Tiquets electrònics

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

PID_00202397

UOC
Universitat Oberta de Catalunya

Els textos i imatges publicats en aquesta obra estan subjectes –llevat que s'indiqui el contrari– a una llicència de Reconeixement-NoComercial-SenseObraDerivada (BY-NC-ND) v.3.0 Espanya de Creative Commons. Podeu copiar-los, distribuir-los i transmetre'ls públicament sempre que en citeu l'autor i la font (FUOC. Fundació per a la Universitat Oberta de Catalunya), no en feu un ús comercial i no en feu obra derivada. La llicència completa es pot consultar a http://creativecommons.org/licenses/by-nc-nd/3.0/es/ legalcode.ca.

Índex

Introducció 5

1. Tiquets electrònics: definició, propietats i requeriments ... 7
1.1. Introducció als tiquets electrònics 7
1.2. Definició de tiquet electrònic 9
1.3. Tiquets electrònics: actors, fases, serveis i informació 9
1.3.1. Actors 9
1.3.2. Fases 10
1.3.3. Serveis 10
1.3.4. Informació 11
1.4. Requeriments dels tiquets electrònics 13
1.4.1. Requeriments de seguretat 13
1.4.2. Requeriments funcionals 21
1.5. Sistemes de tiquets electrònics amb tarificació automàtica 24

2. Descripció d'un sistema de tiquets electrònics amb tarificació automàtica 26
2.1. Participants del sistema 26
2.2. Informació en els tiquets electrònics 27
2.3. Fases del sistema 27
2.4. Configuració inicial 28
2.5. Registre de l'usuari 28
2.6. Entrada en el sistema 29
2.7. Sortida del sistema 29
2.8. Resultat 30

Exercicis d'autoavaluació 31

Bibliografia 32

Introducció

Un tiquet electrònic és un contracte, en format digital, entre un usuari i un proveïdor. Permet reduir tant els costos econòmics com el temps d'ús de molts serveis com són la navegació aèria o el transport públic.

Per tant, la seguretat del tiquet s'ha de garantir completament, així com la privacitat dels seus usuaris. L'ús de tiquets electrònics podria resultar en diversos abusos de la privacitat dels usuaris ja que sovint els tiquets electrònics no presenten la característica d'anonimat. En aquest cas es pot fer un seguiment dels moviments dels usuaris per tal de crear perfils de les seves activitats.

La proliferació de dispositius mòbils amb altes prestacions permet associar l'ús dels tiquets electrònics a aquest tipus de dispositius. Les solucions proposades, per tant, s'han d'adaptar als requeriments i a les característiques dels nous dispositius.

Aquests sistemes han de garantir la seguretat enfront dels intents de frau per part dels usuaris alhora que en garanteixen la privacitat. El proveïdor de servei no ha de poder identificar els usuaris, i diferents usos del mateix usuari no s'han de poder vincular entre ells. Finalment, en cas que un usuari intenti actuar fraudulentament, el seu anonimat hauria de ser revocat.

Determinats serveis no tenen un preu preestablert. El preu a pagar es determina en funció de l'ús que es fa del servei, depenent per exemple, del temps d'ús. Aquests sistemes s'anomenen sistemes de tarificació automàtica. Els tiquets utilitzats en aquests sistemes hauran de funcionar de manera diferent als habituals i el cobrament no es farà en el moment d'emissió del tiquet. En aquest cas es parlarà de tiquets d'entrada i de tiquets de sortida del servei, contindran informacions diferents i seran gestionats per protocols específics, diferents dels protocols utilitzats en el cas general.

Els sistemes de tarificació automàtica (*Automatic Fare Collection*: AFC) calculen la taxa a pagar en funció de l'ús que es fa del sistema, depenent aquest del punt/instant d'accés al servei i el corresponent punt/instant de sortida.

Aquests sistemes, utilitzats en aplicacions com aparcaments o peatges, es basen habitualment en l'ús de paper. Com en el cas general dels tiquets electrònics, la progressiva introducció de les tecnologies de la informació i de la comunicació permeten la reducció del cost del servei al mateix temps que milloren el control de les infraestructures.

1. Tiquets electrònics: definició, propietats i requeriments

1.1. Introducció als tiquets electrònics

L'ús de les tecnologies de la informació (TI) en les operacions del dia a dia està creixent de manera important. El turisme és un exemple de sector afectat per l'ús de les TI. Avui dia és possible obtenir tota la informació sobre un determinat destí, buscar vols arribant a aquest lloc, reservar una habitació d'hotel, museu o aconseguir entrades per a un parc i així successivament. A més, totes aquestes accions es poden realitzar d'una manera molt còmoda: es poden fer a casa i no hi ha restriccions temporals.

Els usuaris dels tiquets en paper s'han de desplaçar a l'entitat emissora de bitllets per rebre'ls, causant una pèrdua de temps, o haver de gestionar un dispositiu capaç d'imprimir el bitllet. Per exemple, un executiu que es mou a l'aeroport amb taxi podria ser capaç de comprar el bitllet utilitzant el seu telèfon mòbil, però el bitllet no es podria imprimir de manera senzilla en aquest escenari. Aquestes limitacions fan que es requereixi passar per l'agència en qüestió, o bé comprar el bitllet en un altre lloc. La manipulació del bitllet de paper té costos per als usuaris i les empreses, que es podrien reduir. Encara que els costos d'una emissió d'un bitllet de paper podria ser baixa, quan hi ha una gran quantitat de bitllets emesos es converteix en un cost que cal tenir en compte. Els costos d'administració també han de ser tinguts en compte.

El grau d'importància d'aquests canvis depèn de l'ús de les TI en mans de les empreses. En general, l'ús de la TI és heterogeni a causa de les diferències entre els sectors i també entre el potencial de cada empresa. Les grans empreses prefereixen explotar les TI amb la finalitat d'obtenir un major rendiment mitjançant l'ús dels últims avenços tecnològics. En cas contrari, les empreses petites inverteixen menys en TI. En el cas de petites empreses relacionades entre elles, l'ús de la TI depèn de l'ús que aquestes empreses petites podria fer.

L'ús de bitllets electrònics en una empresa afecta l'empresa mateixa i l'usuari. Les fases d'adquisició i de recepció podrien ser totalment electròniques, però requereixen que el procés de validació hagi de ser també electrònic. Els usuaris porten bitllets mentre s'estan movent, i els validen per tal d'accedir al servei. Per això, l'usuari ha de tenir un dispositiu adequat per tal de gestionar i utilitzar bitllets electrònics. Els dispositius mòbils (com telèfons mòbils, PDA o telèfons intel·ligents) són considerats com els dispositius millors situats entre els sistemes de taquillatge electrònic. Aquests dispositius ofereixen capacitats de còmput i emmagatzematge adequat i una rica varietat en les últimes tecnologies de comunicació sense fil (Bluetooth, NFC i Wi-Fi). Totes

aquestes característiques estan disponibles en un dispositiu de mida reduïda, proporcionant mobilitat i flexibilitat a aquests sistemes.

A més de les consideracions anteriors, l'aplicació real d'aquests sistemes de bitllets electrònics depèn de la seva seguretat, a causa de la facilitat de còpia dels continguts electrònics i de qüestions relacionades amb la privacitat. Els bitllets electrònics han de ser igualment o fins i tot més segurs que els bitllets de paper.

El transport és un dels principals sectors que utilitzen bitllets en la seva activitat normal. Els bitllets de paper estan essent progressivament substituïts per bitllets electrònics, la qual cosa redueix la despesa de paper i fa tot el procés més dinàmic.

Els tiquets electrònics es poden utilitzar en múltiples serveis de transport. Per exemple, el servei de reserves AMBUS de la República Txeca permet la compra de tiquets SMS. Primer l'usuari rep el tiquet en el seu telèfon mòbil. Aleshores mostra el missatge a l'inspector quan li és sol·licitat.

Les companyies de vol són líders mundials en l'ús de bitllets electrònics i TI emergents. La International Air Transport Association (IATA) va iniciar el 2004 un programa per a introduir l'ús de bitllets electrònics que es va dur a terme completament el 2008. Aquesta iniciativa elimina els costos d'impressores de tiquets, manteniment i distribució de bitllets i representa 3 milions d'estalvi en dòlars anuals a causa del fet que el preu de processar un bitllet electrònic costa un dòlar enfront dels a 10 dòlars per cada bitllet de paper.

Un altre exemple d'això podria ser el cas de les targetes d'embarcament electròniques. Vodafone i Spanair van fer una prova el 2007, en la qual els passatgers rebien la seva targeta d'embarcament electrònica en els seus telèfons mòbils. Altres companyies com Air Canada o Continental han seguit la mateixa direcció i ofereixen serveis similars als seus clients.

Aquests exemples demostren dos fets importants:

1) Hi ha una progressiva introducció dels bitllets electrònics en diferents tipus de serveis.

2) Els telèfons mòbils són la principal plataforma de bitllets electrònics.

A continuació s'enumeren alguns avantatges de l'ús de bitllets electrònics en els telèfons mòbils:

- Els clients poden reservar per tot arreu, fins i tot sense una impressora.
- Les entrades es poden comprar i utilitzar immediatament.
- La comunicació entre els clients i l'empresa és més fàcil i més ràpida.
- La companyia estalvia recursos i accelera el procés de gestió.

Finalment, tot i que el transport és l'escenari més representatiu de l'ús de bitllets electrònics, els bitllets electrònics també es poden utilitzar en altres camps. El sector de l'oci té alguns exemples de sistemes de taquillatge electrònic. Es poden utilitzar per a esdeveniments esportius o qualsevol altre tipus d'espectacle en viu. Per exemple, els seguidors del Leeds United poden reservar un partit i després rebre un SMS amb la confirmació de la reserva juntament amb informació addicional com ara els seus seients assignats.

1.2. Definició de tiquet electrònic

El bitllet o tiquet electrònic és un contracte entre un usuari i un proveïdor de serveis. Si l'usuari demostra la seva possessió del bitllet, obté el dret a utilitzar el servei sota els termes i condicions establerts.

Habitualment, es requereix la validació del tiquet per tal de poder utilitzar el servei. Depenent de les condicions del tiquet aquest pot ser validat una vegada, un nombre predefinit de vegades o bé de manera il·limitada durant un període de temps (fins a una data límit).

Els tiquets han d'incloure elements per a garantir la seguretat del sistema i la privacitat dels usuaris. Els requeriments relacionats amb la seguretat i la privacitat poden ser diferents en diferents aplicacions dels tiquets electrònics. En alguns casos, la seguretat serà un factor crític, com en el cas d'impedir la falsificació en els bitllets de transport aeri. En altres aplicacions, els requeriments de seguretat, com l'anonimat dels usuaris, són indispensables.

A continuació es defineixen els principals requeriments de seguretat, les fases dels sistemes de tiquets electrónics i els participants involucrats en el sistema. També es defineixen determinats camps d'informació inclosos en els tiquets electrònics.

1.3. Tiquets electrònics: actors, fases, serveis i informació

Aquesta secció inclou una anàlisi dels sistemes de tiquets electrònics, primer definint els participants involucrats, les fases relacionades, i la informació que hauria de formar part dels tiquets electrònics.

1.3.1. Actors

A continuació es descriuen els participants que intervenen en el procés de creació i utilització dels tiquets electrònics.

- **Usuari**: rep el tiquet electrònic després de la seva creació i el presenta per a la seva validació per tal de tenir accés al servei.
- **Emissor**: emet el tiquet electrònic i el lliura a l'usuari. Els tiquets electrònics poden ser emesos tant pels mateixos proveïdors de servei com per intermediaris.
- **Proveïdors de servei**: reben els tiquets electrònics dels usuaris i s'encarreguen de la seva validació. Si aquesta validació és satisfactòria proporciona a l'usuari accés al servei associat al tiquet electrònic.

Aquests són els participants principals i habituals dels sistemes de tiquets electrònics, però determinats sistemes incorporen altres participants. Si s'utilitza criptografia de clau pública en el sistema, aleshores es requeriran els serveis d'una autoritat de certificació. En altres casos, el sistema de tiquets electrònics es basa en l'ús de targetes intel·ligents (*Smart-Cards*). En aquest cas també s'inclourà en el sistema l'emissor de targetes. Altres possibles actors són: agents d'usuari, proveïdor de servei d'accés a xarxa, proveïdors de serveis de pagament, bancs, emissors de targetes de crédit, etc.

1.3.2. Fases

En la majoria dels sistemes proposats, els autors determinen tres fases principals:

- Pagament del tiquet electrònic
- Emissió
- Validació

Tot i aquesta aparent uniformitat, aquestes fases no sempre es defineixen de la mateixa manera. Alguns autors agrupen les fases de pagament i emissió, convertint sistemes de tres fases en sistemes d'únicament dues fases.

Altres propostes afegeixen una fase prèvia de registre on els usuaris han de ser identificats i autenticats per tal d'obtenir permís per a accedir al sistema. Puntualment, juntament amb les fases enumerades anteriorment, es considera una fase d'inici de servei i una de finalització de servei.

Aquestes variacions en la definició de les fases dels sistemes de tiquets electrònics és deguda a les grans diferències existents entre les propostes, accentuades per les diferències en els serveis accessibles per cada tipus de tiquets electrònics.

1.3.3. Serveis

Fins ara, les propostes existents de sistemes de tiquets electrònics ofereixen accés a diferents tipus de serveis. Es pot destacar d'entre els sistemes existents

que l'àrea de serveis predominant és la del transport. D'entre elles se'n poden trobar algunes específiques per a sistemes de transport ferroviari, per a transport aeri, autobusos o metro.

També es poden trobar sistemes que utilitzin tiquets electrònics per a la gestió de peatges. En aquest cas el funcionament del sistema és lleugerament diferent ja que els usuaris paguen pel servei una vegada aquest ha estat utilitzat i la quantitat involucrada en el pagament depèn d'algun factor relacionat amb l'ús. El pagament es realitza en el moment de finalització de l'ús del servei utilitzant algún sistema de pagament electrònic. Un cas semblant és el dels taxis. La diferència es troba en el factor a tarificar, en un cas és la distància recorreguda mentre que en l'altra és el temps d'ús. Aquests serveis, s'adeqüen als sistemes de tarificació automàtica (AFC). La tarificació automàtica no es limita als sistemes de transport, també se'n poden trobar aplicacions a altres tipus de serveis, com en l'ús d'insta l·lacions.

1.3.4. Informació

De manera semblant als tiquets basats en paper, els tiquets electrònics han d'incloure un conjunt d'informacions bàsiques per al seu funcionament. Alguns continguts poden ser específics del servei, altres es relacionen amb la seguretat del sistema.

A continuació, aquesta secció descriu els camps d'informació que s'inclouen en els tiquets electrònics.

- **Número de sèrie**
  Número d'identificació únic per a cada tiquet electrònic.

- **Emissor**
  Identitat de l'entitat que és responsable de l'emissió dels tiquets electrònics. L'emissor pot ser el mateix proveïdor de servei o un intermediari.

- **Proveïdor de servei**
  Identitat de l'entitat que ofereix el servei a l'usuari.

- **Usuari**
  Informació sobre el propietari del tiquet electrònic. En cas que en aquest camp aparegui en el tiquet i incorpori la identitat de l'usuari o alguna dada identificativa, aleshores la propietat d'anonimitat no es podria assolir.

- **Servei**
  Descripció del contracte de servei.

- **Termes i condicions del contracte**

  Descripció, dins del mateix tiquet electrònic dels termes i condicions de contractació. Alternativament es pot incloure un enllaç a un lloc extern on es trobin els termes i condicions.

- **Tipus de tiquet electrònic**

  El tiquet electrònic inclou un camp on s'indica el tipus de tiquet.

- **Transferibilitat**

  Si s'incorpora aquest camp, la transferència del tiquet electrònic entre usuaris estarà permesa.

- **Nombre d'usos**

  En el cas de tiquets electrònics reusables un nombre predefinit de vegades, aquest camp indicarà el nombre màxim d'utilitzacions permeses amb el tiquet.

- **Destinació**

  Camp utilitzat en els tiquets específics per al transport on es fixa la destinació.

- **Atributs**

  Altres atributs d'un tiquet electrònic que s'han d'incorporar en el tiquet. En funció del tipus de servei els atributs seran d'un o altre tipus. Per exemple, en un tiquet que representa l'entrada a un teatre s'inclourà un atribut que indiqui el número de seient.

- **Temps de validesa**

  El temps de validesa és determinat per dues dates, la d'inici del servei i la data de caducitat.

- **Data d'emissió**

  Marca temporal de l'instant d'emissió del tiquet electrònic. El temps de validesa pot venir determinat pel valor d'aquest camp i el contingut dels termes i condicions del contracte.

- **Signatura digital de l'emissor**

  L'emissor disposa d'un parell de claus d'un criptosistema de clau pública que li permet signar digitalment el tiquet electrònic.

- **Identificació del dispositiu**

  Camp que especifica, si és el cas, la vinculació del tiquet electrònic a un dispositiu físic específic.

1.4. Requeriments dels tiquets electrònics

Els requeriments dels tiquets electrònics es poden classificar en dues categories. D'una banda els requeriments relacionats amb la seguretat i de l'altra els requeriments funcionals dels tiquets. Alguns dels requeriments són difícils de classificar ja que poden tenir impacte en les dues categories: funcionalitat i seguretat.

1.4.1. Requeriments de seguretat

- **Definició 1: Integritat**

> Ha de ser possible determinar si un tiquet electrònic ha estat manipulat i modificat, respecte del tiquet emès pel corresponent emissor autoritzat.

Tots els participants han de ser capaços de verificar si un tiquet electrònic ha estat manipulat, o el que és el mateix, tots els tiquets han de ser emesos per un emissor autoritzat.

- **Definició 2: Autenticitat**

> Els usuaris han de ser capaços de verificar qui ha emès el tiquet electrònic.

L'assoliment d'aquest requeriment permetrà als usuaris comprovar si l'emissor és l'emissor autoritzat.

- **Definició 3: No-repudi d'origen**

> L'usuari que genera o envia un missatge no ha de ser capaç de denegar la seva emissió o generació una vegada realitzada.

Aquest requeriment pot ser útil en diferents etapes, però és particularment important en relació amb l'emissió de tiquets electrònics vàlids: l'emissor no ha de ser capaç de denegar haver emès aquell tiquet electrònic, i el seu contingut específic. Observeu que, de fet, aquest requeriment inclou els requeriments d'autenticitat i integritat: si l'usuari no pot negar haver emès

un tiquet electrònic significa que es pot verificar que ell ha emès el tiquet (autenticitat) i que ningú ha modificat el contingut del tiquet electrònic (integritat). A vegades serà necessari que l'usuari que ha sol·licitat el tiquet electrònic no sigui capaç de negar la seva sol·licitud.

- **Definició 4: No-repudi de recepció**

  L'usuari que rep un missatge no ha de ser capaç de denegar la seva recepció.

  Aquest requeriment també pot ser útil en diferents etapes en els sistemes de tiquets electrònics. Per exemple, un usuari que ha sol·licitat i rebut un tiquet no ha de ser capaç de denegar que l'ha rebut. Un altre exemple és el cas d'un proveïdor que ha rebut un tiquet electrònic a canvi d'un servei; el proveïdor no ha de ser capaç de negar la recepció del tiquet electrònic.

- **Definició 5: Infalsificabilitat**

  Només els usuaris autoritzats poden emetre tiquets electrònics vàlids.

  En altres paraules, no ha de ser possible crear tiquets electrònics i fer-los passar per tiquets electrònics autèntics, com si haguessin estat creats per un usuari autoritzat. Aquest requeriment està directament relacionat amb el requeriment de no-repudi d'origen, i per tant amb els requeriments d'integritat i autenticitat.

- **Definició 6: Equitat**

  Al final d'un intercanvi entre dues o més parts, o bé cada una de les parts ha rebut els objectes esperats o bé ningú ho ha fet. Per tant, ningú es troba en una situació privilegiada.

  Aquest requeriment està estretament relacionat amb el de no-repudi, però va un pas més enllà ja que cerca no només assegurar que les parts no puguin negar, *a posteriori*, haver participat en la transacció sinó que també vol el compromís de les parts amb una transacció determinada, a través de l'equitat. Amb el compromís establert es tracta d'una transacció que compromet totes les parts o cap. Aquest requeriment pot ser útil en diversos processos relacionats amb la gestió dels tiquets electrònics.

– **Emissió**. Si l'usuari consumidor paga el preu del tiquet electrònic aleshores hauria de rebre de l'emissor un tiquet electrònic vàlid, i viceversa, si l'usuari consumidor rep un tiquet electrònic vàlid ha de pagar el preu corresponent o, depenent del sistema, proporcionar una prova que ha rebut el tiquet electrònic. Hi pot haver excepcions al cas general, com per exemple en el cas de donacions, tiquets gratuïts, etc.

– **Ús**. Si l'usuari consumidor dóna un tiquet electrònic vàlid al proveïdor de servei, el proveïdor de servei ha de donar accés al servei vinculat, i viceversa.

– **Compensació**. Si el proveïdor de servei disposa d'un tiquet electrònic vàlid (rebut d'un usuari) haurà de rebre, si és aplicable en el cas concret, la compensació corresponent (típicament econòmica). Si el proveïdor de servei ha rebut aquesta compensació, aleshores ha de proporcionar una prova que l'ha rebut.

  Per tant, els sistemes de gestió de tiquets electrònics han d'utilitzar protocols d'intercanvi equitatiu i aconseguir algunes de les propietats relacionades amb aquests protocols. S'hauran d'implementar intercanvis equitatius de valors (tiquet electrònic a canvi de pagament, servei a canvi de tiquet...) i incloure les propietats de equitat, *abuse-freeness*, asincronia, verificabilitat de la TTP, etc.

- **Definició 7 (No reutilització o sobreutilització)**

  Els tiquets electrònics es poden utilitzar les vegades acordades en la contractació entre l'emissor i l'usuari consumidor.

  Els tiquets electrònics no reutilitzables només es poden utilitzar una única vegada, per tant després de la seva validació no tenen més utilitat i no s'ha de permetre que l'usuari intenti defraudar presentant el mateix tiquet electrònic en una validació posterior. Els tiquets electrònics reusables es poden utilitzar tantes vegades com s'hagi acordat en el moment de la seva compra i emissió. No s'ha de permetre la seva validació quan ja s'ha arribat al nombre màxim d'utilitzacions.

  Finalment, alguns tiquets electrònics es poden utilitzar de manera ilimitada durant un determinat període de temps (vegeu la propietat de reusabilitat).

  Els mecanismes per a controlar la reutilització poden afectar el requeriment d'anonimitat. La reutilització / sobreutilització es pot prevenir o bé detectar. Si la reutilització / sobreutilització es detecta a la fase de validació no es permetrà i per tant el frau serà previngut.

D'altra banda, si la reutilització / sobreutilització es detecta *a posteriori*, després de la validació es farà necessaria una manera d'identificar el reutilitzador.

Aquest requeriment està íntimament relacionat amb el requeriment d'unicitat dels tiquets basats en paper: aquests són documents únics. Això significa que es pot distingir entre original i còpia (encara que algunes copies són difícils d'identificar). Aquí podem trobar un altre requeriment relacionat amb la unicitat: la falsificació.

En el món electrònic és possible que no tingui sentit parlar d'original i còpia: són dues cadenes de bits idèntiques i per tant indistingibles. Qualsevol document electrònic accessible pot ser susceptible de ser duplicat tantes vegades com es vulgui. Quan es vol parlar de còpies de documents electrònics no usables s'han d'utilitzar les tècniques adequades per a aconseguir aquest requeriment:

a) Dispositius resistents a manipulació. Els dispositius d'aquest tipus (per exemple, les targetes intel·ligents) prevenen que els documents electrònics emmagatzemats en el dispositiu siguin manipulats. Per tant, la distribució de documents amb requeriment d'unicitat és possible utilitzant aquest tipus de dispositius. En aquest cas la seguretat del sistema es basa en el fet que els costs de manipulació han de ser superiors als beneficies que l'atacant pot obtenir. També s'han de tenir en compte tant l'usabilitat com la comoditat dels usuaris a l'hora d'utilitzat el servei.

b) Algunes entitats fan un seguiment dels tiquets electrònics utilitzats de manera centralitzada. Encara que d'aquesta manera no es pot garantir la unicitat del document (tiquet electrònic), sí que es pot garantir la unicitat del seu ús, és a dir, que sigui utilitzat una única vegada.

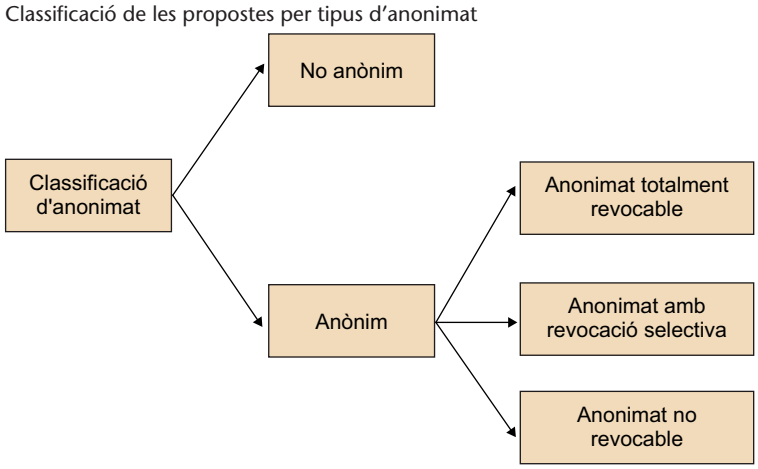
En relació amb el moment en què l'entitat controladora coneix que s'està fent un intent de reutilització es poden distingir dos tipus de tècniques: prevenció (l'intent de reutilització és detectat i no permès, típicament en una transacció en línia amb l'entitat controladora) i detecció *a posteriori* (en aquest cas es realitza la reutilització i després es detecta en alguna fase del protocol).

Qualsevol que sigui la tècnica utilitzada només s'ha de permetre la utilització d'una còpia vàlida del tiquet electrònic.

- **Definició 8: Tiquets electrònics identificats.**

  La identitat del propietari del tiquet electrònic ha de poder ser verificada.

No tots els tiquets basats en paper presenten els mateixos requeriments en relació amb l'anonimat, per tant s'han de distinguir diversos possibles escenaris per als tiquets electrònics. El primer tipus és el dels tiquets electrònics no anònims, on el servei requereix la identificació i la autenticació de l'usuari. Això implica que la identitat s'ha de trobar dins del tiquet electrònic d'una manera o altra, per tal que el proveïdor del servei pugui verificar que l'usuari està autoritzat a gastar el tiquet electrònic. Aquest és el cas dels bitllets d'avió. En l'etapa d'embarcament el personal auxiliar de la companyia de vol ha de ser capaç de verificar que la identitat del viatger és la mateixa que la identitat continguda en el tiquet electrònic.



- **Definició 9: Anonimat totalment revocable.**

L'anonimat dels usuaris es pot revocar, revelant-ne la identitat. Les condicions que permeten la revocació no són selectives sinó que tots els usuaris poden patir la revocació amb independència del seu comportament.

La identitat dels usuaris és inclosa, d'una manera determinada (en forma de pseudònim, identitat real...), en els tiquets electrònics. Típicament només un conjunt reduït d'actors estan capacitats per a revocar l'anonimat, i només ho haurien de fer en cas de detectar una reutilització durant el procés de validació. Això implica que el tiquet podria ser utilitzat més vegades de les desitjades. Per als tiquets electrònics identificats això no és un problema: es coneix la identitat del reutilitzador i per tant es poden dur a terme accions apropiades per a la seva penalització. En canvi, en els tiquets electrònics anònims l'anonimat ha de ser revocable per tal d'identificar els infractors reutilitzadors. Òbviament, els usuaris honestos haurien de romandre anònims o, almenys, haurien de poder demostrar la seva honestedat.

- **Definició 10: Anonimat amb revocació selectiva**

  La identitat dels usuaris fraudulents, i només dels fraudulents, propietaris de tiquets electrònics inicialment anònims pot ser revelada.

  Aquest requeriment és bastant semblant a l'anterior, però és més restrictiu: només els usuaris deshonestos poden perdre el seu anonimat. Des del punt de vista de la privacitat, aquest requeriment és millor que l'anterior (anonimat totalment revocable) i també es pot considerar millor que el següent (anonimat no revocable). El problema és que aquest requeriment pot necessitar solucions tècniques més complexes.

- **Definició 11: Tiquets electrònics anònims**

  L'usuari d'un tiquet electrònic és anònim i serà anònim en qualsevol circumstància.

  Alguns tiquets basats en paper permeten que l'usuari sigui anònim i no hagi de mostrar la seva identitat ni a l'emissor, ni al validador ni al proveïdor de servei. Seria lògic que els tiquets electrònics associats als mateixos serveis mantinguessin aquesta propietat. Aquest requeriment es relaciona amb el tiquet electrònic, amb la manera de fer l'emissió i en la manera d'utilitzar-lo. L'anonimat es manté durant tot el cicle de vida del tiquet electrònic.

  Tot i així, depenent del mètode de pagament utilitzat, l'usuari podria ser identificat en aquesta fase. En qualsevol cas, l'usuari consumidor ha de ser capaç de gastar el tiquet electrònic sense cap identificació. Ni tan sols la confabulació entre l'emissor i el proveïdor de servei ha de ser capaç de trencar l'anonimat dels consumidors. Alguns serveis requereixen tiquets electrònics amb aquesta propietat i en cap cas ha de ser possible identificar l'usuari.

- **Definició 12: Exculpabilitat**

  L'usuari consumidor d'un servei ha de ser capaç de demostrar que ha validat el tiquet electrònic abans de fer ús del servei.
  A més, el proveïdor de servei no pot acusar falsament un usuari consumidor honest d'haver utilitzat prèviament el tiquet electrònic.

Aquest requeriment ha esta proposat recentment a Vives-Guasch i altres (2012), per a tiquets electrònics. Un usuari honest que ha validat un tiquet electrònic ha de disposar de proves que li permetin demostrar aquest fet. Presentant aquestes proves evitarà que el proveïdor de servei el pugui acusar falsament.

- **Definició 13: Reusabilitat**

> El tiquet electrònic pot ser creat amb la intenció que pugui ser utilitzat més d'una vegada.

Habitualment un tiquet electrònic pot ser utilitzat tan sols una vegada. És el cas dels tiquets electrònics no reusables. En els tiquets no reusables els intents de realitzar un segon ús amb el mateix tiquet electrònic es consideraria reutilització.

Si el tiquet electrònic presenta la propietat de reusabilitat podrà ser utilitzat diverses vegades sense que això representi una reutilització. Els nombre d'usos que es permeti fer del tiquet electrònic dependrà del tipus de reutilització. La reutilització amb un nombre d'usos prefixat es presenta en serveis com alguns casos de transport públic urbà, on un abonament permet realitzar un nombre prefixat de viatges. El comptador associat a l'abonament es decrementa en cada viatge. El segon tipus de reutilització no prefixa el nombre d'usos sinó que permet un nombre il·limitat d'usos en un període determinat. Fins i tot, es poden trobar casos on el mateix tiquet pot ser utilitzat en diferents serveis (per exemple, bus i metro).

En qualsevol cas, la sobreutilització dels tiquets electrònics s'ha d'evitar (prevenció o detecció). Els tiquets electrònics han d'incorporar mesures de seguretat per a permetre només l'ús del tiquet en el període indicat o bé respectar el nombre d'usos màxim.

A vegades es parla de reutilització anomenant-la divisibilitat, entenent cada ús del tiquet electrònic com una divisió del tiquet complert.

- **Definició 14: Transferabilitat**

> Un usuari pot transferir de manera segura el seu tiquet electrònic a un altre usuari perquè aquest darrer l'utilitzi.

En molts casos, els tiquets basats en paper es poden transferir d'un usuari a un altre. És el cas de les entrades per a espectacles, bitllets d'autobus...).

Òbviament aquest no és el cas dels tiquets electrònics identificats (bitllets d'avió...).

Els usuaris que reben un tiquet electrònic a través d'una transferència i no directament d'un emissor autoritzat han de ser capaços de verificat que el tiquet electrònic rebut és vàlid (no serà complicat si el tiquet electrònic satisfà els requeriments de no-repudi, integritat i autenticitat). També hauria de poder comprovar que l'usuari que li ha transmès el tiquet electrònic no l'ha utilitzat prèviament (ni tampoc els usuaris anteriors). En el cas de regals o donacions entre gent que es té confiança no farien falta mesures especials per a assegurar que el tiquet electrònic no ha estat utilitzat prèviament, i la reutilització serà un assumpte a resoldre personalment.

Si els tiquets electrònics es revenen (sempre que el servei permeti la revenda) l'entitat que paga per rebre la transferència d'un tiquet electrònic s'ha d'assegurar tant que el tiquet electrònic sigui vàlid com que no hagi estat utilitzat prèviament. Podria ser que l'usuari transmissor intentés la reutilització a través d'una utilització i una transferència. Aquet intent de frau s'ha de tractar com els casos estàndard de reutilització. Per tant, en cas de sistemes amb anonimat revocable, la revocació s'ha d'aplicar també a aquest nou tipus de frau.

La transferibilitat implica un intercanvi entre dos usuaris consumidors. L'equitat pot ser requerida també en aquest nou intercanvi.

Atesa la descripció anterior, dues noves definicions de transferibilitat es fan necessàries.

- **Definició 15: Transferibilitat debil**

  El tiquet electrònic és transferible però la reutilització no es pot verificar en la fase de transferència.

En aquest cas el tiquet electrònic pot ser utilitzat per un usuari diferent de l'usuari que ha estat el primer propietari del tiquet. El receptor del tiquet electrònic a través d'una transferència no podrà estar segur de poder utilitzar el tiquet. Podria ser que, en el moment de la recepció del tiquet, aquest ja hagués estat utilitzat pel transmissor o bé que el transmissor hagués transmès el tiquet electrònic a diversos receptors. Serà en el moment de presentar el tiquet electrònic per a la seva validació quan el receptor sabrà si el tiquet és vàlid ja que el proveïdor de servei li indicarà si el tiquet ja ha estat utilitzat. Aquest inconvenient es pot suavitzar si el receptor pot demostrar que el transmissor és qui ha comès el frau.

- **Definició 16: Transferibilitat forta**

  El tiquet electrònic és transferible i el receptor pot verificar que el tiquet rebut podrà ser utilitzat.

  En aquest cas el receptor ha de poder estar segur que podrà utilitzar el tiquet electrònic. Això implica que el tiquet no ha d'estar utilitzat i també que no es podrà transmetre a altres usuaris.

1.4.2. Requeriments funcionals

Hi ha altres requeriments que no estan directament relacionats amb la seguretat però que es poden considerar tan importants com els descrits prèviament.

- **Definició 17: Data de caducitat**

  Un tiquet electrònic només és vàlid durant un interval de temps.

  El compliment d'aquest requeriment pot ser útil per tal de minimitzar la mida de la base de dades que conté la informació dels tiquets electrònics ja utilitzats.

- **Definició 18: Verificació fora de línia**

  La verificació dels tiquets electrònics es pot realitzar sense cap connexió externa.

  En algunes situacions no serà possible contactar amb bases de dades externes o terceres parts de confiança per tal de comprovar si els tiquets electrònics són vàlids o no. Potser no serà el cas general, però s'ha de tenir prevista una solució per a aquest problema. Aquest requeriment està íntimament relacionat amb els mecanismes de seguretat utilitzats.

- **Definició 19: Verificació en línia**

La verificació dels tiquets electrònics requereix una connexió persistent amb un sistema centralitzat de confiança.

Típicament l'opció fora de línia és la preferible per raons de cost, possibles colls d'ampolla, etc.; però en el món digital on milions de transaccions mitjançant targeta de crèdit es realitzen en línia i on companyies com Google o Facebook treballen amb un poder computacional molt elevat, sembla que aquest argument no sigui vàlid.

En termes de seguretat, la verificació en línia és millor pel tractament de la reutilització o sobreutilització.

- **Definició 20: Portabilitat**

Els tiquets electrònics han de poder ser emmagatzemats en dispositius mòbils.

Els tiquets electrònics, com els tiquets en paper, han de poder ser transportats pels usuaris. No hauria de ser necessari un ordinador per a la gestió dels tiquets electrònics. Telèfons mòbils, telèfons intel·ligents, targetes intel·ligents... hauran de ser capaços d'emmagatzemar i processar tiquets electrònics.

- **Definició 21: Mida reduïda**

Els tiquets electrònics han de ser tan petits com sigui possible.

Típicament, els tiquets electrònics s'emmagatzemaran en dispositius mòbils i a vegades aquests dispositius tenen una memòria amb importants limitacions (com en el cas de les targetes). Per aquests motius, els tiquets electrònics han de tenir la mida més petita possible.

- **Definició 22: Flexibilitat**

Els tiquets electrònics s'han de poder utilitzar en múltiples entorns.

Podem pensar en moltes aplicacions diferents dels tiquets electrònics (bitllets d'avió, bitllets de bus, entrades de concerts, entrades de museu, etc.). Es pot dissenyar un sistema de tiquets electrònics per a cada aplicació o es pot adaptar un sistema general de tiquets a cada situació. Òbviament, la darrera solució és preferible per tal d'economitzar la solució, i permetre una millor anàlisi de seguretat.

- **Definició 23: Facilitat d'ús**

  L'aprenentatge d'ús dels tiquets electrònics ha de ser senzill.

  Estem pensant en els tiqets electrònics com a solució per al públic general (usuaris de tiquets en paper i no necessàriament especialista en l'ús de dispositius electrònics). Els tiquets electrònics han de ser tan fàcils d'utilitzar com els tiquets basats en paper i sense que comportin problemes per als usuaris.

- **Definició 24: Eficiència**

  El processament dels tiquets electrònics no ha de requerir el consum elevat de recursos.

  Es pot pensar en l'eficiència des de dos punts de vista. Primer, els terminals mòbils poden tenir limitacions en termes de poder computacional i per tant les operacions incloses en els protocols, especialment les operacions criptogràfiques s'han de reduir a només les imprescindibles.

  En segon lloc, la capacitat de comunicació també pot ser limitada i per tant el protocol s'ha de dissenyar tenint en compte aquesta limitació. Per tant, el retard degut a la verificació del tiquet electrònic ha de ser raonable en una proposta de tiquets electrònics.

- **Definició 25: Flexibilitat de pagament**

  Els tiquets electrònics s'han de poder obtenir utilitzant sistemes de pagament habituals.

  El disseny d'un sistema de tiquets electrònics ha de tenir en compte que en molts casos requerirà l'ús d'un sistema de pagament. Per això els sistemes

de tiquets han de permetre l'ús de diferents sistemes de pagament per tal d'obtenir el tiquet en la fase d'emissió.

- **Definició 26: Utilització global**

  Els usuaris consumidors haurien de ser capaços d'utilitzar els tiquets electrònics en qualsevol dels proveïdors de serveis autoritzats.

  Aquesta propietat s'oposa a la de tiquets utilitzables selectivament. En aquest darrer cas els tiquets només es poden utilitzar en un proveïdor específic.

- **Definició 27: Disponibilitat**

  Els tiquets electrònics han de poder ser utilitzats en el moment requerit.

  Aquest requeriment es pot veure com un requeriment de seguretat, però és complicat fer front a aquest problema només des del punt de vista de la seguretat. Podem estar pensant en atacs de denegació de servei, situacions catastròfiques o malfuncionaments temporals. Això podria significar que els tiquets electrònics no podrien ser validats, i podrien causar el retard en el servei (concert, vol...). S'ha de dissenyar un procediment per a gestionar situacions d'aquest estil.

1.5. Sistemes de tiquets electrònics amb tarificació automàtica

Determinats serveis susceptibles d'utilitzar tiquets electrònics tenen un funcionament lleugerament diferent. Es tracta de serveis on el preu d'utilització no està prefixat i depèn de l'ús que en faci l'usuari consumidor.

Exemples d'aquests serveis són els peatges que es paguen a les autopistes. En el moment de començar a utilitzar el servei els usuaris obtenen un tiquet però no paguen per ell, ja que en aquell moment el preu que pagaran encara no està determinat. La incorporació de les tecnologíes de la informació i les comunicacions (TIC) en els sistemes de peatges permet reduir costos i obtenir millores en el control de les infraestructures, com podria ser la monitorització de la densitat de tránsit en temps real, o la planificació de les infraestructures en funció dels fluxos de viatgers.

Però els sistemes de tarificació automàtica no es limiten als peatges. Diversos sistemes de tarificació automàtica s'apliquen al transport públic. Es tracta dels

casos on l'usuari no especifica prèviament la seva destinació, sinó que la tarifa es calcula en funció del lloc pel que s'accedix al servei i del lloc per on se surt del sistema. En aquest sentit, és neccesari habilitar una gestió segura de les entrades (*check-in*) i de les sortides (*check-out*), atès que els usuaris paguen en funció d'aquesta utilització.

Si el sistema identifica cada usuari i coneix els seus moviments, pot fer-ne un seguiment vulnerant la seva privacitat. Per aquest motiu, els sistemes de tarificació automàtica han d'incorporar mesures per tal de preservar la privacitat dels usuaris.

La distància és un factor que pot ser la base per al càlcul de la tarifa a pagar en un sistema de tarificació automàtica però no és l'únic. També es poden trobar serveis on el factor a farificar és el temps. És el cas d'ús d'instal·lacions o bé de serveis de transports com els taxis.

A l'hora de dissenyar un sistema de tiquets electrònics amb tarificació automàtica s'han de redefinir les fases, ja que ara hi haurà una fase d'entrada al sistema, en la qual s'obtindrà el tiquet electrònics d'entrada i una altra fase de sortida on es realitzarà el pagament i s'obtindrà el tiquet electrònic de sortida.

A continuació es descriu un sistema de tiquets electrònics on la tarificació es fa de manera automàtica.

2. Descripció d'un sistema de tiquets electrònics amb tarificació automàtica

Una vegada descrits els sistemes de tiquetatge electrònic, aquest capítol pretén mostrar, de manera més pràctica, com seria un sistema de gestió de tiquets electrònics. Per a fer-ho, aquest capítol descriu, en forma d'exemple, un sistema de tiquets electrònics amb tarificació automàtica. Amb la descripció d'aquest sistema es veuran diferents tècniques que s'apliquen al sistema per a anar aconseguint algunes de les propietats descrites amb anterioritat. El sistema satisfà diversos dels requeriments exposats anteriorment, com ara l'anonimat revocable i la no-vinculabilitat. El protocol presentat és una simplificació del protocol (Isern-Deyà, 2012) deixant de banda alguns aspectes per la seva sofisticació. El protocol es va dissenyar amb l'objectiu que els usuaris utilitzin els seus dispositius mòbils per a l'accés al servei. Com s'ha comentat anteriorment, en tractar-se d'un sistema de tarificació automàtica, un servei al qual es podria aplicar la proposta seria un sistema de peatges. Cal destacar que els usuaris no necessiten obtenir una credencial nova cada vegada que realitzen un viatge.

A continuació es desciu el protocol que protegeix l'anonimat dels usuaris mitjançant signatures de grup. Per a fer-ho es descriuen els participants del sistema, les propietats de seguretat, la informació dels bitllets d'entrada i sortida, i les fases del sistema.

Signatura de grup

Mètode per a permetre a un membre d'un grup signar un missatge de tal manera que en la verificació de la signatura es pugui determinar que es tracta d'un membre vàlid del grup però no es pugui determinar de quin membre concret es tracta.

2.1. Participants del sistema

En el sistema descrit participen els actors següents:

- Usuari $\mathcal{U}$: accedeix al sistema de transport i paga pel servei rebut a la sortida.
- Proveïdor de serveis ($\mathcal{P}_\mathcal{S}$ és el proveïdor d'origen, $\mathcal{P}_\mathcal{D}$ és el proveïdor de destinació): estació que controla els tiquets electrònics utilitzats per l'usuari $\mathcal{U}$.
- TTP de pagament $\mathcal{M}_\mathcal{C}$: gestiona els pagaments dels usuaris quan aquests acaben d'utilitzar el servei i realitzen la sortida del sistema.
- TTP de grup $\mathcal{M}_\mathcal{G}$: gestiona les claus de grup, les llistes de revocació dels usuaris, etc. Té potestat de revocar l'anonimat d'un usuari si aquest actua deshonestament a partir de la signatura de grup dels tiquets electrònics d'entrada i sortida.

2.2. Informació en els tiquets electrònics

En tractar-se d'un sistema amb tarificació automàtica, el sistema maneja dos tipus de tiquets electrònics: els d'entrada i els de sortida. A continuació, es descriu la informació que tenen els tiquets electrònics d'entrada (Taula 1) i de sortida (Taula 2), a més de mostrar la notació (Taula 3).

Taula 1. Informació del tiquet electrònic d'entrada ($t_{in}{}^*$)

Nom	Notació	Descripció
Nombre de sèrie	Sn	generat per $\mathcal{P}_\mathcal{S}$
Estació d'entrada	Ps	identificador de $\mathcal{P}_\mathcal{S}$
Timestamp d'entrada	τ_1	marca de temps d'entrada
Temps de validessa	τ_v	temps per a ser verificat
Compromís de $\mathcal{U}$	σ^*	compromís de l'usuari signat
Signatura digital	$Sign_{\mathcal{P}_\mathcal{S}}(t_{in})$	contingut signat per $\mathcal{P}_\mathcal{S}$

Taula 2. Informació del tiquet electrònic de sortida ($t_{out}{}^*$)

Nom	Notació	Descripció
Informació de validació	θ^*	enviat per $\mathcal{U}$
Tarifa	a	quantitat pagada
Timestamp de pagament	τ_5	marca de temps del pagament
Signatura digital	$Sign_{\mathcal{P}_\mathcal{D}}(t_{out})$	contingut signat per $\mathcal{P}_\mathcal{D}$

Taula 3. Informació de la notació, ordenada por ordre d'aparició

Nom	Notació
Clau pública de grup	gpk
Llista de claus privades per a cada usuari del grup	$gsk[\,]$
Llista de revocacions del grup	$grt[\,]$
Base d'exponenciació	α
Nombre primer	p
Nombre primer	q
Pseudònim de $\mathcal{U}$ (per al pagament)	$y_\mathcal{U}$
Exponenciació inversa de $y_\mathcal{U}$ (secreta)	$x_\mathcal{U}$
Nombre aleatori	r
Exponenciació de r	δ_1
Encriptació probabilística de $y_\mathcal{U}$	δ_2
i-èssima marca de temps	τ_i
Signatura digital del contingut *content* per a l'entitat E	$Sign_E(content)$
Tiquet electrònic d'entrada signat per $\mathcal{P}_\mathcal{S}$	$t_{in}{}^*$
Repte per a $\mathcal{U}$ per tal de demostrar l'autoria de $y_\mathcal{U}$	c
Repte i tarifa signats per $\mathcal{P}_\mathcal{D}$ per a $\mathcal{U}$	β^*
Resposta de $\mathcal{U}$ al repte c	ω
Encriptació probabilística de ω	γ
Acceptació del cobrament signada per part de $\mathcal{M}_\mathcal{C}$	ok^*
Tiquet electrònic de sortida signat per $\mathcal{P}_\mathcal{D}$	$t_{out}{}^*$

2.3. Fases del sistema

Els participants en el sistema realitzaran les accions descrites en un conjunt d'operacions. En el sistema es defineixen les fases següents:

- Configuració inicial: $\mathcal{M}_\mathcal{G}$ genera totes les claus de grup, llistes de revocació, etc.

- Registre de l'usuari: $\mathcal{U}$ es registra a $\mathcal{M}_\mathcal{G}$, adquirint un parell de claus de grup. També crea un compte amb $\mathcal{M}_\mathcal{C}$ mitjançant un pseudònim que serà utilitzat únicament per als pagaments.

- Entrada al sistema: els usuaris entren a la seva estació origen i generen una signatura de grup que certifica que són usuaris vàlids registrats del sistema. Aquesta signatura no revela la seva identitat. A partir d'aquesta signatura reben un tiquet electrònic d'entrada que hauran de mostrar a la sortida.

- Sortida del sistema: l'usuari s'autentica una altra vegada a l'estació de destinació com a usuari vàlid del grup i mostra el seu bitllet d'entrada. El proveïdor $\mathcal{P}_\mathcal{D}$ calcula la quantitat que ha de pagar l'usuari a partir de la tarifa vigent. L'usuari accepta el pagament i genera l'acceptació que s'envia a $\mathcal{M}_\mathcal{C}$. A partir de l'acceptació $\mathcal{M}_\mathcal{C}$ carrega l'import en el compte de $\mathcal{U}$. Si tot el procés és correcte, l'usuari rep un tiquet electrònic de sortida.

2.4. Configuració inicial

Aquesta fase s'executa únicament una vegada per al conjunt d'usuaris. $\mathcal{M}_\mathcal{G}$ genera el grup de la mida establerta, generant com a sortida (gpk,gsk[ ],grt[ ],α,p,q), essent gpk la clau pública compartida del grup, cada clau privada de l'usuari és $gsk[i]$, la llista d'usuaris revocats en el grup és grt[ ], i (α,p,q) són paràmetres públics, essent α la base pública d'exponenciació, i (p,q) nombres primers tals que $p = 2q + 1$, cardinals dels seus grups corresponents $\mathbb{Z}_p$ y $\mathbb{Z}_q$. A més, els proveïdors de servei generaran les seves pròpies parelles de claus mostrant les seves respectives claus públiques. Les claus privades dels usuaris $gsk[i]$ seran entregades en el moment del registre de cada usuari.

2.5. Registre de l'usuari

$\mathcal{U}$ es registra a la TTP de grup $\mathcal{M}_\mathcal{G}$ i rep la parella de claus de grup (gpk,$gsk[i]$). A continuació, $\mathcal{U}$ també es registra a la TTP de pagament $\mathcal{M}_\mathcal{C}$; l'usuari té un pseudònim essent una exponenciació precalculada $y_\mathcal{U} = \alpha^{x_\mathcal{U}} \pmod p$ atès un cert valor aleatori $x_\mathcal{U} \overset{R}{\leftarrow} \mathbb{Z}_q$; únicament la informació $y_\mathcal{U}$ serà mostrada a la TTP de pagament $\mathcal{M}_\mathcal{C}$, i autenticada mitjançant Schnorr demostrant el coneixement de $x_\mathcal{U}$ sense donar-lo a conèixer. D'aquesta manera, es preserva l'anonimat de l'usuari, però podria ser revocat per $\mathcal{M}_\mathcal{G}$ si fos necessari.

Prova de Schnorr

La prova de coneixement nul de Schnorr permet demostrar el coneixement d'un valor sense necessitat de revelar-lo.

2.6. Entrada en el sistema

Quan l'usuari $\mathcal{U}$ entra correctament en el sistema rep un tiquet electrònic d'entrada t_{in}. A la sortida del sistema $\mathcal{U}$ ha de mostrar el tiquet electrònic perquè es pugui calcular la quantitat que ha de pagar. A continuació es descriu el protocol d'entrada.

1) L'usuari $\mathcal{U}$ realitza les accions dels passos següents:

a) genera un valor aleatori $r \overset{R}{\leftarrow} \mathbb{Z}_q$;

b) calcula $\delta_1 = \alpha^r \pmod p$;

c) calcula $\delta_2 = PK_{\mathcal{M}_C}(y_{\mathcal{U}})$ (el criptosistema utilitzat és probabilístic);

d) genera un *timestamp* τ_0;

e) composa $\sigma = (\delta_1,\delta_2,\tau_0)$, i ho signa amb la seva clau de grup $\sigma^* = (\sigma,Sign_{\mathcal{G}}(\sigma))$;

f) envia σ^* a $\mathcal{P}_{\mathcal{S}}$;

2) El proveïdor de serveis origen $\mathcal{P}_{\mathcal{S}}$ realitza els passos següents:

a) verifica la signatura de σ^*, és a dir, comprova si es tracta d'un usuari vàlid del grup i a més que no es tracti d'un usuari que hagi estat revocat anteriorment;

b) genera un *timestamp* τ_1;

c) emplena amb la informació el bitllet d'entrada al sistema $t_{in} = (Sn,Ps,\tau_1,\tau_v,\sigma^*)$ i calcula la signatura ${t_{in}}^* = (t_{in},Sign_{\mathcal{P}_{\mathcal{S}}}(t_{in}))$;

d) envia ${t_{in}}^*$ a $\mathcal{U}$;

3) $\mathcal{U}$ verifica la signatura de ${t_{in}}^*$ i el seu contingut;

2.7. Sortida del sistema

Quan l'usuari surt del sistema, envia el tiquet electrònic d'entrada t_{in} a l'estació de sortida $\mathcal{P}_{\mathcal{D}}$, i es calcula la quantitat que ha de pagar. Si $\mathcal{U}$ actua honestament rep un bitllet de sortida t_{out} com a rebut del pagament.

1) $\mathcal{U}$ envia ${t_{in}}^*$ a $\mathcal{P}_{\mathcal{D}}$;

2) El proveïdor de serveis destinació $\mathcal{P}_{\mathcal{D}}$ realitza els passos següents:

a) verifica la signatura de ${t_{in}}^*$ calculada per $\mathcal{P}_{\mathcal{S}}$;

b) comprova que $t_{in}.Sn$ no hagi estat utilitzat amb anterioritat;

c) verifica que no hagi expirat el temps de validessa τ_v;

d) obté un *timestamp* τ_2;

e) calcula la quantitat a pagar depenent del punt d'entrada ($t_{in}.Ps$), de sortida (Pd) i dels seus respectius temps ($t_{in}.\tau_1$ i τ_2): $a = f(t_{in}.Ps,Pd,t_{in}.\tau_1,\tau_2)$;

f) genera un repte $c \overset{R}{\leftarrow} \mathbb{Z}_q$;

g) composa $\beta = (t_{in}{}^*, a, c, \tau_2, Pd)$, i ho signa $\beta^* = (\beta, Sign_{\mathcal{P}_\mathcal{D}}(\beta))$;

h) envia β^* a $\mathcal{U}$;

3) $\mathcal{U}$ realitza els passos següents:

a) verifica la signatura de β^* calculada per $\mathcal{P}_\mathcal{D}$;

b) calcula $\omega = r + c \cdot x_\mathcal{U} \pmod q$;

c) genera un *timestamp* τ_3;

d) composa i xifra $\gamma = PK_{\mathcal{M}_\mathcal{C}}(\omega, t_{in}.Sn, \tau_3, a)$;

e) composa $\theta = (\beta^*, \gamma, \tau_3)$ i ho signa amb la signatura de grup: $\theta^* = (\theta, Sign_\mathcal{G}(\theta))$;

f) envia θ^* a $\mathcal{P}_\mathcal{D}$;

4) $\mathcal{P}_\mathcal{D}$ verifica la signatura de θ^* i el seu contingut, i l'envia a la TTP de pagament $\mathcal{M}_\mathcal{C}$;

5) $\mathcal{M}_\mathcal{C}$ realitza els passos següents:

a) verifica la signatura de θ^*;

b) descifra γ para obtener la prueba de Schnorr para ser verificada ω;

c) desencripta $\sigma.\delta_2$ per a obtenir el pseudónim a qui carregar el cost del viatge $y_\mathcal{U}$;

d) verifica la identitat de $\mathcal{U}$ mitjançant Schnorr: $\alpha^\omega \stackrel{?}{=} \delta_1 \cdot (y_\mathcal{U})^c$;

e) si és correcte, carrega el compte amb l'import a a l' usuari a qui apunta $y_\mathcal{U}$;

f) genera un *timestamp* τ_4;

g) genera $ok = (t_{in}.Sn, a, \tau_4)$ i ho signa $ok^* = (ok, Sign_{\mathcal{M}_\mathcal{C}}(ok))$;

h) envia ok^* a $\mathcal{P}_\mathcal{D}$;

6) $\mathcal{P}_\mathcal{D}$ realitza els passos següents:

a) genera un *timestamp* τ_5;

b) composa $t_{out} = (\theta^*, a, \tau_5)$ i ho signa $t_{out}{}^* = (t_{out}, Sign_{\mathcal{P}_\mathcal{D}}(t_{out}))$;

c) envia $t_{out}{}^*$ a $\mathcal{U}$ i permet sortir del sistema a l'usuari;

2.8. Resultat

Aquest exemple mostra com confeccionar tiquets d'entrada i sortida en un sistema de tiquets electrònics amb tarificació automàtica. Partint d'aquest exemple, s'ha de tenir en compte que els continguts dels tiquets s'hauran d'adaptar a cada sistema, en funció de les prestacions i el servei ofert. Examinant l'exemple també s'observa que les fases estan íntimament relacionades amb els requeriments de privacitat del sistema. Sistemes amb diferents prestacions respecte a l'anonimat poden constar de fases diferents i utilitzar mecanismes d'anonimat amb altres tècniques. L'exemple del sistema descrit es pot utilitzar per a veure el tractament dels requeriments, analitzant la seva presència o absència.

Exercicis d'autoavaluació

1. Avalueu alguns tíquets físics i observeu quins tipus d'informació dels estudiats inclou.
S'utilitzen mesures de seguretat? Quines?
Quins requeriments dels llistats a l'apartat 1.4 es podrien aplicar en cada cas?

2. Quines creieu que són les diferències principals i les semblances entre els sistemes de pagament electrònic i els sistemes de tiquets electrònics?

3. Quines relacions hi ha entre els requeriments exposats en el mòdul?
Idntifiqueu les incompatibilitats i els conjunts de propietats que s'han de satisfer de manera conjunta. Feu les suposicions o utilitzeu escenaris concrets si és necessari.

Bibliografia

Arnau Vives-Guasch, Magdalena Payeras-Capellà, Macià Mut Puigserver, Jordi Castellà-Roca, Josep Lluís Ferrer-Gomila. *A Secure E-Ticketing Scheme for Mobile Devices with Near Field Communication (NFC) That Includes Exculpability and Reusability*, IEICE Transactions, volume 95-D, 2012.

Andreu Pere Isern-Deyà, Arnau Vives-Guasch, Macià Mut Puigserver, Magdalena Payeras-Capellà, Jordi Castellà-Roca. *A Secure Automatic Fare Collection System for Time-Based or Distance-Based Services with Revocable Anonymity for Users*, The Computer Journal, 2012.

Macià Mut Puigserver, M. Magdalena Payeras-Capellà, Josep-Lluís Ferrer-Gomila, Arnau Vives-Guasch, Jordi Castellà-Roca. *A survey of electronic ticketing applied to transport*, Computers & Security, 2012.