En aquest cas algunes de les comunicacions seran directament entre remitent i destinatari, i en d'altres participarà la TTP. En primer lloc, A envia el missatge xifrat amb una clau secreta k a B:

$$\text{A} \rightarrow \text{B: } c = E_k(M), Sign_A(c)$$

D'aquesta manera és A directament qui fa saber a B que li vol enviar un correu certificat. Per evitar que pugui fer trampes en un futur i deixar B sense poder llegir el missatge, ha de retransmetre la clau que ha utilitzat per a fer el xifratge a la TTP:

$$\text{A} \rightarrow \text{T: } k, Sign_A(k)$$

D'altra banda, B ha de decidir si vol rebre el correu certificat (entenem que és impossible obligar B a rebre un missatge). Si és el cas, ha d'enviar un acusament de recepció, bé a A o bé a la TTP. Per simplificar l'explicació suposarem que el remet a la TTP:

$$\text{B} \rightarrow \text{T: } AR_B = Sign_B(c)$$

En aquest moment la TTP disposa dels elements que volen intercanviar les dues parts: la clau k que permet llegir el missatge i l'acusament de recepció AR_B. A continuació la TTP ha de retransmetre els elements a A i B:

$\text{T} \rightarrow \text{B: } k, Sign_A(k)$
$\text{T} \rightarrow \text{A: } AR_B = Sign_B(c)$

Per tant, A i B disposaran dels elements que esperaven, i la intervenció de la TTP (en aquest cas *on-line* perquè no ha intervingut en cada pas) ha garantit l'equitat de l'intercanvi.

Amb aquests exemples senzills detectem alguns inconvenients generals de les solucions amb TTP *in-line* i *on-line* (més accentuat en les primeres), i alguns de particulars de les solucions concretes presentades.

D'una banda, el fet que la TTP hagi d'intervenir en cada intercanvi pot representar un problema de coll d'ampolla pel que fa a les comunicacions amb aquesta, o en qualsevol cas la intervenció en cada execució pot encarir el servei de correu electrònic certificat. Per això se solen preferir aquelles solucions que no requereixen una participació en totes les execucions de la TTP.

Un altre aspecte que cal considerar és la confiança que cal dipositar en la TTP, com a mínim des de dos punts de vista. D'una banda, és fàcil observar que la TTP pot afavorir una de les parts, proporcionant l'acusament de recepció, per exemple, de B a A i no el missatge de A a B. Això conduiria a una situació no equitativa per culpa de la TTP.

D'altra banda, tal com s'ha dissenyat el protocol, la TTP té accés a tota la informació relacionada amb el contingut del missatge; per tant, la privacitat i el secret de la transacció queda també en mans de la TTP, que la pot difondre a tercers sense el coneixement de A i B.

Solució amb TTP *off-line* asíncrona

Per a resoldre alguns dels problemes indicats anteriorment, explicarem a continuació una solució optimista o amb TTP *off-line*. En aquesta solució apareixeran tres subprotocols: un subprotocol d'intercanvi, un de cancel·lació i un de finalització. Començarem explicant el d'intercanvi. Els passos que cal seguir són els següents:

A → B: $c = E_k(M), K = PU_T(k), Sign_A(c,K)$
B → A: $AR_B = Sign_B(c)$
A → B: $k, Sign_A(k)$

Una vegada intercanviada la informació anterior s'ha proporcionat el servei de correu electrònic certificat. Per a A l'acusament de recepció és senzillament la signatura de B sobre el criptograma rebut en la primera transmissió, i B rep en la primera transmissió el missatge xifrat amb una clau secreta k que en aquest moment desconeix, però que li proporcionen en el tercer enviament.

En la proposta anterior es pot observar una millora que introduïm respecte del correu certificat convencional en paper. En el correu certificat en paper típicament signem un acusament de recepció a canvi d'un sobre que suposadament

conté un document a l'interior. Però pot passar que el sobre no contingui res, o que contingui un document sense cap tipus de signatura del remitent, és a dir, que en el moment concret d'expedir l'acusament de recepció no tenim constància explícita de què ens estem comprometent a rebre.

En el protocol presentat, en el primer pas, el remitent A fa una signatura electrònica sobre el criptograma que transmet a B, i també sobre la clau que envia xifrada amb la clau pública de la TTP. Aquesta signatura no li permetrà negar *a posteriori* haver enviat aquesta informació concreta i no cap altra.

D'altra banda, l'acusament de recepció que expedeix B està directament vinculat al criptograma que ha rebut en el pas anterior. Per tant, B no emet un acusament de recepció genèric i arbitrari, sinó un acusament de recepció vinculat directament al missatge que A s'ha compromès a posar a disposició seva.

Finalment, el remitent envia la clau que permetrà fer el desxifratge del criptograma del primer pas, però un cop més acompanya aquesta transmissió amb una signatura de A, que farà que no pugui negar *a posteriori* haver enviat aquesta clau i no cap altra. Per aquest motiu, si A intenta fer trampes en el darrer pas, proporcionant una clau que no permeti llegir el missatge, no trencarà l'equitat de l'intercanvi: B podrà demostrar el comportament deshonest de A.

En qualsevol cas, noteu que si les dues parts actuen correctament (i no hi ha problemes de comunicacions) la TTP no ha d'intervenir.

En una solució optimista o amb TTP *off-line*, si les parts actuen correctament i no es produeixen problemes de comunicacions, s'aconsegueix la propietat d'equitat sense que hagi d'intervenir la TTP.

Ara cal resoldre les possibles situacions en què una de les parts intenti fer trampes. Per exemple, cal resoldre la possible situació en la qual A, un cop que disposa de l'acusament de recepció de B, no envia la clau en el tercer pas. Si A actués d'aquesta manera, ella tindria l'acusament de recepció de B i B només disposaria de la prova que A volia enviar un missatge certificat, però no de la clau k, que li permetria llegir el correu. Per tant, la situació no seria equitativa. Per això cal un subprotocol que si es dóna aquesta situació permeti a B restablir l'equitat de l'intercanvi. Es tracta del subprotocol de finalització.

Ara es podrà entendre per què en el primer enviament A va remetre la clau secreta k xifrada amb la clau pública de la TTP PU_T. Vegem el subprotocol de finalització:

$$\text{B} \rightarrow \text{T: } c = E_k(M), K = PU_T(k), Sign_A(c,K), AR_B = Sign_B(c)$$

Amb la informació anterior la TTP pot comprovar que A es va comprometre a enviar un correu certificat determinat, i si la signatura de A és correcta, pot procedir a desxifrar el criptograma K amb la seva clau privada PR_T, amb la qual cosa recuperarà la clau k:

$$\text{T: } PR_T(K) = k$$

Ara pot enviar aquesta clau a B perquè pugui llegir el missatge M:

$$\text{T} \rightarrow \text{B: } k, Sign_T(k)$$

La clau k va acompanyada d'una signatura de la TTP sobre aquesta, perquè B pugui verificar (i demostrar, si escau) que aquesta va ser la clau que li va transmetre la TTP.

En resum, si la TTP no disposa de més informació (A no hi havia contactat abans), la TTP envia a B la clau k que hauria d'haver enviat A (però ara signada per la TTP). D'aquesta manera hem restablert l'equitat per a B.

Però a continuació podem observar que es pot donar una situació no desitjable per a A. Amb el subprotocol anterior hem aconseguit que B, una vegada ha rebut el primer pas de A, pugui finalitzar l'execució del protocol de correu electrònic certificat en qualsevol moment, fins i tot sense enviar (ni intentar-ho) la informació del segon pas a A.

A priori això no representa un problema greu d'equitat per a A, perquè si B no contacta amb la TTP, cap dels dos no té res que comprometi l'altra part, i si B contacta amb la TTP, l'únic que cal fer és permetre que A també pugui contactar amb la TTP, la qual li hauria de proporcionar l'acusament de recepció de B (que aquest havia remès a la TTP quan hi va contactar):

$\text{A} \rightarrow \text{T: } c = E_k(M), K = PU_T(k), Sign_A(c, K)$
$\text{T} \rightarrow \text{A: } AR_B = Sign_B(c)$

Però en el cas que B no hagi contactat amb la TTP en el moment que ho faci A, què ha de fer la TTP? Una primera opció seria que no fes res, però d'aquesta manera A quedaria en una situació no desitjable: A sap que B pot contactar amb la TTP en qualsevol moment i obtenir la clau k, que li permetrà llegir el correu certificat. Per a solucionar aquesta situació conflictiva, hi ha dues solucions.

En primer lloc, podem establir una data d'expiració després de la qual la TTP no pot resoldre noves peticions, o bé es pot afegir una resposta nova de la TTP per a cancel·lar l'intercanvi:

$\text{A} \rightarrow \text{T: } c = E_k(M), K = PU_T(k), Sign_A(c, K)$
$\text{T} \rightarrow \text{A: } Sign_T(cancel - correu - M)$

És a dir, que si la TTP no ha rebut cap petició de B (per tant, la TTP pensa que de moment per a B tot és correcte), el que ha de fer és enviar un missatge de cancel·lació vinculat al missatge *M* a A. Ara hauríem de combinar els dos casos anteriors en un únic subprotocol per a A:

A → T: $c = E_k(M), K = PU_T(k), Sign_A(c,K)$
Si B_ha_contactat_amb_T then T → A: $AR_B = Sign_B(c)$
Else T → A: $Sign_T(cancel - correu - M)$

D'aquesta manera tenim en compte les dues situacions possibles que es poden donar quan A contacta amb la TTP. Quedaria ara per completar el subprotocol de finalització que havíem explicat per a B. Ara cal tractar el cas que A hagi contactat amb la TTP abans que B:

B → T: $c = E_k(M), K = PU_T(k), Sign_A(c,K), AR_B = Sign_B(c)$
Si A_ha_contactat_amb_T then T → B: $Sign_T(cancel - correu - M)$
Else T → B: $k, Sign_T(k)$

Ara el protocol de manera global compleix la propietat fonamental d'equitat. Per comprovar-ho, analitzem les situacions possibles que es poden donar:

- A i B finalitzen l'execució del subprotocol d'intercanvi. En aquest cas queda clar que després d'executar els tres passos totes dues parts acaben obtenint el que esperaven: B el correu *M* i A l'acusament de recepció de B AR_B.

- A envia el primer missatge i no rep res de B (perquè B no ha enviat la resposta, o perquè s'ha perdut mentre estava en trànsit). A ha de contactar amb la TTP i si B no havia contactat amb T (això significa que B no pot tenir el missatge *M*) rebrà un missatge de cancel·lació; per tant, cap de les dues parts no tindrà l'element de l'altra part (perquè de fet no es considerarà enviat el correu electrònic certificat). En el cas que B ja hagués contactat amb la TTP, aquesta havia proporcionat la clau *k* a B (i per tant, B pot llegir el missatge *M*), i ara ha de proporcionar l'acusament de recepció de B a A: llavors totes dues parts tindran l'element que esperaven de l'altra part.

- B envia el seu acusament de recepció i no rep la clau de desxifratge. B ha de contactar amb la TTP. Si A havia contactat amb la TTP, B rebrà un missatge de cancel·lació, i cap de les dues parts no disposarà dels elements (útils) de l'intercanvi. Si A no havia contactat amb la TTP, aquesta proporcionarà la clau de desxifratge *k* a B.

Ja hem demostrat que el protocol anterior és equitatiu, però ara explicarem una situació aparentment contradictòria que es pot donar.

Suposem que s'executa el protocol d'intercanvi sense cap problema, però a més *a posteriori* A contacta amb la TTP per cancel·lar l'intercanvi. Com que la TTP no disposa de més informació (B no hi ha contactat) ha de proporcio-

nar un missatge de cancel·lació a A. D'aquesta manera A disposa d'una doble prova: la prova que el missatge *M* ha estat rebut (amb l'acusament de recepció aportat per B) i que l'intercanvi ha estat cancel·lat (amb la prova aportada per T).

Però en el cas que hi hagi litigis entre A i B, per a un àrbitre extern quedarà clar que A és trampós si intenta al·legar que l'intercanvi ha estat cancel·lat. Si A intenta fer prevaler la prova de cancel·lació davant un àrbitre, B aportarà els dos missatges enviats per A (la primera transmissió de A i la clau *k* rebuda de A). En concret, la clau *k* rebuda per A demostra que aquesta és tramposa, ja que en cap cas A no hauria enviat aquesta clau sense haver disposat abans de l'acusament de recepció de B. En conclusió, A va contactar amb la TTP després d'haver rebut l'acusament de recepció de B, i va intentar fer trampes.

Un dels problemes que plantejaven les solucions presentades amb TTP *in-line* i amb TTP *on-line* era que calia dipositar molta confiança en la TTP. Ens hauríem de preguntar ara com és el nou protocol des del punt de vista de possibles aliances amb les diferents parts. Tècnicament denominem *verificabilitat de la TTP* aquesta propietat.

> Direm que un protocol de correu electrònic certificat amb TTP compleix la propietat que la TTP és verificable si les parts intervinents poden demostrar un mal comportament de la TTP si aquesta no segueix els passos previstos en el protocol.

Per fer l'anàlisi del protocol proposat anteriorment, observarem els dos possibles atacs que pot portar a terme la TTP. Una assumpció que farem és que la TTP sempre respon les peticions de les parts (en cas contrari seria possible demostrar aquest mal comportament de la TTP amb un àrbitre extern).

El primer atac que es podria fer és una aliança de la TTP amb A. Així, l'objectiu seria proporcionar l'acusament de recepció de B a A, i deixar B sense el missatge *M*. Però aquesta situació no és possible perquè si B contacta amb la TTP, aquesta o bé li ha de proporcionar la clau *k* que va generar A o el missatge de cancel·lació. Si es dóna la primera situació, l'atac ha fracassat. I si es dóna la segona situació, B disposarà d'una prova que li permetrà demostrar *a posteriori* (si A intenta fer valer l'acusament de recepció de B) que o A o T van fer trampes.

El segon atac que es podria produir és l'aliança de T amb B. En aquest cas l'objectiu és proporcionar el missatge *M* a B, i intentar deixar A sense l'acusament de recepció. Per a això la TTP proporciona la clau *k* que va generar A i el missatge de cancel·lació que genera la TTP a B, i un missatge de cancel·lació a A. Aquesta situació no pot ser detectada *a priori* per A. En aquest moment B es troba en una situació de privilegi perquè si *a posteriori* li interessa afirmar

que va rebre el missatge, aportarà la informació de A, i en cas contrari només aportarà la cancel·lació de T. Al contrari, des del punt de vista de A l'intercanvi està cancel·lat. Com es pot donar aquesta situació? Recordem que hi havia la possibilitat que després de finalitzar l'intercanvi A contactés amb la TTP per obtenir un missatge de cancel·lació i intentar fer trampes. Aquesta possible situació ara s'ha tornat en contra seva.

Podria semblar que la situació anterior invalida el protocol presentat, i no necessàriament ha de ser així. Situacions similars es poden donar en el món en paper. Imaginem el cas de l'agent de correus que proporciona el missatge al destinatari sense reclamar l'acusament de recepció corresponent. En aquest cas, el destinatari disposa del missatge i el remitent s'haurà quedat sense l'acusament de recepció. Evidentment, davant la falta de l'acusament de recepció, el remitent podrà reclamar el missatge original, i davant d'això l'agent o l'empresa de correus en podran al·legar la pèrdua. Per tant, el que indiquem és que la TTP ha de ser de confiança elevada per a A (que és qui tria aquesta entitat).

En els protocols amb TTP *in-line* i *on-line* hem dit que les parts havien de dipositar molta confiança en la TTP perquè tenia accés al contingut del missatge. En la nova proposta hem millorat el problema una mica, però no totalment. Si la TTP no ha d'intervenir, no tindria accés al missatge, però si la TTP ha d'intervenir observem que les parts envien el text del missatge, M, a la TTP. Encara que estigui xifrat amb una clau k, la TTP pot recuperar aquesta clau k desxifrant el criptograma K amb la clau privada PR_T. Per tant, podrà desxifrar el criptograma c i llegir el missatge M.

$$\text{T: } PR_T(K) = k$$
$$\text{T: } D_k(c) = M$$

Un protocol de correu electrònic certificat compleix la propietat de confidencialitat si només remitent i destinatari tenen accés al contingut, i ni tan sols la TTP té accés a aquest contingut.

Per tant, el protocol plantejat és millorable des del punt de vista de la confidencialitat de la informació intercanviada. En aquest cas, a diferència del protocol equivalent de signatura electrònica de contractes, un espia que tingui accés al canal de comunicacions no podria accedir al contingut del missatge M (aquest s'envia xifrat en la transmissió entre A a B).

Ara introduirem unes petites millores per aconseguir la propietat de confidencialitat. Per a això farem un xifratge addicional sobre el missatge, de manera que solament el destinatari pugui tenir accés a la informació:

A → B: $c = E_l(E_k(M)), PU_B(l), K = PU_T(k), Sign_A(c,K)$
B → A: $AR_B = Sign_B(c)$
A → B: $k, Sign_A(k)$

El mecanisme utilitzat és senzill i consisteix a xifrar el criptograma resultant de xifrar M amb la clau k, un altre cop amb un criptosistema simètric (per exemple, AES) amb una altra clau secreta generada per A que "compartirà" amb B. Però B necessitarà conèixer aquesta clau secreta, i per això xifrem la clau secreta, l, amb la clau pública de B d'un criptosistema de clau pública (per exemple, RSA). Quan B rep la informació del primer pas, la primera operació que ha de fer és un desxifratge amb la seva clau privada per recuperar la clau l.

$$B: PR_B(PU_B(l)) = l$$

Amb aquesta clau l pot fer el desxifratge del criptograma que conté el missatge xifrat amb la clau k:

$$B: D_l(c) = E_k(M)$$

D'aquesta manera aconseguirem que la TTP no tingui accés al contingut del missatge. La informació que B ha d'enviar a la TTP, en cas que calgui, és la següent:

$$B \rightarrow T: c = E_l(E_k(M)), K = PU_T(k), Sign_A(c,K), AR_B = Sign_B(c)$$

La TTP podrà recuperar la clau k, però com que desconeix la clau l no tindrà accés al contingut del missatge. Ara sí que podem afirmar que el protocol compleix la propietat de confidencialitat.

Una propietat interessant del protocol que acabem de presentar és que no s'han introduït restriccions temporals. Les parts poden contactar amb la TTP quan vulguin per finalitzar l'execució del protocol. Per això diem que el protocol és asíncron (no requereix la sincronització dels rellotges de cap de les parts que hi intervenen).

Un protocol de correu electrònic certificat compleix la propietat de temporalitat (*timeliness* en anglès) si les parts poden tenir la garantia que l'execució del protocol es pot finalitzar quan elles vulguin, sense assumir el risc de perdre l'equitat de l'intercanvi.

Solució amb TTP *off-line* síncrona

Hem vist que el fet que el protocol fos asíncron (les parts podien contactar amb la TTP en qualsevol moment) obligava a introduir un subprotocol de

cancel·lació per a A. Ara veurem com podríem modificar la proposta si establim un temps límit, és a dir, que un cop transcorregut un certs temps ja només es puguin fer consultes a la TTP de quin és l'estat de la transacció, però no demanar-li que faci cap acció de modificar l'estat de l'intercanvi. Suposem que el subprotocol d'intercanvi coincideix amb l'anterior:

A → B: $c = E_k(M), K = PU_T(k), Sign_A(c,K)$
B → A: $AR_B = Sign_B(c)$
A → B: $k, Sign_A(k)$

Tal com passava abans, es pot donar la situació que B enviï l'acusament de recepció, però no rebi la clau de A. Per això hem d'establir un subprotocol perquè B pugui restablir l'equitat de l'intercanvi. Però ara imposem una condició addicional a B, i és que ha de contactar amb la TTP abans d'un determinat valor temporal t. Si es troba en una situació no equitativa i no contacta amb la TTP abans de t, el problema ja no tindrà solució: quedarà en desavantatge davant A (però a causa de la seva inacció). Per tant, el subprotocol queda com segueix:

B → T: $c = E_k(M), PU_T(k), Sign_A(c,K), AR_B = Sign_B(c)$
Si t-actual<t then T → B: $k, Sign_T(k)$
Else T → B: $Sign_T[fora-de-termini]$

En aquest cas no té sentit que A contacti amb la TTP per cancel·lar l'intercanvi, ja que A sap que si no rep l'acusament de recepció de B després de transcórrer el temps t (que ella ha triat), podrà consultar la TTP per saber l'estat de l'intercanvi. El subprotocol per a A seria:

A → T: $c = E_k(M), K = PU_T(k), Sign_A(c,K)$
Si B_ha_contactat_amb_T then T → A: $AR_B = Sign_B(c)$
Else T → A: $Sign_T(cancel-correu-M)$

De fet, en el cas que B no hagi contactat amb la TTP, no caldria que T enviés un missatge de cancel·lació a A, perquè després del temps t, B ja no podrà aconseguir la clau de A ni de T, i per tant, cap de les parts no tindrà res que comprometi l'altra.

La introducció d'una restricció temporal simplifica el protocol plantejat (i les accions que ha de fer la TTP), però pot representar un inconvenient per als participants en el protocol de correu certificat (en aquest cas per a B). D'una banda, B ha de tenir el rellotge sincronitzat amb la TTP, ja que en cas contrari, que la petició sigui rebutjada per haver arribat fora de termini.

D'altra banda, encara que els rellotges estiguin sincronitzats, en cas que hi hagi problemes amb el canal de comunicacions, l'equitat de l'intercanvi es pot veure compromesa per a B, per la impossibilitat de contactar amb la TTP dins del termini establert.

Una altra solució amb TTP *off-line*

Arribats a aquest punt, en el qual ja s'han presentat dues solucions optimistes (síncrona i asíncrona) per al correu electrònic certificat, es podria plantejar la qüestió del perquè d'un protocol de tres passos: seria possible un protocol de dos passos? La resposta és que no, perquè la TTP no tindria manera de prendre una decisió que garantís l'equitat al remitent del missatge.

D'altra banda, es podria pensar en una solució de quatre passos. Òbviament, l'eficiència disminuiria, però potser s'aconseguiria alguna millora respecte al protocol de tres passos. Un protocol de quatre passos seria de la manera següent:

A → B: $c = E_k(M), K = PU_T(k), Sign_A(c,K)$
B → A: $AR_B = Sign_B(c)$
A → B: $k, Sign_A(k)$
B → A: $AR-2_B = Sign_B(k)$

Es pot observar que s'ha aconseguit una certa simetria entre les dues parts que participen en l'intercanvi d'un correu electrònic certificat. Ara la prova per a A són els dos acusaments de recepció que genera i envia B, ja que B necessita dos passos per a poder accedir al contingut del missatge certificat. El primer acusament de recepció de B permet verificar que ha rebut el criptograma del primer pas, i el segon acusament de recepció permet verificar que ha rebut la clau de desxifratge.

Per no complicar l'explicació, hem suprimit la millora de proporcionar el servei de confidencialitat respecte de la TTP, és a dir, amb l'esquema proposat, la TTP tindria accés al contingut del missatge. Ja hem vist que resoldre aquest problema és relativament senzill.

Quedaria ara per veure com queden alterats els subprotocols per als casos de conflicte. Per a això suposarem el cas en què vulguem un protocol asíncron (queda com a exercici el cas síncron).

Noteu que ara el que ràpidament pot quedar en desavantatge és A (a diferència d'abans), perquè una vegada que A ha enviat la clau de desxifratge k, queda en mans de B, que pot enviar o no el segon acusament de recepció (necessari per a A). Per això hem d'establir un protocol de finalització per a A amb la TTP:

A → T: $c = E_k(M), K = PU_T(k), Sign_A(c,K), AR_B, k, Sign_A(k)$
T → A: $Sign_T(k)$

De manera anàloga al que hem explicat en el primer protocol optimista, ara seria B qui podria quedar en una situació no equitativa, si no dissenyem un subprotocol de finalització per a ell. Es podria donar el cas que A fes trampes, i sense haver enviat el tercer missatge contactés amb la TTP. D'aquesta ma-

nera, A aconsegueix les proves que necessita (l'acusament de recepció de B i l'acusament de recepció de T) i B només té el primer missatge de A, que no és suficient. Per això necessitem el subprotocol següent:

B → T: $c = E_k(M), PU_T(k), Sign_A(c,K), AR_B = Sign_B(c)$
T → B: $k, Sign_T(k)$

Amb aquest subprotocol hem restablert la possible inequitat de l'intercanvi. Si A pot tenir accés als dos acusaments de recepció, B té accés a la clau de desxifratge *k*.

Ara podríem decidir si volem que la solució sigui síncrona (establint un termini per a poder contactar amb la TTP), o si volem una solució asíncrona (i llavors hauríem de dissenyar un subprotocol de cancel·lació per a B, amb l'objectiu que no hagi d'esperar indefinidament a l'espera de veure què fa A). Inicialment, hem indicat que volíem una solució asíncrona, i per tant, necessitem un subprotocol de cancel·lació:

B → T: $c = E_k(M), PU_T(k), Sign_A(c,K), AR_B = Sign_B(c)$
Si A ha contactat amb la TTP then T → B: $k, Sign_T(k)$
else T → B: $Sign_T(cancel - correu - M)$

I el subprotocol per a A quedarà de la manera següent:

A → T: $c = E_k(M), K = PU_T(k), Sign_A(c,K), AR_B, k, Sign_A(k)$
Si B ha contactat amb la TTP then T → A: $Sign_T(cancel - correu - M)$
else T → A: $Sign_T(k)$

Aquest protocol en quatre passos (tant la versió síncrona com l'asíncrona) introdueix una millora respecte de les versions en tres passos, i és que el comportament de la TTP és verificable, és a dir, que si la TTP intenta fer trampes aquesta situació podrà ser detectada i demostrada per remitent i destinatari.

2. Solucions per al correu electrònic certificat sense TTP

Si hem dit que les solucions amb TTP *on-line* o *in-line* no són convenients perquè la TTP es pot convertir en un coll d'ampolla pel que fa a les comunicacions, o no volem assumir el cost que puguin comportar, la mateixa crítica, encara que en menys grau, es pot dirigir a les solucions amb TTP *off-line*.

Així, ens hem de preguntar si hi ha propostes de solucions sense TTP per al correu electrònic certificat. La resposta és que sí, i que un dels tipus de solucions sense TTP es basa en el que es coneix com l'intercanvi gradual de secrets. De manera senzilla podem dir que la idea consisteix a intercanviar el missatge i l'acusament de recepció a trossos (a continuació veurem que això és una simplificació una mica burda).

Per a explicar un exemple concret de protocol basat en l'intercanvi gradual de secrets necessitem el mateix protocol de transferència transcordada que hem apuntat en el cas de la signatura electrònica de contractes.

Recordem que per a entendre el concepte necessari hem explicat un protocol per al joc de "cara o creu", del qual ens interessava que una de les parts A proporciona a l'altra un de dos valors possibles (cara o creu) amb la mateixa probabilitat, i sense que A sàpiga quin dels dos li ha proporcionat. Aquesta característica es denomina *transferència inconscient*. Per explicar un protocol de correu electrònic certificat sense TTP suposarem que disposem d'un protocol similar, que etiquetarem com:

$$\mathrm{A} \rightarrow \mathrm{B}\text{: } trans - transc(x,y)$$

que significa que A transmet a B un de dos possibles valors (x o y), de manera equiprobable i sense que A sàpiga quin dels dos ha transferit.

Protocol de correu electrònic certificat sense TTP

Expliquem aquí un protocol de correu electrònic certificat sense TTP, és a dir, en l'execució d'aquest protocol només intervenen remitent i destinatari del missatge.

El protocol l'inicia A generant de manera aleatòria $N + 1$ claus de criptografia simètrica (per exemple, d'AES o DES), des de a_0 fins a a_N, i calcula N claus addicionals a partir de les anteriors de la manera següent:

$$a_{N+i} = a_0 XOR a_i \text{ (per a } i = 1 \text{ fins a } N)$$

D'aquesta manera, A ha generat N parells de claus que estan relacionades per a_0:

$$(a_1,a_{N+1}),(a_2,a_{N+2}),\ldots,(a_N,a_{2N})$$

A continuació A ha de xifrar un text arbitrari S amb les $2N$ claus que ha generat anteriorment i el missatge que vol enviar certificat M amb la clau a_0, i envia el criptograma associat a M i els $2N$ criptogrames associats a S a B:

$$\text{A} \rightarrow \text{B: } C = E_{a_0}(M), C_i = E_{a_i}(S) \text{ (per a } i = 1 \text{ fins a } 2N)$$

Si B pot obtenir una qualsevol de les parelles de claus, podrà recuperar el missatge que vol remetre certificat A. Per les propietats de l'operació XOR tenim que es compleix la igualtat següent:

$$a_i XOR a_{N+i} = a_0$$

Amb la clau a_0 podrà fer el desxifratge del criptograma C, i per tant, podrà llegir el missatge M.

En aquest moment B procediria de manera anàloga als passos que havíem explicat en el protocol de signatura electrònica de contractes. En primer lloc, generaria $2N$ claus de criptografia simètrica i les agruparia en parelles:

$$\text{B: } (b_1,b_{N+1}),(b_2,b_{N+2}),\ldots,(b_N,b_{2N})$$

A continuació també xifra el text arbitrari S amb les $2N$ claus que ha generat anteriorment, i envia els $2N$ criptogrames a A:

$$\text{B} \rightarrow \text{A: } D_i = E_{b_i}(S) \text{ (per a } i = 1 \text{ fins a } 2N)$$

B acorda amb A que reconeixerà que ha rebut el missatge M si A pot obtenir una o més de les parelles de claus que ha generat (i que en aquest moment només coneix B). És a dir, el fet de disposar d'una parella de claus es converteix en l'acusament de recepció que vincula B amb la recepció del missatge M. L'extrem anterior queda fora de l'explicació detallada del protocol, però apuntem que representaria enviar un missatge signat, indicant aquest acord.

En el pas següent és quan necessitem el protocol de transferència inconscient. A i B l'utilitzaran per a transmetre una de les dues claus de cada un dels N parells de claus que han generat, respectivament. Comencem per A:

$$\text{A} \rightarrow \text{B: } trans-transc(a_i,a_{i+N}) \text{ (per a totes les parelles de claus)}$$

En finalitzar aquest pas, A haurà transferit a B una de les dues claus de cada parell, amb dues característiques molt importants per a la seguretat del protocol: A no sap quina de les dues claus de la parella ha proporcionat a B, i el fet que hagi proporcionat una o l'altra (de cada parell) és equiprobable.

B ha de fer el mateix pas amb els seus parells de claus:

$$B \rightarrow A: trans - transc(b_i, b_{i+N}) \text{ (per a totes les parelles de claus)}$$

En aquest punt de l'execució del protocol, A i B disposen de la meitat dels secrets de l'altra part. Això no representa un compromís per a cap dels dos, ja que B necessita un parell de claus per a recuperar el missatge M, i A necessita un parell de claus, ja que segons el compromís establert, això representa l'acusament de recepció (per tant, en aquest moment no disposen de prou informació).

A continuació A i B intercanvien bit per bit totes les claus que van generar en la primera fase del protocol. Aquest intercanvi l'han de fer de manera intercalada, perquè en tot moment tots dos disposin aproximadament de la mateixa informació de l'altra part. Òbviament, la part que inicií l'intercanvi estarà en desavantatge, però si l'intercanvi és bit per bit aquest desavantatge serà molt petit. Vegem com quedaria el protocol:

FOR i = 1 TO L DO (en què L és la longitud de cada clau)
A → B: el bit i de totes les claus a_i (menys a_0)
B → A: el bit i de totes les claus b_i

Si cap de les dues parts no atura l'execució d'aquest pas, al final A i B disposaran dels N parells de claus de l'altra part. Totes dues parts poden verificar que els parells són correctes fent el desxifratge dels criptogrames que han intercanviat a l'inici de l'execució del protocol.

B només necessitava un parell de claus per a recuperar el missatge que A li ha remès. Amb un parell de claus podia recuperar a_0, i amb aquesta clau pot desxifrar C i llegir el missatge M. A necessitava un parell de claus per a disposar de l'acusament de recepció de B.

Analitzem ara què passa si una de les dues parts intenta fer trampes. El primer intent de fer un frau es podria produir en el moment de transferir una de les dues claus amb la transferència inconscient, és a dir, intentar enviar una clau que no ha estat utilitzada per a xifrar el text arbitrari S. D'aquesta manera la part fraudulenta el que intenta és obtenir un parell de claus de l'altra part, i deixar-la sense la possibilitat d'obtenir els seus parells de claus. La transferència inconscient no permet aquest atac, ja que és clar que l'atacant no pot canviar les dues claus. Una de les dues és transferida en el pas de transferència inconscient, i per tant, si les dues claus són "falses" l'altre extrem ho detectarà ràpidament, ja que aquesta clau no es correspondrà amb cap dels criptogrames rebuts en el primer pas del protocol.

Per tant, l'atacant només pot canviar un dels dos components de cada parell. Però tampoc no podrà fer aquest atac, ja que recordeu que es transfereix una clau de cada parell de manera inconscient, és a dir, l'emissor no sap quin dels

dos components ha rebut l'altre extrem. Si l'emissor canvia un dels dos components aleatòriament en un parell té el 50% de probabilitats de ser detectat per l'altra part (que s'hagi transferit la clau canviada). Ara s'observa la importància que siguin N parells de claus, ja que hem vist que la probabilitat de no ser detectat en una transferència és del 50% (que tingui la sort que l'altre extrem rebi la clau correcta, la no canviada). En un segon parell de claus la probabilitat de no ser detectat també serà del 50%, però la probabilitat acumulada de no ser detectat és del $0,5 \cdot 0,5 = 0,25$, és a dir, el 25%, i així successivament, i s'arriba a una probabilitat per a N parells de:

$$\text{Prob\_no\_detecció} = 2^{-N}$$

Per a un valor relativament petit de N, la probabilitat de no ser detectat es pot fer menyspreable. Com a conclusió, no és possible aquesta via d'atac.

Una segona possibilitat de fer trampes que tenen A i B és intentar enviar bits incorrectes durant la fase d'intercanvi de les claus bit per bit. Vegem que tampoc no és possible aquest atac. En cada pas de l'intercanvi bit per bit de les claus, A i B proporcionen un bit de cada clau de les $2N$ claus que han generat en el primer pas del protocol. Però en aquest punt l'altre extrem disposa d'una de les dues claus de cada parell de manera segura (com acabem de veure). Si A o B intenten enviar bits incorrectes de les dues claus de cada parell, seran immediatament detectats, ja que l'altra part disposa d'una de les dues claus.

Si intenten enviar bits incorrectes d'una de les dues claus de cada parell també seran detectats, ja que no saben de quina de les dues claus disposa l'altra part. Si una part detecta que rep bits incorrectes, aturarà immediatament l'execució del protocol per no quedar en situació de desavantatge (proporcionar un parell a l'altra part i quedar-se sense la possibilitat de disposar d'un parell de l'altra part). Per tant, tampoc no és possible aquest atac.

Com a conclusió podem afirmar que A i B no poden fer cap dels dos atacs plantejats sense assumir un risc molt elevat que l'intent de fer trampes sigui detectat.

Es podria concloure que el protocol presentat és prou segur, i sense necessitat de TTP, però per a això cal assumir que totes dues parts disposen de la mateixa potència de càlcul. Per observar la necessitat d'aquesta assumpció ens hem de plantejar què passa si una de les dues parts atura l'execució del protocol en la fase d'intercanvi de bits quan ja s'han intercanviat X bits de cada clau. És cert que cada part disposa aproximadament de la mateixa informació que l'altra (com a molt, hi ha la diferència d'un bit més per a B, si A és el primer que transmet els seus bits).

Un cop aturada l'execució del protocol, l'única possibilitat que queda a totes dues parts és el que es coneix com a *atac per força bruta*, és a dir, provar les

combinacions de bits possibles dels que no han estat proporcionats per l'altra part. Si han aturat l'execució quan només faltava un bit, totes dues parts podran deduir el bit que falta sense cap problema, ja que només han de fer dues proves possibles (0 o 1). Però si resten t bits hauran de fer 2^t proves, i en funció de t això pot requerir una elevada potència de càlcul perquè l'atac pugui fructificar. Aquí és on hi ha el problema del protocol: el que per a una part pot ser un problema trivial (disposa de la potència de càlcul necessària per a fer les 2^t proves en un temps raonable) per a l'altra part pot ser un problema irresoluble (pot necessitar un temps i recursos de què no disposa). Suposar que les parts que intervenen en el protocol de correu electrònic certificat disposen de la mateixa potència de càlcul és poc realista i perillós des del punt de vista de la seguretat (compareu la potència de càlcul d'un particular enfront de la potència de càlcul de Google). Per aquest motiu, no se solen recomanar les solucions sense TTP, malgrat l'avantatge aparent de no necessitar la intervenció d'actors diferents del remitent i el destinatari.

Les solucions per al correu electrònic certificat sense TTP basades en l'intercanvi gradual de secrets se solen descartar perquè per garantir-ne la seguretat assumeixen que les parts disposen de la mateixa potència de càlcul, assumpció que és poc realista en la pràctica.

3. Solucions per al correu electrònic certificat multipart

Fins ara hem presentat solucions per al cas que siguin dues les parts involucrades en el correu electrònic certificat. Però també es pot donar el cas que un usuari vulgui remetre el mateix correu electrònic certificat a múltiples destinataris (per exemple, la convocatòria d'una junta d'accionistes). Llavors parlem de protocols multipart per al correu electrònic certificat.

Solució per al correu electrònic certificat multipart amb TTP *in-line*

Com en el cas del correu certificat entre dues parts, començarem amb la solució més senzilla possible. Es tracta d'una solució amb TTP *in-line*, en la qual totes les parts intervinents (R, el remitent, i C_1 a C_N, els destinataris) envien la informació a la TTP. En primer lloc, R envia el missatge a la TTP:

$$\mathrm{R} \rightarrow \mathrm{T}: M, Sign_R(M)$$

Ara la TTP ha d'enviar un "avís" als destinataris que disposen d'un correu certificat pendent de ser "recollit":

$$\mathrm{T} \rightarrow C_i: c = E_k(M), Sign_T(c)$$

Els destinataris que vulguin rebre el correu certificat han d'enviar l'acusament de recepció a la TTP:

$$C_i \rightarrow \mathrm{T}: AR_i = Sign_i(c)$$

Una vegada que la TTP disposa de la informació de totes les parts, en verifica la correcció i en cas que siguin correctes ha de retransmetre els acusaments de recepció a R i el missatge als destinataris:

$\mathrm{T} \rightarrow C_i$: $k, Sign_t(k)$
$\mathrm{T} \rightarrow \mathrm{R}$: AR_i (per a $i = 1$ fins a N)

Amb aquesta senzilla solució aconseguim la propietat més important del correu electrònic certificat: l'equitat. Però aquesta solució comparteix els mateixos defectes que l'equivalent per a dues parts, especialment el possible cost d'una TTP que ha d'intervenir en totes les execucions del protocol, i amb un cost computacional considerable.

Solució per al correu electrònic certificat multipart amb TTP *off-line* síncrona

Continuem considerant que les solucions optimistes són preferibles, ja que reduir la intervenció de la TTP ha de significar reduir el risc que es converteixi en un coll d'ampolla, o com a mínim, reduir els costos associats. Per això a continuació exposem una solució optimista síncrona, cosa que significa que s'estableix un termini, una data límit per a portar a terme l'intercanvi de missatge per l'acusament de recepció. De fet, veurem que la data límit, més que amb el correu certificat directament, té a veure amb la intervenció de la TTP.

Ja hem vist que un protocol optimista ha de tenir un subprotocol en el qual només intervinguin remitent i destinataris (subprotocol d'intercanvi) i un subprotocol (o més d'un) en el qual ha d'intervenir la TTP.

Començarem explicant el subprotocol d'intercanvi:

$\mathrm{R} \rightarrow C_i$: $c = E_k(M), K = PU_T(k), Sign_A(c,K)$
$C_i \rightarrow \mathrm{R}$: $AR_i = Sign_i(c)$
$\mathrm{R} \rightarrow C_i$: $k, Sign_R(k)$

En un primer pas el remitent envia el missatge xifrat amb la clau k a tots els destinataris. A continuació, cada destinatari ha d'enviar un acusament de recepció al remitent per confirmar que ha rebut el missatge xifrat. Finalment, el remitent envia la clau k que permet desxifrar el missatge M.

Com en el cas del correu certificat entre dues parts, ara cal proporcionar un subprotocol per al cas que alguna de les parts no compleixi el que està previst en el subprotocol d'intercanvi. Establim que les parts tenen un temps t per a contactar amb la TTP, temps després del qual la TTP no pot acceptar peticions de resolució amb relació a aquest correu, i l'únic que pot fer és notificar la resolució a la qual va arribar abans d'aquest període, si escau.

Si un destinatari ha enviat l'acusament de recepció i no rep la clau de desxifratge, ha d'enviar a la TTP les proves de l'intercanvi:

$$C_i \rightarrow \mathrm{T}: c = E_k(M), K = PU_T(k), Sign_A(c,K), AR_i = Sign_i(c)$$

Les proves aportades per C_i demostren que el remitent havia iniciat el procés d'enviar un correu certificat. Essent així, la TTP ha de proporcionar la clau k que permeti fer el desxifratge del missatge a C_i:

$$\mathrm{T} \rightarrow C_i: k, Sign_T(k)$$

En aquest cas el protocol no és atòmic, en el sentit que no totes les parts han de finalitzar necessàriament l'intercanvi.

És senzill veure que el protocol proposat compleix la propietat d'equitat.

Solució per al correu electrònic certificat multipart amb TTP *off-line* asíncrona

De la mateixa manera que hem presentat una solució asíncrona per al cas d'un remitent i un destinatari, també hi ha propostes de solució asíncrones per al cas que siguin múltiples els destinataris del mateix correu electrònic certificat.

El protocol consta de tres subprotocols, com el cas de dues parts: un subprotocol d'intercanvi, un de cancel·lació i un de finalització. Començarem descrivint el subprotocol d'intercanvi:

$R \rightarrow C_i$: $c = E_k(M), K = PU_T(k), Sign_R(c,K)$
$C_i \rightarrow R$: $AR_i = Sign_i(c)$
$R \rightarrow C_i$: $k, Sign_R(k)$

Si cap de les parts no atura l'execució del subprotocol d'intercanvi, i si no es presenten problemes de comunicacions, cada part disposarà dels elements esperats, i sense necessitat que intervingui la TTP. El remitent disposarà dels acusaments de recepció i els destinataris del missatge.

Però, com en casos anteriors, ara ens hem de plantejar què passa si sorgeixen problemes de comunicacions, o alguna de les parts intenta fer trampes. Òbviament, els actors honestos han de contactar amb la TTP per recuperar l'equitat de l'intercanvi. Però hem d'establir les regles que ha de seguir la TTP per garantir l'equitat de totes les parts honestes.

Veurem que en el cas del correu electrònic certificat, com que es tracta d'intercanvis entre el remitent i cada un dels destinataris, les regles de la TTP s'assemblen molt al cas del protocol entre dues parts.

Si un dels destinataris no rep la clau de desxifratge k després d'haver remès l'acusament de recepció, ha de sol·licitar la intervenció de la TTP:

$$C_i \rightarrow T: c = E_k(M), K = PU_T(k), Sign_R(c,K), AR_i = Sign_i(c)$$

La TTP verificarà si el remitent hi havia contactat prèviament en relació amb aquest correu i destinatari. Si no s'havia produït aquest contacte, la TTP ha de registrar que aquest destinatari hi ha contactat, i n'ha d'emmagatzemar l'acusament de recepció per si posteriorment el remitent hi contacta. D'altra banda, ha d'enviar a aquest destinatari la clau de desxifratge k:

$$T \rightarrow C_i: k, Sign_T(k)$$

Si és el remitent qui contacta amb la TTP, i indica que un subconjunt de remitents no han enviat l'acusament de recepció esperat, la TTP ha de verificar si algun d'ells hi havia contactat prèviament. Ara la TTP ha d'actuar, per a cada destinatari del subconjunt demandat pel remitent, de dues maneres possibles. Per a aquells destinataris que hi havien contactat, i als quals havia proporci-

onat la clau *k*, ha d'enviar l'acusament de recepció que havia emmagatzemat llavors:

$$T \rightarrow R: AR_i = Sign_i(c), AR_j = Sign_j(c), \ldots$$

En la transmissió anterior haurien d'aparèixer tants acusaments de recepció com destinataris han finalitzat l'intercanvi amb la TTP prèviament.

Per als destinataris que no hagin contactat amb la TTP, aquesta ha d'enviar un missatge de cancel·lació a R:

$$T \rightarrow R: Sign_T(cancel - missatge - M - relacio - destinataris)$$

Aquest missatge ha de contenir la identitat de tots els destinataris per als quals es considera cancel·lat l'intercanvi. La TTP ha de conservar aquesta informació per a resoldre les possibles peticions dels destinataris. Ara podem completar el subprotocol de finalització:

$C_i \rightarrow T: c = E_k(M), K = PU_T(k), Sign_A(c,K), AR_i = Sign_i(c)$
If cancel·lat per a C_i then $T \rightarrow C_i: Sign_T(cancel - missatge - M)$
Else $T \rightarrow C_i: k, Sign_T(k)$

Amb els subprotocols de cancel·lació i de finalització podem afirmar que el protocol presentat garanteix l'equitat per a les parts honestes, i és del tipus optimista i asíncron.

4. Les notificacions electròniques

El correu electrònic certificat pot ser útil en qualsevol entorn en el qual un usuari (un particular, una empresa, etc.) vol tenir constància que un determinat document ha arribat al destinatari, amb el requisit afegit que el remitent vol alguna prova que no permeti negar la recepció d'aquest document al destinatari. Però no hi ha dubte que és en el si de l'Administració pública on ràpidament es detecta la necessitat d'un servei com el que s'ha plantejat en aquest mòdul, especialment per al que se solen denominar notificacions electròniques.

Així, tenim que la Llei 11/2007, de 22 de juny, d'accés dels ciutadans als serveis públics, i el Reial decret 1671/2009, de 6 de novembre, pel qual es desplega parcialment la Llei 11/2007, regulen explícitament les notificacions electròniques. Analitzarem a continuació, succintament, alguns aspectes tècnics de la legislació esmentada.

En primer lloc, cal indicar que la legislació, de manera general, no obliga el ciutadà a utilitzar els mitjans electrònics per a rebre notificacions electròniques, sinó que en principi queda a elecció seva. Però també es preveu que per a determinats processos administratius, i per a determinats col·lectius (persones jurídiques o persones físiques a les quals se suposi la capacitat d'utilitzar mitjans electrònics), es pugui establir l'obligació d'utilitzar les notificacions electròniques. El ciutadà, en els casos en què no estigui obligat a utilitzar notificacions electròniques, pot canviar del sistema electrònic al convencional, i viceversa, en qualsevol moment, sempre amb l'antelació adequada.

Perquè les comunicacions per mitjans electrònics siguin vàlides hi ha d'haver constància de la transmissió i recepció, de les dates, del contingut íntegre de les comunicacions, i cal identificar-ne fidedignament el remitent i el destinatari. És a dir, el legislador està indicant que cal adoptar les mesures de seguretat necessàries per a garantir la integritat, autenticitat, no-repudi i data de les comunicacions electròniques.

Encara que la legislació no parla directament del servei de confidencialitat amb relació a la informació intercanviada per mitjans electrònics, sí que es fa referència a la protecció de dades de caràcter personal. D'aquesta manera, sí que queda recollida l'obligació de dotar-se dels mitjans necessaris per a garantir aquesta protecció, i per tant, quan escaigui, el secret de la informació intercanviada.

El sistema de notificacions electròniques ha de permetre acreditar la data i hora en la qual es produeix la posada a disposició de l'interessat de l'acte objecte

de notificació, i també la d'accés al contingut, moment a partir del qual la notificació es considera practicada a tots els efectes. En els protocols presentats, i amb l'objectiu de no complicar més les explicacions, s'han obviat les referències als aspectes temporals, però en el si de l'Administració són essencials.

La legislació estableix que quan hi hagi constància que s'ha posat a disposició del destinatari la notificació, i transcorrin deu dies naturals sense que s'accedeixi al contingut d'aquesta, s'entén que la notificació ha estat rebutjada. Aquesta previsió és especialment important, ja que és cert que "protegeix" l'Administració dels rebutjos selectius, però deixa en una posició molt feble l'administrat.

El fet que una notificació ha estat posada a disposició del destinatari l'ha d'acreditar el proveïdor del servei de notificacions electròniques, però el destinatari no té la manera de demostrar si efectivament ha pogut accedir o no a la notificació. D'aquesta manera estem convertint el proveïdor en una TTP, però que a més difícilment serà verificable. D'altra banda, aquesta previsió estableix la càrrega a l'administrat de consultar periòdicament la bústia on ha de rebre les notificacions electròniques.

L'obligació anterior, fent una simplificació que caldria matisar, seria equivalent a considerar que una notificació en paper es considera rebutjada quan s'ha dipositat a la bústia convencional i un cop passats deu dies no n'hagi estat recollida.

Exercicis d'autoavaluació

1. Modifiqueu les solucions per al correu electrònic certificat (entre dues parts) amb TTP *in-line* i *on-line*, de manera que la TTP no pugui tenir accés al contingut del missatge.

2. Demostreu que els protocols amb TTP *off-line* que vulguin complir la propietat de temporalitat (*timeliness*) han de tenir un subprotocol de cancel·lació.

3. Dissenyeu un protocol de correu electrònic certificat amb TTP *off-line*, en el qual un remitent vulgui enviar un mateix correu certificat a dos destinataris, però el remitent no vol lliuraments parcials: o l'han de rebre (i per tant, enviar acusament de recepció) tots dos destinataris o no l'ha de rebre cap.