Tiques electrónicos

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

PID_00202399

UOC
Universitat Oberta de Catalunya

Índice

Introducción

Un tique electrónico es un contrato, en formato digital, entre un usuario y un proveedor. Permite reducir tanto los costes económicos como el tiempo de uso de muchos servicios, como son la navegación aérea o el transporte público.

Por tanto, la seguridad del tique se debe garantizar completamente, así como la privacidad de sus usuarios. El uso de tiques electrónicos podría originar distintos abusos de la privacidad de los usuarios, ya que a menudo los tiques electrónicos no presentan la característica de anonimato. En este caso se puede hacer un seguimiento de los movimientos de los usuarios para crear perfiles de sus actividades.

La proliferación de dispositivos móviles con altas prestaciones permite asociar el uso de los tiques electrónicos a este tipo de dispositivos. Las soluciones propuestas, por tanto, se deben adaptar a los requisitos y a las características de los nuevos dispositivos.

Estos sistemas deben garantizar la seguridad frente a los intentos de fraude por parte de los usuarios, al mismo tiempo que garanticen su privacidad. El proveedor de servicio no debe poder identificar a los usuarios, y diferentes usos del mismo usuario no se deben poder vincular entre sí. Finalmente, en caso de que un usuario intente actuar fraudulentamente, su anonimato debería ser revocado.

Determinados servicios no tienen un precio preestablecido. El precio que haya que pagar se determinará en función del uso que se hace del servicio, dependiendo por ejemplo del tiempo de uso. Estos sistemas se denominan sistemas de tarificación automática. Los tiques utilizados en estos sistemas deberán funcionar de manera diferente a los habituales y el cobro no se hará en el momento de emisión del tique. En este caso se hablará de tiques de entrada y de tiques de salida del servicio, contendrán informaciones diferentes y serán gestionados por protocolos específicos, diferentes de los protocolos utilizados en el caso general.

Los sistemas de tarificación automática (*automatic fare collection, AFC*) calculan la tasa que se debe pagar en función del uso que se hace del sistema, dependiendo este del punto/instante de acceso al servicio y el correspondiente punto/instante de salida.

Estos sistemas, utilizados en aplicaciones como aparcamientos o peajes, se basan habitualmente en el uso de papel. Como en el caso general de los tiques

electrónicos, la progresiva introducción de las tecnologías de la información y de la comunicación permiten la reducción del coste del servicio al mismo tiempo que mejoran el control de las infraestructuras.

1. Tiques electrónicos: definición, propiedades y requisitos

1.1. Introducción a los tiques electrónicos

El uso de las tecnologías de la información (TI) en las operaciones del día a día está creciendo de manera importante. El turismo es un ejemplo de sector afectado por el uso de las TI. Hoy en día es posible obtener toda la información sobre un determinado destino, buscar vuelos a este lugar, reservar una habitación de hotel o conseguir entradas para un parque o museo y así sucesivamente. Además, todas estas acciones se pueden realizar de una manera muy cómoda: se pueden realizar en casa y no hay restricciones temporales.

Los usuarios de los tiques en papel se deben desplazar a la entidad emisora de billetes para recibirlos, lo que provoca una pérdida de tiempo, o han de gestionar un dispositivo capaz de imprimir el billete. Por ejemplo, un ejecutivo que vaya el aeropuerto en taxi podría ser capaz de comprar el billete utilizando su teléfono móvil, pero el billete no se podría imprimir de manera sencilla en este escenario. Estas limitaciones obligan a pasar por la agencia en cuestión o a comprar el billete en otro sitio. La manipulación del billete de papel tiene costes para los usuarios y las empresas, que se podrían reducir. Aunque los costes de la emisión de un billete de papel podría ser baja, cuando existe una gran cantidad de billetes emitidos se convierte en un coste que hay que tener en cuenta. Los costes de administración también deben ser tenidos en cuenta.

El grado de importancia de estos cambios depende del uso de las TI en manos de las empresas. En general, el uso de las TI es heterogéneo a causa de las diferencias entre los sectores y también entre el potencial de cada empresa. Las grandes empresas prefieren explotar las TI con la finalidad de obtener un mayor rendimiento mediante el uso de los últimos avances tecnológicos. En caso contrario, las empresas pequeñas invierten menos en TI. En el caso de pequeñas empresas relacionadas entre ellas, el uso de las TI depende del uso que estas empresas pequeñas podría hacer.

El uso de billetes electrónicos en una empresa afecta a la propia empresa y al usuario. Las fases de adquisición y de recepción podrían ser totalmente electrónicas, pero requieren que el proceso de validación deba ser también electrónico. Los usuarios llevan billetes mientras se están moviendo y los validan para acceder al servicio. Por ello, el usuario debe tener un dispositivo adecuado para gestionar y utilizar billetes electrónicos. Los dispositivos móviles (como teléfonos móviles, PDA o teléfonos inteligentes) son considerados los dispositivos mejor situados entre los sistemas de taquillaje electrónico. Estos

dispositivos ofrecen capacidades de cómputo y almacenaje adecuado y una rica variedad en las últimas tecnologías de comunicación sin cable (Bluetooth, NFC y Wi-Fi). Todas estas características están disponibles en un dispositivo de medida reducida, lo que proporciona movilidad y flexibilidad a estos sistemas.

Además de las consideraciones anteriores, la aplicación real de estos sistemas de billetes electrónicos depende de su seguridad, a causa de la facilidad de copia de los contenidos electrónicos y de cuestiones relacionadas con la privacidad. Los billetes electrónicos deben ser tanto o incluso más seguros que los billetes de papel.

El transporte es uno de los principales sectores que utilizan billetes en su actividad normal. Los billetes de papel están siendo progresivamente sustituidos por billetes electrónicos, lo que reduce el gasto de papel y hace todo el proceso más dinámico.

Los tiques electrónicos se pueden utilizar en múltiples servicios de transporte. Por ejemplo, el servicio de reservas AMBUS de la República Checa permite la compra de tiques SMS: el usuario recibe el tique en su teléfono móvil y muestra el mensaje al inspector cuando le es solicitado.

Las compañías de vuelo son líderes mundiales en el uso de billetes electrónicos y TI emergentes. La International Air Transport Association (IATA) inició en el 2004 un programa para introducir el uso de billetes electrónicos, que se llevó a cabo completamente en el año 2008. Esta iniciativa elimina los costes de impresión de tiques, mantenimiento y distribución y representa tres millones de dólares de ahorro al año, pues el precio de procesar un billete electrónico cuesta un dólar frente a los diez dólares por cada billete en papel.

Otro ejemplo de esto podría ser el caso de las tarjetas de embarque electrónicas. Vodafone y Spanair hicieron una prueba en el año 2007, en la que los pasajeros recibían su tarjeta de embarque electrónica en sus teléfonos móviles. Otras compañías, como Air Canada o Continental, han seguido la misma dirección y ofrecen servicios similares a sus clientes.

Estos ejemplos demuestran dos hechos importantes:

1) Existe una progresiva introducción de los billetes electrónicos en diferentes tipos de servicios.

2) Los teléfonos móviles son la principal plataforma de billetes electrónicos.

A continuación se enumeran algunas ventajas del uso de billetes electrónicos en los teléfonos móviles:

- Los clientes pueden reservar en cualquier parte, incluso sin una impresora.
- Las entradas se pueden comprar y utilizar inmediatamente.
- La comunicación entre los clientes y la empresa es más fácil y más rápida.
- La compañía ahorra recursos y acelera el proceso de gestión.

Finalmente, aunque el transporte es el escenario más representativo del uso de billetes electrónicos, los billetes electrónicos también se pueden utilizar en otros campos. El sector del ocio tiene algunos ejemplos de sistemas de taquillaje electrónico. Se pueden utilizar para eventos deportivos o cualquier otro tipo de espectáculo en vivo. Por ejemplo, los seguidores del Leeds United pueden reservar un partido y después recibir un SMS con la confirmación de la reserva junto a información adicional, como la de sus asientos asignados.

1.2. Definición de tique electrónico

El billete o tique electrónico es un contrato entre un usuario y un proveedor de servicios. Si el usuario demuestra su posesión del billete, obtiene el derecho a utilizar el servicio bajo los términos y las condiciones establecidas.

Habitualmente, se requiere la validación del tique para poder utilizar el servicio. Dependiendo de las condiciones del tique este puede ser validado una vez, un número predefinido de veces o de manera ilimitada durante un periodo de tiempo (hasta una fecha límite).

Los tiques deben incluir elementos para garantizar la seguridad del sistema y la privacidad de los usuarios. Los requisitos relacionados con la seguridad y la privacidad pueden ser diferentes en distintas aplicaciones de los tiques electrónicos. En algunos casos, la seguridad será un factor crítico, como en el caso de impedir la falsificación en los billetes de transporte aéreo. En otras aplicaciones, los requisitos de seguridad, como el anonimato de los usuarios, son indispensables.

A continuación se definen los principales requisitos de seguridad, las fases de los sistemas de tiques electrónicos y los participantes involucrados en el sistema. También se definen determinados campos de información incluidos en los tiques electrónicos.

1.3. Tiques electrónicos: actores, fases, servicios e información

Esta sección incluye un análisis de los sistemas de tiques electrónicos, primero definiendo a los participantes involucrados, las fases relacionadas y la información que debería formar parte de los tiques electrónicos.

1.3.1. Actores

A continuación se describen los participantes que intervienen en el proceso de creación y utilización de los tiques electrónicos.

- **Usuario**: recibe el tique electrónico después de su creación y lo presenta para su validación y poder tener acceso al servicio.
- **Emisor**: emite el tique electrónico y lo entrega al usuario. Los tiques electrónicos pueden ser emitidos tanto por los propios proveedores del servicio como por intermediarios.
- **Proveedores de servicio**: reciben los tiques electrónicos de los usuarios y se encargan de su validación. Si esta validación es satisfactoria, proporciona al usuario acceso al servicio asociado al tique electrónico.

Estos son los participantes principales y habituales de los sistemas de tiques electrónicos, pero determinados sistemas incorporan a otros participantes. Si se utiliza criptografía de clave pública en el sistema, se requerirán los servicios de una autoridad de certificación. En otros casos, el sistema de tiques electrónicos se basa en el uso de tarjetas inteligentes (*smart-cards*). En este caso también se incluirá en el sistema al emisor de tarjetas. Otros posibles actores son: agentes de usuario, proveedor de servicio de acceso a red, proveedores de servicios de pago, bancos, emisores de tarjetas de crédito, etc.

1.3.2. Fases

En la mayoría de los sistemas propuestos, los autores determinan tres fases principales:

- Pago del tique electrónico
- Emisión
- Validación

Pese a esta aparente uniformidad, estas fases no siempre se definen de la misma manera. Algunos autores agrupan las fases de pago y emisión, convirtiendo sistemas de tres fases en sistemas de solo dos fases.

Otras propuestas añaden una fase previa de registro donde los usuarios deben ser identificados y autenticados para obtener permiso para acceder al sistema. Puntualmente, junto a las fases enumeradas anteriormente, se considera una fase de inicio de servicio y otra de finalización de servicio.

Estas variaciones en la definición de las fases de los sistemas de tiques electrónicos se deben a las grandes diferencias existentes entre las propuestas, acentuadas por las diferencias en los servicios accesibles por cada tipo de tiques electrónicos.

1.3.3. Servicios

Hasta ahora, las propuestas existentes de sistemas de tiques electrónicos ofrecen acceso a diferentes tipos de servicios. Se puede destacar, entre los sistemas existentes, que el área de servicios predominante es la del transporte. Y entre estas pueden encontrarse algunas específicas para sistemas de transporte ferroviario, para transporte aéreo, autobuses o metro.

También se pueden encontrar sistemas que utilizan tiques electrónicos para la gestión de peajes. En este caso el funcionamiento del sistema es ligeramente diferente, ya que los usuarios pagan por el servicio una vez que este ha sido utilizado y la cantidad involucrada en el pago depende de algún factor relacionado con el uso. El pago se realiza en el momento de finalización del uso del servicio utilizando algún sistema de pago electrónico. Un caso parecido es el de los taxis. La diferencia se encuentra en el factor de tarificación, en un caso es la distancia recorrida y en otro el tiempo de uso. Estos servicios se adecuan a los sistemas de tarificación automática (AFC). La tarificación automática no se limita a los sistemas de transporte, también se pueden encontrar aplicaciones en otros tipos de servicios, como en el uso de instalaciones.

1.3.4. Información

De manera similar a los tiques basados en papel, los tiques electrónicos deben incluir un conjunto de informaciones básicas para su funcionamiento. Algunos contenidos pueden ser específicos del servicio, otros se relacionan con la seguridad del sistema.

A continuación, esta sección describe los campos de información que se incluyen en los tiques electrónicos.

- **Número de serie**
  Número de identificación único para cada tique electrónico.

- **Emisor**
  Identidad de la entidad que es responsable de la emisión de los tiques electrónicos. El emisor puede ser el propio proveedor de servicio o un intermediario.

- **Proveedor de servicio**
  Identidad de la entidad que ofrece el servicio al usuario.

- **Usuario**
  Información sobre el propietario del tique electrónico. Si este campo aparece en el tique e incorpora la identidad del usuario o algún dato identificativo, la propiedad de anonimato no se podría dar.

- **Servicio**

  Descripción del contrato de servicio.

- **Términos y condiciones del contrato**

  Descripción, dentro del mismo tique electrónico, de los términos y condiciones de contratación. Alternativamente se puede incluir un enlace a un lugar externo donde se encuentren los términos y las condiciones.

- **Tipos de tique electrónico**

  El tique electrónico incluye un campo donde se indica el tipo de tique.

- **Transferibilidad**

  Si se incorpora este campo, la transferencia del tique electrónico entre usuarios estará permitida.

- **Número de usos**

  En el caso de tiques electrónicos reusables un número predefinido de veces, este campo indicará el número máximo de utilizaciones permitidas con el tique.

- **Destino**

  Campo utilizado en los tiques específicos para el transporte donde se fija el destino.

- **Atributos**

  Otros atributos de un tique electrónico que se deben incorporar en el tique. En función del tipo de servicio los atributos serán de un tipo u otro. Por ejemplo, en un tique que representa la entrada a un teatro se incluirá un atributo que indique el número de asiento.

- **Tiempo de validez**

  El tiempo de validez se determina por dos fechas, la de inicio del servicio y la de caducidad.

- **Fecha de emisión**

  Marca temporal del instante de emisión del tique electrónico. El tiempo de validez puede estar determinado por el valor de este campo y el contenido de los términos y las condiciones del contrato.

- **Firma digital del emisor**

  El emisor dispone de un par de claves de un criptosistema de clave pública que le permite firmar digitalmente el tique electrónico.

- **Identificación del dispositivo**

  Campo que especifica, si es el caso, la vinculación del tique electrónico a un dispositivo físico específico.

1.4. Requisitos de los tiques electrónicos

Los requisitos de los tiques electrónicos se pueden clasificar en dos categorías. Por un lado, los requisitos relacionados con la seguridad y, por otro, los funcionales. Algunos de los requisitos son difíciles de clasificar, ya que pueden tener impacto en las dos categorías: funcionalidad y seguridad.

1.4.1. Requisitos de seguridad

- **Definición 1: Integridad**

  Ha de ser posible determinar si un tique electrónico ha sido manipulado y modificado respecto al tique emitido por el correspondiente emisor autorizado.

  Todos los participantes deben ser capaces de verificar si un tique electrónico ha sido manipulado o, lo que es lo mismo, todos los tiques deben estar emitidos por un emisor autorizado.

- **Definición 2: Autenticidad**

  Los usuarios deben ser capaces de verificar que se ha emitido el tique electrónico.

  La obtención de este requisito permitirá a los usuarios comprobar si el emisor es el que está autorizado.

- **Definición 3: No rechazo de origen**

  El usuario que genera o envía un mensaje no debe ser capaz de denegar su emisión o generación una vez realizada.

  Este requisito puede ser útil en diferentes etapas, pero es particularmente importante en relación con la emisión de tiques electrónicos válidos: el emisor no debe ser capaz de denegar haber emitido aquel tique electrónico, así como su contenido específico. Observad que, de hecho, este requisito incluye los requisitos de autenticidad e integridad: si el usuario no puede negar haber emitido un tique electrónico significa que se puede verificar

que él ha emitido el tique (autenticidad) y que nadie ha modificado el contenido del tique electrónico (integridad). A veces será necesario que el usuario que ha solicitado el tique electrónico no sea capaz de negar su solicitud.

- **Definición 4: No rechazo de recepción**

> El usuario que recibe un mensaje no debe ser capaz de denegar su recepción.

Este requisito también puede ser útil en diferentes etapas en los sistemas de tiques electrónicos. Por ejemplo, un usuario que haya solicitado y recibido un tique no debe ser capaz de negar que lo ha recibido. Otro ejemplo es el caso de un proveedor que ha recibido un tique electrónico a cambio de un servicio; el proveedor no debe ser capaz de negar la recepción del tique electrónico.

- **Definición 5: Infalsificabilidad**

> Solo los usuarios autorizados pueden emitir tiques electrónicos válidos.

En otras palabras, no debe ser posible crear tiques electrónicos y hacerlos pasar por tiques electrónicos auténticos, como si hubiesen sido creados por un usuario autorizado. Este requisito está directamente relacionado con el requisito de no rechazo de origen, y por tanto, con los requisitos de integridad y autenticidad.

- **Definición 6: Equidad**

> Al final de un intercambio entre dos o más partes, o bien cada una de las partes ha recibido los objetos esperados o bien ninguna lo ha hecho. Por tanto, ninguna se encuentra en una situación privilegiada.

Este requisito está estrechamente relacionado con el de no rechazo, pero va un paso más allá, dado que no solo busca asegurar que las partes no puedan negar *a posteriori* haber participado en la transacción, sino que también quiere el compromiso de las partes con una transacción determinada, a través de la equidad. Con el compromiso establecido se trata de una transacción que compromete a todas las partes o a ninguna. Este re-

quisito puede ser útil en varios procesos relacionados con la gestión de los tiques electrónicos.

– **Emisión**. Si el usuario consumidor paga el precio del tique electrónico, debería recibir del emisor un tique electrónico válido, y viceversa, si el usuario consumidor recibe un tique electrónico válido, debe pagar el precio correspondiente o, dependiendo del sistema, proporcionar una prueba de que ha recibido el tique electrónico. Puede haber excepciones al caso general, como en el caso de donaciones, tiques gratuitos, etc.

– **Uso**. Si el usuario consumidor da un tique electrónico válido al proveedor de servicio, el proveedor de servicio debe dar acceso al servicio vinculado, y viceversa.

– **Compensación**. Si el proveedor de servicio dispone de un tique electrónico válido (recibo de un usuario) deberá recibir, si es aplicable en el caso concreto, la compensación correspondiente (típicamente económica). Si el proveedor de servicio ha recibido esta compensación, debe proporcionar una prueba de que la ha recibido.

Por tanto, los sistemas de gestión de tiques electrónicos deben utilizar protocolos de intercambio equitativo y conseguir algunas de las propiedades relacionadas con estos protocolos. Deberán implementarse intercambios equitativos de valores (tique electrónico a cambio de pago, servicio a cambio de tique, etc.) e incluir las propiedades de equidad, *abuse-freeness*, asincronía, verificabilidad de la TTP, etc.

- **Definición 7: No reutilización o sobreutilización**

> Los tiques electrónicos se pueden utilizar las veces acordadas en la contratación entre el emisor y el usuario consumidor.

Los tiques electrónicos no reutilizables solo se pueden utilizar una única vez; por tanto, después de su validación no tienen más utilidad y no se debe permitir que el usuario intente defraudar presentando el mismo tique electrónico en una validación posterior. Los tiques electrónicos reusables se pueden utilizar tantas veces como se haya acordado en el momento de su compra y emisión. No debe permitirse su validación cuando ya se ha llegado al número máximo de usos.

Finalmente, algunos tiques electrónicos se pueden utilizar de manera ilimitada durante un determinado periodo de tiempo (consultad la propiedad de reusabilidad).

Los mecanismos para controlar la reutilización pueden afectar al requisito de anonimato. La reutilización/sobreutilización se puede prevenir o detectar. Si la reutilización/sobreutilización se detecta en la fase de validación, no se permitirá y por tanto el fraude será prevenido.

Por otro lado, si la reutilización/sobreutilización se detecta *a posteriori*, después de la validación será necesaria una manera de identificar al reutilizador.

Este requisito está íntimamente relacionado con el de unicidad de los tiques basados en papel: estos son documentos únicos. Esto significa que se puede distinguir entre original y copia (aunque algunas copias son difíciles de identificar). Aquí podemos encontrar otro requisito relacionado con la unicidad: la falsificación.

En el mundo electrónico es posible que no tenga sentido hablar de original y copia: son dos cadenas de bits idénticas y por tanto indistinguibles. Cualquier documento electrónico accesible puede ser susceptible de ser duplicado tantas veces como se quiera. Cuando se quiera hablar de copias de documentos electrónicos no usables, se deben utilizar las técnicas adecuadas para conseguir este requisito:

a) Dispositivos resistentes a manipulación. Los dispositivos de este tipo (por ejemplo, las tarjetas inteligentes) previenen que los documentos electrónicos almacenados en el dispositivo sean manipulados. Por tanto, la distribución de documentos con requisito de unicidad es posible utilizando este tipo de dispositivos. En este caso la seguridad del sistema se basa en el hecho de que los costes de manipulación deben ser superiores a los beneficios que el atacante puede obtener. También se deben tener en cuenta tanto la usabilidad como la comodidad de los usuarios a la hora de utilizar el servicio.

b) Algunas entidades efectúan un seguimiento de los tiques electrónicos utilizados de manera centralizada. Aunque de esta manera no se puede garantizar la unicidad del documento (tique electrónico), sí que se puede garantizar la unicidad de su uso, es decir, que sea utilizado una única vez.

En relación con el momento en el que la entidad controladora conoce que se está haciendo un intento de reutilización se pueden distinguir dos tipos de técnicas: prevención (el intento de reutilización es detectado y no permitido, típicamente en una transacción en línea con la entidad controladora) y detección *a posteriori* (en este caso se realiza la reutilización y después se detecta en alguna fase del protocolo).

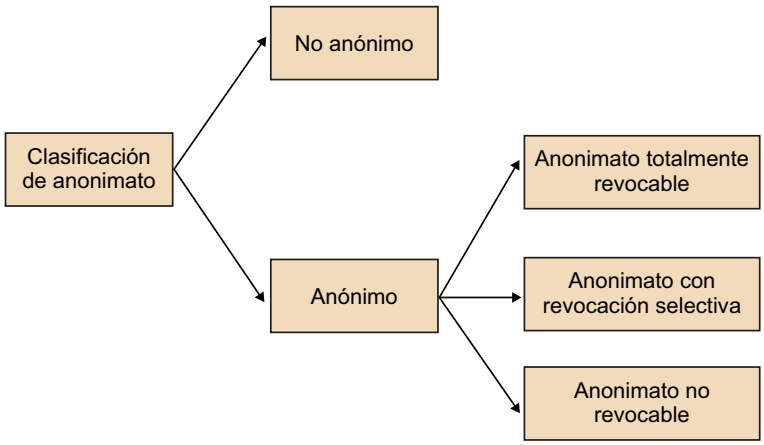
Cualquiera que sea la técnica utilizada solo se debe permitir la utilización de una copia válida del tique electrónico.

- **Definición 8: Tiques electrónicos identificados.**

> La identidad del propietario del tique electrónico debe poder ser verificada.

No todos los tiques basados en papel presentan los mismos requisitos en relación con el anonimato; por tanto, hay que distinguir distintos escenarios posibles para los tiques electrónicos. El primer tipo es el de los tiques electrónicos no anónimos, donde el servicio requiere la identificación y la autenticación del usuario. Esto implica que la identidad debe encontrarse dentro del tique electrónico de una manera u otra para que el proveedor del servicio pueda verificar que el usuario está autorizado a gastar el tique electrónico. Este es el caso de los billetes de avión. En la etapa de embarque el personal auxiliar de la compañía de vuelo debe ser capaz de verificar que la identidad del viajero es la misma que la identidad contenida en el tique electrónico.

Clasificación de las propuestas por tipo de anonimato



- **Definición 9: Anonimato totalmente revocable.**

> El anonimato de los usuarios se puede revocar, revelando su identidad. Las condiciones que permiten la revocación no son selectivas, sino que todos los usuarios pueden sufrir la revocación con independencia de su comportamiento.

La identidad de los usuarios está incluida de una manera determinada (en forma de pseudónimo, identidad real, etc.) en los tiques electrónicos. Normalmente solo un conjunto reducido de actores están capacitados para revocar el anonimato, y solo deberían hacerlo en caso de detectar una reutilización durante el proceso de validación. Esto implica que el tique

podría ser utilizado más veces de las deseadas. Para los tiques electrónicos identificados así no es un problema: se conoce la identidad del reutilizador y por tanto se pueden llevar a cabo acciones apropiadas para su penalización. En cambio, en los tiques electrónicos anónimos el anonimato debe ser revocable para identificar a los infractores reutilizadores. Obviamente, los usuarios honestos deberían permanecer anónimos o, al menos, deberían poder demostrar su honestidad.

- **Definición 10: Anonimato con revocación selectiva**

  La identidad de los usuarios fraudulentos, y solo de los fraudulentos, propietarios de tiques electrónicos inicialmente anónimos puede ser revelada.

Este requisito es bastante parecido al anterior, pero es más restrictivo: solo los usuarios deshonestos pueden perder su anonimato. Desde el punto de vista de la privacidad, este requisito es mejor que el anterior (anonimato totalmente revocable) y también se puede considerar mejor que el siguiente (anonimato no revocable). El problema es que puede necesitar soluciones técnicas más complejas.

- **Definición 11: Tiques electrónicos anónimos**

  El usuario de un tique electrónico es anónimo y será anónimo en cualquier circunstancia.

Algunos tiques basados en papel permiten que el usuario sea anónimo y no deba mostrar su identidad ni al emisor, ni al validador ni al proveedor de servicio. Sería lógico que los tiques electrónicos asociados a los mismos servicios mantuviesen esta propiedad. Este requisito se relaciona con el tique electrónico, con la manera de hacer la emisión y con el modo de utilizarlo. El anonimato se mantiene durante todo el ciclo de vida del tique electrónico.

No obstante, dependiendo del método de pago utilizado, el usuario podría ser identificado en esta fase. En cualquier caso, el usuario consumidor debe ser capaz de gastar el tique electrónico sin ninguna identificación. Ni siquiera la confabulación entre el emisor y el proveedor de servicio debe ser capaz de romper el anonimato de los consumidores. Algunos servicios requieren tiques electrónicos con esta propiedad y en ningún caso debe ser posible identificar al usuario.

- **Definición 12: Exculpabilidad**

  El usuario consumidor de un servicio debe ser capaz de demostrar que ha validado el tique electrónico antes de hacer uso del servicio.
  Además, el proveedor de servicio no puede acusar falsamente a un usuario consumidor honesto de haber utilizado previamente el tique electrónico.

  Este requisito ha sido propuesto recientemente en Vives-Guasch y otros (2012) para tiques electrónicos. Un usuario honesto que ha validado un tique electrónico debe disponer de pruebas que le permitan demostrar este hecho. Presentando estas pruebas evitará que el proveedor de servicio lo pueda acusar falsamente.

- **Definición 13: Reusabilidad**

  El tique electrónico puede ser creado con la intención de que pueda ser utilizado más de una vez.

  Habitualmente un tique electrónico puede ser utilizado solo una vez. Es el caso de los tiques electrónicos no reusables. En los tiques no reusables los intentos de realizar un segundo uso con el mismo tique electrónico se consideraría reutilización.

  Si el tique electrónico presenta la propiedad de reusabilidad, podrá ser utilizado varias veces sin que eso represente una reutilización. El número de usos que se permita hacer del tique electrónico dependerá del tipo de reutilización. La reutilización con un número de usos prefijado se presenta en servicios como algunos casos de transporte público urbano, donde un abono permite realizar un número prefijado de viajes. El contador asociado al abono disminuye en cada viaje. El segundo tipo de reutilización no prefija el número de usos, sino que permite un número ilimitado de usos en un periodo determinado. Incluso se pueden encontrar casos donde el mismo tique puede ser utilizado en diferentes servicios (por ejemplo, bus y metro).

  En cualquier caso, la sobreutilización de los tiques electrónicos se debe evitar (prevención o detección). Los tiques electrónicos deben incorporar medidas de seguridad para permitir solo el uso del tique en el periodo indicado o respetar el número de usos máximo.

A veces se habla de reutilización denominándola divisibilidad, entendiendo cada uso del tique electrónico como una división del tique completo.

- **Definición 14: Transferibilidad**

> Un usuario puede transferir de manera segura su tique electrónico a otro usuario para que este último lo utilice.

En muchos casos, los tiques basados en papel se pueden transferir de un usuario a otro. Es el caso de las entradas para espectáculos, billetes de autobús, etc. Obviamente, este no es el caso de los tiques electrónicos identificados (billetes de avión, por ejemplo).

Los usuarios que reciben un tique electrónico mediante una transferencia y no directamente de un emisor autorizado deben ser capaces de verificar que el tique electrónico recibido es válido (no será complicado si el tique electrónico satisface los requisitos de no rechazo, integridad y autenticidad). También deberá poder comprobar que el usuario que le ha transmitido el tique electrónico no lo ha utilizado previamente (ni tampoco los usuarios anteriores). En el caso de regalos o donaciones entre gente que se tiene confianza, no serían necesarias medidas especiales para asegurar que el tique electrónico no ha sido utilizado previamente, y la reutilización será un asunto que resolver personalmente.

Si los tiques electrónicos se revenden (siempre que el servicio permita la reventa), la entidad que paga por recibir la transferencia de un tique electrónico se debe asegurar tanto de que el tique electrónico es válido como de que no haya sido utilizado previamente. Podría ser que el usuario transmisor intentara la reutilización mediante una utilización y una transferencia. Este intento de fraude se debe tratar como los casos estándares de reutilización. Por tanto, en caso de sistemas con anonimato revocable, la revocación se debe aplicar también a este nuevo tipo de fraude.

La transferibilidad implica un intercambio entre dos usuarios consumidores. La equidad puede ser requerida también en este nuevo intercambio.

Teniendo en cuenta la descripción anterior, dos nuevas definiciones de transferibilidad se hacen necesarias.

- **Definición 15: Transferibilidad débil**

> El tique electrónico es transferible pero la reutilización no se puede verificar en la fase de transferencia.

En este caso el tique electrónico puede ser utilizado por un usuario diferente del usuario que ha sido el primer propietario del tique. El receptor del tique electrónico mediante una transferencia no podrá estar seguro de poder utilizar el tique. Podría ser que, en el momento de la recepción del tique, este ya hubiese sido utilizado por el transmisor o que el transmisor hubiese emitido el tique electrónico a varios receptores. Sería en el momento de presentar el tique electrónico para su validación cuando el receptor sabrá si el tique es válido, ya que el proveedor de servicio le indicará si este ya ha sido utilizado. Este inconveniente se puede suavizar si el receptor puede demostrar que el transmisor es quien ha cometido el fraude.

- **Definición 16: Transferibilidad fuerte**

  El tique electrónico es transferible y el receptor puede verificar que el tique recibido podrá ser utilizado.

En este caso el receptor debe poder estar seguro de que podrá utilizar el tique electrónico. Esto implica que el tique no debe haber sido utilizado y también que no se podrá transmitir a otros usuarios.

1.4.2. Requisitos funcionales

Existen otros requisitos que no están directamente relacionados con la seguridad pero que se pueden considerar tan importantes como los descritos previamente.

- **Definición 17: Fecha de caducidad**

  Un tique electrónico solo es válido durante un intervalo de tiempo.

El cumplimiento de este requisito puede ser útil para minimizar la medida de la base de datos que contiene la información de los tiques electrónicos ya utilizados.

- **Definición 18: Verificación fuera de línea**

  La verificación de los tiques electrónicos se puede realizar sin ninguna conexión externa.

En algunas situaciones no será posible contactar con bases de datos externos o terceras partes de confianza para comprobar si los tiques electrónicos son válidos o no. Quizá no será el caso general, pero se debe tener prevista una solución para este problema. Este requisito está íntimamente relacionado con los mecanismos de seguridad utilizados.

- **Definición 19: Verificación en línea**

  La verificación de los tiques electrónicos requiere una conexión persistente con un sistema centralizado de confianza.

  Normalmente la opción fuera de línea es la preferible por razones de coste, posibles cuellos de botella, etc., pero en el mundo digital, donde millones de transacciones mediante tarjeta de crédito se realizan en línea y donde compañías como Google o Facebook trabajan con un poder computacional muy elevado, parece que este argumento no sea válido.

  En términos de seguridad, la verificación en línea es mejor por el tratamiento de la reutilización o sobreutilización.

- **Definición 20: Portabilidad**

  Los tiques electrónicos deben poder ser almacenados en dispositivos móviles.

  Los tiques electrónicos, como los tiques en papel, deben poder ser transportados por los usuarios. No debería ser necesario un ordenador para la gestión de los tiques electrónicos. Teléfonos móviles, teléfonos inteligentes, tarjetas inteligentes, etc., deberán ser capaces de almacenar y procesar tiques electrónicos.

- **Definición 21: Tamaño reducido**

  Los tiques electrónicos deben ser tan pequeños como sea posible.

  Normalmente, los tiques electrónicos se almacenan en dispositivos móviles y a veces estos dispositivos tienen una memoria con importantes limitaciones (como en el caso de las tarjetas). Por estos motivos, los tiques electrónicos deben tener la medida más pequeña posible.

- **Definición 22: Flexibilidad**

  Los tiques electrónicos deben poderse utilizar en múltiples entornos.

  Podemos pensar en muchas aplicaciones diferentes de los tiques electrónicos (billetes de avión, billetes de bus, entradas de conciertos, entradas de museo, etc.). Se puede diseñar un sistema de tiques electrónicos para cada aplicación o se puede adaptar un sistema general de tiques a cada situación. Obviamente, la última solución es preferible para economizar la solución y permitir un mejor análisis de seguridad.

- **Definición 23: Facilidad de uso**

  El aprendizaje de uso de los tiques electrónicos debe ser sencillo.

  Estamos pensando en los tiques electrónicos como solución para el público general (usuarios de tiques en papel y no necesariamente especialistas en el uso de dispositivos electrónicos). Los tiques electrónicos deben ser tan fáciles de utilizar como los tiques basados en papel y sin que impliquen problemas para los usuarios.

- **Definición 24: Eficiencia**

  El proceso de los tiques electrónicos no debe requerir el consumo elevado de recursos.

  Se puede pensar en la eficiencia desde dos puntos de vista. Primero, los terminales móviles pueden tener limitaciones en términos de poder computacional y por tanto las operaciones incluidas en los protocolos, especialmente las operaciones criptográficas, se deben reducir a solo las imprescindibles.

  En segundo lugar, la capacidad de comunicación también puede ser limitada y por tanto el protocolo se debe diseñar teniendo en cuenta esta limitación. Así pues, el retraso debido a la verificación del tique electrónico debe ser razonable en una propuesta de tiques electrónicos.

- **Definición 25: Flexibilidad de pago**

  Los tiques electrónicos deben poderse obtener utilizando sistemas de pago habituales.

  El diseño de un sistema de tiques electrónicos debe tener en cuenta que en muchos casos requerirá el uso de un sistema de pago. Por ello los sistemas de tiques deben permitir el uso de diferentes sistemas de pago para obtener el tique en la fase de emisión.

- **Definición 26: Utilización global**

  Los usuarios consumidores deberían ser capaces de utilizar los tiques electrónicos en cualquiera de los proveedores de servicios autorizados.

  Esta propiedad se opone a la de tiques utilizables selectivamente. En este último caso los tiques solo se pueden utilizar en un proveedor específico.

- **Definición 27: Disponibilidad**

  Los tiques electrónicos deben poder ser utilizados en el momento requerido.

  Este requisito se puede ver como un requisito de seguridad, pero es complicado hacer frente a este problema desde el punto de vista de la seguridad. Podemos estar pensando en ataques de denegación de servicio, situaciones catastróficas o malos funcionamientos temporales. Esto podría significar que los tiques electrónicos no podrían ser validados y podrían causar el retraso en el servicio (concierto, vuelo, etc.). Se debe diseñar un procedimiento para gestionar situaciones de este estilo.

1.5. Sistemas de tiques electrónicos con tarificación automática

Determinados servicios susceptibles de utilizar tiques electrónicos tienen un funcionamiento ligeramente diferente. Se trata de servicios donde el precio de utilización no está prefijado y depende del uso que haga de este el usuario consumidor.

Ejemplos de estos servicios son los peajes que se pagan en las autopistas. En el momento de comenzar a utilizar el servicio los usuarios obtienen un tique pero no pagan por él, ya que en ese momento el precio que pagarán no está todavía determinado. La incorporación de las tecnologías de la información y las comunicaciones (TIC) en los sistemas de peajes permite reducir costes y obtener mejoras en el control de las infraestructuras, como podría ser la monitorización de la densidad de tráfico en tiempo real o la planificación de las infraestructuras en función de los flujos de viajeros.

Pero los sistemas de tarificación automática no se limitan a los peajes. Distintos sistemas de tarificación automática se aplican al transporte público. Se trata de los casos donde el usuario no especifica previamente su destino, sino que la tarifa se calcula en función del lugar por el que se accede al servicio y del lugar por donde se sale del sistema. En este sentido, es necesario habilitar una gestión segura de las entradas (*check-in*) y de las salidas (*check-out*), teniendo en cuenta que los usuarios pagan en función de esta utilización.

Si el sistema identifica a cada usuario y conoce sus movimientos, puede realizar un seguimiento vulnerando su privacidad. Por este motivo, los sistemas de tarificación automática deben incorporar medidas para preservar la privacidad de los usuarios.

La distancia es un factor que puede ser la base para el cálculo de la tarifa que se debe pagar en un sistema de tarificación automática pero no es el único. También se pueden encontrar servicios donde el factor que se ha de tarificar es el tiempo. Es el caso de uso de instalaciones o de servicios de transportes como los taxis.

A la hora de diseñar un sistema de tiques electrónicos con tarificación automática se deben redefinir las fases, ya que ahora habrá una fase de entrada al sistema, en la que se obtendrá el tique electrónico de entrada, y otra fase de salida, donde se realizará el pago y se obtendrá el tique electrónico de salida.

A continuación se describe un sistema de tiques electrónicos donde la tarificación se realiza de manera automática.

2. Descripción de un sistema de tiques electrónicos con tarificación automática

Una vez descritos los sistemas de tiquetaje electrónico, este capítulo pretende mostrar, de manera más práctica, cómo sería un sistema de gestión de tiques electrónicos. Para hacerlo, este capítulo describe, a modo de ejemplo, un sistema de tiques electrónicos con tarificación automática. Con la descripción de este sistema se verán diferentes técnicas que se aplican al sistema para ir consiguiendo algunas de las propiedades descritas con anterioridad. El sistema satisface varios de los requisitos expuestos anteriormente, como el anonimato revocable y la no vinculabilidad. El protocolo presentado es una simplificación del protocolo Isern-Deyà, 2012, dejando de lado algunos aspectos por su sofisticación. El protocolo se diseñó con el objetivo de que los usuarios utilicen sus dispositivos móviles para el acceso al servicio. Como se ha comentado anteriormente, al tratarse de un sistema de tarificación automática, un servicio al que se podría aplicar la propuesta sería un sistema de peajes. Hay que destacar que los usuarios no necesitan obtener una credencial nueva cada vez que realicen un viaje.

A continuación se describe el protocolo que protege el anonimato de los usuarios mediante firmas de grupo. Para hacerlo, se describen los participantes del sistema, las propiedades de seguridad, la información de los billetes de entrada y salida, y las fases del sistema.

Firma de grupo

Método para permitir a un miembro de un grupo firmar un mensaje de tal manera que en la verificación de la firma se pueda determinar que se trata de un miembro válido del grupo pero no se pueda determinar de qué miembro concreto se trata.

2.1. Participantes del sistema

En el sistema descrito participan los actores siguientes:

- Usuario $\mathcal{U}$: accede al sistema de transporte y paga por el servicio recibido a la salida.
- Proveedor de servicios ($\mathcal{P}_S$ es el proveedor de origen, $\mathcal{P}_D$ es el proveedor de destino): estación que controla los tiques electrónicos utilizados por el usuario $\mathcal{U}$.
- TTP de pago $\mathcal{M}_C$: gestiona los pagos de los usuarios cuando estos acaban de utilizar el servicio y realizan la salida del sistema.
- TTP de grupo $\mathcal{M}_G$: gestiona las claves de grupo, las listas de revocación de los usuarios, etc. Tiene potestad de revocar el anonimato de un usuario si este actúa deshonestamente a partir de la firma de grupo de los tiques electrónicos de entrada y salida.

2.2. Información en los tiques electrónicos

Al tratarse de un sistema con tarificación automática, el sistema maneja dos tipos de tiques electrónicos: los de entrada y los de salida. A continuación, se describe la información que tienen los tiques electrónicos de entrada (tabla 1) y de salida (tabla 2), además de mostrar la notación (tabla 3).

Tabla 1. Información del tique electrónico de entrada ($t_{in}{}^*$)

Nombre	Notación	Descripción
Número de serie	Sn	generado por $\mathcal{P}_\mathcal{S}$
Estación de entrada	Ps	identificador de $\mathcal{P}_\mathcal{S}$
Timestamp de entrada	τ_1	marca de tiempo de entrada
Tiempo de validez	τ_v	tiempo para ser verificado
Compromiso de $\mathcal{U}$	σ^*	compromiso del usuario firmado
Firma digital	$Sign_{\mathcal{P}_\mathcal{S}}(t_{in})$	contenido firmado por $\mathcal{P}_\mathcal{S}$

Tabla 2. Información del tique electrónico de salida ($t_{out}{}^*$)

Nombre	Notación	Descripción
Información de validación	θ^*	enviado por $\mathcal{U}$
Tarifa	a	cantidad pagada
Timestamp de pago	τ_5	marca de tiempo del pago
Firma digital	$Sign_{\mathcal{P}_\mathcal{D}}(t_{out})$	contenido firmado por $\mathcal{P}_\mathcal{D}$

Tabla 3. Información de la notación, ordenada por orden de aparición

Nombre	Notación
Clave pública de grupo	gpk
Lista de claves privadas para cada usuario del grupo	$gsk[\,]$
Lista de revocaciones del grupo	$grt[\,]$
Base de exponenciación	α
Número primo	p
Número primo	q
Pseudónimo de $\mathcal{U}$ (para el pago)	$y_\mathcal{U}$
Exponenciación inversa de $y_\mathcal{U}$ (secreta)	$x_\mathcal{U}$
Número aleatorio	r
Exponenciación de r	δ_1
Encriptación probabilística de $y_\mathcal{U}$	δ_2
i-ésima marca de tiempo	τ_i
Firma digital del contenido *content* para la entidad E	$Sign_E(content)$
Tique electrónico de entrada firmado por $\mathcal{P}_\mathcal{S}$	$t_{in}{}^*$
Reto para $\mathcal{U}$ para demostrar la autoría de $y_\mathcal{U}$	c
Reto y tarifa firmados por $\mathcal{P}_\mathcal{D}$ para $\mathcal{U}$	β^*
Respuesta de $\mathcal{U}$ al reto c	ω
Encriptación probabilística de ω	γ
Aceptación del cobro firmada por parte de $\mathcal{M}_\mathcal{C}$	ok^*
Tique electronico de salida firmado por $\mathcal{P}_\mathcal{D}$	$t_{out}{}^*$

2.3. Fases del sistema

Los participantes en el sistema realizarán las acciones descritas en un conjunto de operaciones. En el sistema se definen las fases siguientes:

- Configuración inicial: $\mathcal{M}_\mathcal{G}$ genera todas las claves de grupo, listas de revocación, etc.

- Registro del usuario: $\mathcal{U}$ se registra en $\mathcal{M}_\mathcal{G}$, adquiriendo un par de claves de grupo. También crea una cuenta con $\mathcal{M}_\mathcal{C}$ mediante un pseudónimo que será utilizado solo para los pagos.

- Entrada al sistema: los usuarios entran en su estación origen y generan una firma de grupo que certifica que son usuarios válidos registrados del sistema. Esta firma no revela su identidad. A partir de esta firma reciben un tique electrónico de entrada que deberán mostrar a la salida.

- Salida del sistema: el usuario se autentica otra vez en la estación de destino como usuario válido del grupo y muestra su billete de entrada. El proveedor $\mathcal{P}_\mathcal{D}$ calcula la cantidad que debe pagar el usuario a partir de la tarifa vigente. El usuario acepta el pago y genera la aceptación que se envía a $\mathcal{M}_\mathcal{C}$. A partir de la aceptación $\mathcal{M}_\mathcal{C}$ carga el importe en la cuenta de $\mathcal{U}$. Si todo el proceso es correcto, el usuario recibe un tique electrónico de salida.

2.4. Configuración inicial

Esta fase se ejecuta únicamente una vez para el conjunto de usuarios. $\mathcal{M}_\mathcal{G}$ genera el grupo de la medida establecida, generando como salida (gpk,gsk[ ],grt[ ], α,p,q), siendo gpk la clave pública compartida del grupo, cada clave privada del usuario es $gsk[i]$, la lista de usuarios revocados en el grupo es grt[ ], y (α,p,q) son parámetros públicos, siendo α la base pública de exponenciación, y (p,q) números primos tales que $p = 2q + 1$, cardinales de sus grupos correspondientes $\mathbb{Z}_p$ y $\mathbb{Z}_q$. Además, los proveedores de servicio generarán sus propios pares de claves mostrando sus respectivas claves públicas. Las claves privadas de los usuarios $gsk[i]$ serán entregadas en el momento del registro de cada usuario.

2.5. Registro del usuario

$\mathcal{U}$ se registra en la TTP de grupo $\mathcal{M}_\mathcal{G}$ y recibe el par de claves de grupo (gpk,$gsk[i]$). A continuación, $\mathcal{U}$ también se registra en la TTP de pago $\mathcal{M}_\mathcal{C}$; el usuario tiene un pseudónimo siendo una exponenciación precalculada $y_\mathcal{U} = \alpha^{x_\mathcal{U}} \pmod p$ considerando un cierto valor aleatorio $x_\mathcal{U} \overset{R}{\leftarrow} \mathbb{Z}_q$; únicamente la información $y_\mathcal{U}$ será mostrada a la TTP de pago $\mathcal{M}_\mathcal{C}$, y autenticada mediante Schnorr, demostrando el conocimiento de $x_\mathcal{U}$ sin darlo a conocer. De esta manera, se preserva el anonimato del usuario, pero podría ser revocado por $\mathcal{M}_\mathcal{G}$ si fuese necesario.

Prueba de Schnorr

La prueba de conocimiento nulo de Schnorr permite demostrar el conocimiento de un valor sin necesidad de revelarlo.

2.6. Entrada en el sistema

Cuando el usuario $\mathcal{U}$ entra correctamente en el sistema recibe un tique electrónico de entrada t_{in}. A la salida del sistema $\mathcal{U}$ debe mostrar el tique electrónico para que se pueda calcular la cantidad que debe pagar. A continuación se describe el protocolo de entrada.

1) El usuario $\mathcal{U}$ realiza las acciones de los pasos siguientes:

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

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

c) calcula $\delta_2 = PK_{\mathcal{M}_C}(y_{\mathcal{U}})$ (el criptosistema utilizado es probabilístico);

d) genera un *timestamp* τ_0;

e) compone $\sigma = (\delta_1,\delta_2,\tau_0)$, y lo firma con su clave de grupo $\sigma^* = (\sigma,Sign_{\mathcal{G}}(\sigma))$;

f) envía σ^* a $\mathcal{P}_{\mathcal{S}}$.

2) El proveedor de servicios origen $\mathcal{P}_{\mathcal{S}}$ realiza los pasos siguientes:

a) verifica la firma de σ^*, es decir, comprueba si se trata de un usuario válido del grupo y además que no se trate de un usuario que haya sido revocado anteriormente;

b) genera un *timestamp* τ_1;

c) completa con la información el billete de entrada en el sistema $t_{in} = (Sn,Ps,\tau_1,\tau_v,\sigma^*)$ y calcula la firma ${t_{in}}^* = (t_{in},Sign_{\mathcal{P}_{\mathcal{S}}}(t_{in}))$;

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

3) $\mathcal{U}$ verifica la firma de ${t_{in}}^*$ y su contenido.

2.7. Salida del sistema

Cuando el usuario sale del sistema, envía el tique electrónico de entrada t_{in} a la estación de salida $\mathcal{P}_{\mathcal{D}}$, y se calcula la cantidad que debe pagar. Si $\mathcal{U}$ actúa honestamente, recibe un billete de salida t_{out} como recibo del pago.

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

2) El proveedor de servicios destino $\mathcal{P}_{\mathcal{D}}$ realiza los pasos siguientes:

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

b) comprueba que $t_{in}.Sn$ no haya sido utilizado con anterioridad;

c) verifica que no haya expirado el tiempo de validez τ_v;

d) obtiene un *timestamp* τ_2;

e) calcula la cantidad que debe pagar dependiendo del punto de entrada ($t_{in}.Ps$), de salida (Pd) y de sus respectivos tiempos ($t_{in}.\tau_1$ i τ_2): $a = f(t_{in}.Ps,Pd,t_{in}.\tau_1,\tau_2)$;

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

g) compone $\beta = (t_{in}{}^*, a, c, \tau_2, Pd)$, y lo firma $\beta^* = (\beta, Sign_{\mathcal{P}_\mathcal{D}}(\beta))$;

h) envía β^* a $\mathcal{U}$.

3) $\mathcal{U}$ realiza los pasos siguientes:

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

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

c) genera un *timestamp* τ_3;

d) compone y cifra $\gamma = PK_{\mathcal{M}_\mathcal{C}}(\omega, t_{in}.Sn, \tau_3, a)$;

e) compone $\theta = (\beta^*, \gamma, \tau_3)$ y lo firma con la firma de grupo: $\theta^* = (\theta, Sign_\mathcal{G}(\theta))$;

f) envía θ^* a $\mathcal{P}_\mathcal{D}$.

4) $\mathcal{P}_\mathcal{D}$ verifica la firma de θ^* y su contenido, y lo envía a la TTP de pago $\mathcal{M}_\mathcal{C}$.

5) $\mathcal{M}_\mathcal{C}$ realiza los pasos siguientes:

a) verifica la firma de θ^*;

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

c) desencripta $\sigma.\delta_2$ para obtener el pseudónimo a quien cargar el coste del viaje $y_\mathcal{U}$;

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

e) si es correcto, carga la cuenta con el importe a al usuario a quien apunta $y_\mathcal{U}$;

f) genera un *timestamp* τ_4;

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

h) envía ok^* a $\mathcal{P}_\mathcal{D}$.

6) $\mathcal{P}_\mathcal{D}$ realiza los pasos siguientes:

a) genera un *timestamp* τ_5;

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

c) envía $t_{out}{}^*$ a $\mathcal{U}$ y permite salir del sistema al usuario.

2.8. Resultado

Este ejemplo muestra cómo confeccionar tiques de entrada y salida en un sistema de tiques electrónicos con tarificación automática. Partiendo de este ejemplo, se debe tener en cuenta que los contenidos de los tiques deberán adaptarse a cada sistema, en función de las prestaciones y el servicio ofrecido. Examinando el ejemplo también se observa que las fases están íntimamente relacionadas con los requisitos de privacidad del sistema. Sistemas con diferentes prestaciones respecto al anonimato pueden constar de fases diferentes y utilizar mecanismos de anonimato con otras técnicas. El ejemplo del sistema descrito se puede utilizar para ver el trato de los requisitos, analizando su presencia o ausencia.

Ejercicios de autoevaluación

1. Evaluad algunos tiques físicos y observad qué tipos de información de los estudiados incluyen.
¿Se utilizan medidas de seguridad? ¿Cuáles?
¿Qué requisitos de los listados en el apartado 1.4 se podrían aplicar en cada caso?

2. ¿Cuáles creéis que son las diferencias y las semejanzas principales entre los sistemas de pago electrónico y los sistemas de tiques electrónicos?

3. ¿Qué relaciones existen entre los requisitos expuestos en el módulo?
Identificad las incompatibilidades y los conjuntos de propiedades que se deben satisfacer de manera conjunta. Haced las suposiciones o utilizad escenarios concretos si es necesario.

Bibliografía

Vives Guasch, A.; Payeras Capellà, M.; Mut Puigserver, M.; Castellà Roca, J.; Ferrer Gomila, J. Ll. (2012). "A Secure E-Ticketing Scheme for Mobile Devices with Near Field Communication (NFC) That Includes Exculpability and Reusability". *IEICE Transactions (vol. 95-D)*.

Isern Deyà, A. P.; Vives Guasch, A.; Mut Puigserver, M.; Payeras Capellà, M.; Castellà Roca, J. (2012). "A Secure Automatic Fare Collection System for Time-Based or Distance-Based Services with Revocable Anonymity for Users". *The Computer Journal*.

Mut Puigserver, M.; Payeras Capellà, M.; Ferrer Gomila, J. Ll.; Vives Guasch, A.; Castellà Roca, J. (2012). "A survey of electronic ticketing applied to transport". *Computers & Security*.