

## Tarjetas de Crédito Anónimas para garantizar la privacidad de los ciudadanos

Justo A. Carracedo Gallardo<sup>1</sup>, Jose-David Carracedo Verde<sup>2</sup>

<sup>1</sup> Departamento de Ingeniería y Arquitecturas Telemáticas (Diatel). Universidad Politécnica de Madrid (UPM)  
Ctra. de Valencia Km 7, 28031 Madrid  
carracedo@diatel.upm.es

<sup>2</sup> Departamento de Ciencia Política y de la Administración III. Universidad Complutense de Madrid (UCM)  
Campus de Somosaguas, 2823 Madrid  
jdcarracedo@proyectos.diatel.upm.es

**Resumen.** El uso de tarjetas de crédito convencionales conlleva, aparte de problemas de falta de seguridad y fiabilidad, un peligro cierto relacionado con la vigilancia de las acciones y hábitos de los ciudadanos. En el artículo se recoge cómo este problema de control ha sido estudiado y analizado minuciosamente por los investigadores sociales. También se describe la solución que para los problemas de seguridad aporta el uso de tarjetas inteligentes para configurar tarjetas de crédito, aunque se comprueba que no solucionan, sino que acrecientan, los riesgos asociados a las prácticas de vigilancia. Para neutralizar esta amenaza se propone el uso de Tarjetas de Crédito Anónimas, ACCs, mediante las cuales se consigue el anonimato de los compradores de forma análoga a lo que se produce utilizando dinero en metálico. Por último se presenta una propuesta concreta de ACC: las entidades de comunicación que intervienen y los intercambios de información que garantizan el anonimato de las transacciones realizadas.

### 1 Comercio y Privacidad en la Sociedad de la Información

En los últimos años se ha producido un cambio tecnológico que ha tenido en las llamadas Tecnologías de la Información y las Comunicaciones (TIC), uno de sus más claros exponentes. En concreto, ha sido espectacular el aumento de las Comunicaciones Mediante Computadores (CMC). El uso del ordenador tiene un crecimiento exponencial y su penetración prosigue extendiéndose cada vez a más esferas sociales, ya sean relacionadas con el mundo comercial o con el tiempo de ocio.

Para la realización de compras de bienes o servicios a través de sistemas telemáticos (ya sea mediante pago “presencial” ante el comerciante, o de forma remota a través de Internet) es interesante el uso de **dinero digital**. Como tal, podemos entender cualquier intercambio de piezas de información, en formato electrónico, que ofrezca

garantías al vendedor de que obtendrá, a través de una entidad bancaria, una cantidad de dinero equivalente al precio de la mercancía que acaba de ceder.

En un mundo globalizado, subsumido en la Sociedad de la Información, el uso de dinero en metálico resulta a veces incómodo y sujeto a múltiples limitaciones. No obstante, es necesario resaltar que el dinero en metálico es un viejo mecanismo que permite mantener el anonimato del comprador. El vendedor tiene una garantía razonable de que el comprador está en posesión de un recurso que le permite llevar a cabo una determinada transacción comercial, siendo habitualmente desconocida la identidad del cliente. El banco puede conservar un registro de todas las cantidades de dinero que hemos sacado de la cuenta corriente, pero no puede saber en qué hemos gastado ese dinero

Por otra parte, el uso de tarjetas de crédito convencionales es cómodo y eficaz, pero permite que se creen registros en los que se relacione qué compramos, cuándo y dónde. El uso de **tarjetas inteligentes** para configurar tarjetas de crédito o tarjetas de débito<sup>1</sup> no sólo no resuelve este problema sino que lo magnifica, debido a que, según se prevé, cada vez más actividades de la vida diaria serán realizadas con este tipo de tarjetas, pudiendo darse la situación de que muchísimas de nuestras actividades, desde que nos levantamos hasta que nos acostemos, estén grabadas en registros informáticos, con el enorme peligro que ello conlleva de pérdida de **privacidad**.

En algunas publicaciones en español se traduce la palabra inglesa *privacy* por *intimidación*. A nuestro entender, la idea de *intimidación* está más relacionada con la “zona espiritual íntima y reservada de una persona o grupo” como la define el muy conservador Diccionario de la Real Academia. Aquí se ha optado por traducir “*privacy*” por el neologismo **privacidad** (no recogido en el diccionario de la Academia), resaltando su carácter de derecho ciudadano a mantener protegido aquello que afecta a comportamientos sociales que sólo incumben a una persona o un grupo reducido de ellas. Podríamos, por tanto, considerar que la privacidad es la extensión de la intimidación a aspectos más formales y públicos relacionados con las sociedades modernas y sus dinámicas de mercantilización.

Con frecuencia, principalmente en la literatura técnica procedente de países de habla inglesa, se tiende a considerar *confidencialidad* como casi sinónimo de *privacidad* (confusión inexistente en la literatura socio-política, donde sí está suficientemente distinguido). El Servicio de *Confidencialidad de los datos (Data Confidentiality)* proporciona la protección adecuada para evitar que los datos sean revelados, accidental o deliberadamente, a un usuario no autorizado. Es decir, garantiza que los datos tan sólo van a ser *entendibles* por el destinatario o destinatarios del mensaje.

Si bien es cierto que en multitud de casos la *confidencialidad* es fundamental para la obtención de la *privacidad*, no deben confundirse, ya que, el *uso coordinado* de los distintos servicios y políticas de seguridad es el que proporciona, en su conjunto y

---

<sup>1</sup> Por tarjeta de débito se entiende aquella en la que el banco deduce de la cuenta corriente la cantidad equivalente a la compra en el mismo momento en que ésta se produce. Para la problemática social que aquí se aborda, esta distinción es poco relevante, por lo que en lo sucesivo cuando se haga referencia a los requisitos de privacidad exigidos a las *tarjetas de crédito*, deberá entenderse que ello afecta también a este otro tipo de tarjetas.

dependiendo de cada caso, la necesaria privacidad en las operaciones que realizan los ciudadanos a través de redes telemáticas.

De hecho, en el caso de los mecanismos de pago a través de sistemas telemáticos, como en muchos otros casos, es necesaria la inclusión del *Servicio de Anonimato* para obtener la privacidad. Este servicio de seguridad es requerido en situaciones en las cuales es conveniente y necesario mantener oculta la identidad de la persona que protagoniza una determinada operación telemática.

Algunos sectores de la población temen que, inevitablemente, la informatización de la mayoría de las actividades de comunicación de los ciudadanos desembocará en una merma de su privacidad y de sus derechos. Por contra, podemos afirmar que la adecuada implantación de servicios de seguridad, no sólo garantiza los derechos ya existentes, sino que permite expandir y mejorar dichos derechos. Para ello, consideramos necesario que, además de realizar los trabajos de ingeniería correspondientes, se hagan análisis sociológicos para determinar las necesidades de los usuarios y la viabilidad de los sistemas.

Los autores de la presente ponencia se encuentran comprometidos en una línea de investigación que pretende la indagación, desarrollo e implementación de sistemas que contribuyan a la mejora de los derechos ciudadanos y minimicen los efectos negativos que pueden tener sobre ellos la implantación de la Sociedad de la Información y maximizar sus ventajas [1] [2].

En el campo concreto de los medios de pago, consideramos que sería necesario que el uso de las tarjetas de crédito estuviera dotado no sólo de confidencialidad, sino además protegido con servicios de anonimato, de forma que el banco sepa cuanto dinero se ha gastado el cliente, pero no dónde ni en qué, y el vendedor tenga certeza de que cobra el importe, pero no tenga capacidad para saber de quién. Este tipo de comportamiento sería el que se correspondería con un nuevo tipo de tarjetas inteligentes que operasen bajo una infraestructura telemática: las **Tarjetas de Crédito Anónimas** (Anonymous Credit Cards, ACCs).

## 2 Uso de las tarjetas inteligentes como tarjetas de crédito

En la actualidad, se constata que, de forma creciente, un gran número de las operaciones comerciales realizadas por los ciudadanos son llevadas a cabo mediante tarjetas de crédito. El uso masivo de tarjetas de crédito ha alertado a amplios sectores de la sociedad y atraído la atención de muchos investigadores sociales, ya que está siendo sumamente pernicioso para la conservación de la privacidad. Para Castells ha sido “el instrumento a través del cual se han establecido perfiles sobre las vidas de las personas, se han analizado y utilizado para fines comerciales” [3].

Además, desde el punto de vista de la seguridad, las tarjetas de crédito convencionales presentan múltiples deficiencias. En las tarjetas convencionales de banda magnética es relativamente fácil falsificar la autenticación que le es exigida al usuario cuando éste accede a un cajero automático o a una máquina de pago ubicada en un punto de venta. Cuando las tarjetas de crédito son usadas para adquirir bienes a través del teléfono o de Internet, el simple conocimiento del número de la tarjeta y de su

fecha de caducidad suelen ser suficientes para llevar a cabo la operación. Otras veces, el mecanismo de “autenticación” se “refina” y se exige un fax firmado. Obviamente, todos estos mecanismos resultan manifiestamente insuficientes para garantizar que el comprador es realmente el titular de la tarjeta. La estadística sobre el número de fraudes y deficiencias que se producen es mal conocida porque son precisamente las entidades bancarias emisoras de estas tarjetas las primeras interesadas en no informar acerca de la inseguridad de un producto financiero que, a juzgar por la insistencia con que nos lo ofertan, es de gran valor para sus intereses.

Una característica sumamente perniciosa de las tarjetas de crédito convencionales la constituye el hecho de que el banco conoce el PIN del usuario. Este hecho puede dar lugar a problemas cuando un comprador rechaza o niega haber realizado una cierta compra. El banco puede aducir que esa transacción fue realizada usando la identificación personal del usuario, pero éste puede rechazarla argumentando que el secreto de su PIN no ha sido adecuadamente custodiado, o ha sido interceptado en una comunicación debido a las insuficientes medidas de protección establecidas, o, incluso, que el banco está simulando una falsa operación de compra con fines maliciosos. Todo está confuso y revuelto: nadie tiene pruebas contundentes de nada.

Estos problemas, derivados de la simple existencia de un PIN y de la falsa imputación de transacciones, pueden ser resueltos mediante el uso de *tarjetas inteligentes* dotadas de mecanismos criptográficos de clave pública. Una tarjeta inteligente (*smart card* o *IC*, en inglés) es una tarjeta de plástico de aspecto similar a las tarjetas de crédito convencionales, dotada de un circuito integrado (por eso se las ha llamado también *tarjetas chip*) que contiene una CPU o microprocesador, memoria volátil y memoria no volátil. Esta memoria aloja las pequeñas aplicaciones de usuario y un reducido Sistema Operativo, el SCOS o *Smart Card Operating System* también denominado a veces *máscara* o *Smart Mask*.

Utilizando estos componentes y una circuitería adicional, la tarjeta permite guardar datos particulares de cada usuario y datos para la aplicación específica. Dependiendo de la capacidad de la tarjeta, también se pueden almacenar en ella varias claves públicas, certificada o no, e incluso una serie de informaciones asociadas al entorno en el que se use la tarjeta, haciendo que ésta funcione como memoria *caché* de una aplicación o de una serie de aplicaciones.

La tarjeta se comunica con el exterior a través de unos pequeños contactos físicos del Chip que la ponen en contacto con la ULE, *Unidad de Lectura-Escritura* (en inglés, *WRU*, *Writing-Reading Unit*). Algunas tarjetas carecen de contactos y la transmisión se realiza mediante radiofrecuencia. La tarjeta puede llevar a cabo un conjunto limitado de funciones criptográficas y una serie de funciones de comunicación con el exterior a través de la ULE. Estos periféricos son muy simples y de bajo coste, de forma que su instalación en los PCs o terminales de usuarios no presentan relevantes problemas técnicos o económicos. Además, existen ULEs que se pueden insertar en la ranura destinada a los disquetes portátiles, con lo cual se reducen aún más los requisitos de equipamiento necesarios.

Aunque existen varias generaciones de tarjetas inteligentes que han ido resolviendo sucesivamente distintos problemas de seguridad, las que se proponen para ser usadas como tarjetas de crédito inteligente están dotadas de mecanismos criptográficos, tanto de clave secreta como de clave pública (tipo RSA). Garantizan el almacenamiento de

la *clave privada* del usuario de forma segura, ya que las operaciones de cifrado que deban realizarse usando esta clave se llevarán a cabo **dentro de la tarjeta**, garantizando que la clave nunca viaje por la red, ni salga de los estrictos límites de la tarjeta. También pueden almacenar el *certificado* de su *clave pública* y un número de certificados de otros agentes que intervienen en la comunicación.

En algunas configuraciones, la generación del par de claves de cada usuario (privada y pública) se realiza en un centro especializado y autorizado para ello dentro del dominio de seguridad. En este caso, las claves son introducidas en la tarjeta en la fase de personalización, siendo ésta entregada al usuario para su uso y custodia. En ese momento, el centro generador de claves debe borrar la clave privada del usuario para que sea él, y solo él, quien posea esta clave, responsabilizándose (incluso jurídicamente) de todas las operaciones de cifrado que con ella se realicen. Un problema asociado a este método consiste en que el usuario ha de fiarse de los gestores del centro de generación de claves acerca del hecho de que su clave privada ha sido efectivamente borrada, resignándose a no tener una **prueba** robusta de ello.

Frente a esta forma de proceder, es menester hacer notar que para que se puedan resolver problemas similares a los que se dan en las tarjetas de crédito convencionales, es sumamente conveniente que cada usuario, una vez recibida una primera versión de su par de claves (privada y pública) esté facultado para **generar un nuevo par de claves**, almacenando por sus propios medios la clave privada en su tarjeta inteligente y haciendo llegar la clave pública a una Autoridad de Certificación para que genere el correspondiente de certificado. De esta manera, es insoslayable la responsabilidad que el usuario contrae en cuanto al uso y custodia de sus claves, **no existiendo resquicio alguno** que le permita atribuir a terceros una posible firma que haya sido realizada usando su propia clave privada. De igual forma, esa custodia de su clave privada le proporcionan la seguridad de que nadie, ni siquiera el banco, podrá imputarle la realización de transacciones que él o ella no hayan llevado a cabo. Algunas tarjetas inteligentes están capacitadas para generar de por sí un nuevo par de claves, con lo que se refuerzan estas salvaguardas de confinación de la clave privada dentro de la tarjeta.

Existen múltiples iniciativas para la implantación de tarjetas inteligentes con funciones de tarjetas de crédito y de débito. Así, por ejemplo, Visa y MasterCard, en colaboración con otras compañías involucradas en temas de seguridad, han propuesto y especificado el SET (*Secure Electronic Transactions*) que es un muy elaborado conjunto de procedimientos y protocolos que regulan la comunicación entre diversas entidades y agentes telemáticos implicados en la obtención de una autorización para realizar una compra. La arquitectura SET permite operaciones de Comercio Electrónico sin necesidad de que el usuario sea poseedor de una tarjeta inteligente, pero la configuración que aquí nos interesa es aquella en que los clientes (*cardholders*) constituyen entidades comunicantes que en el futuro estarán en posesión de una tarjeta de crédito inteligente a través de la cual podrán realizar operaciones firmadas digitalmente.

Gracias al uso de certificados emitidos por diversas Autoridades de Certificación (CAs), las distintas partes que intervienen en la comunicación adquieren pruebas irrefutables acerca de las transacciones realizadas. La infraestructura de certificación está constituida por un conjunto de CAs organizadas jerárquicamente, que representan a las distintas partes implicadas en la operación de compra: clientes, comerciantes,

bancos y entidades financieras emisoras de tarjetas. Aunque la especificación del SET apareció hace ya algunos años, la complejidad de la arquitectura y la multiplicidad de agentes telemáticos que conlleva hace que su implantación esté resultando más lenta de lo previsto. De forma equivalente, otras compañías también disponen de desarrollos de tarjetas de crédito inteligentes soportadas por Infraestructuras de Clave Pública (PKIs), que también se encuentran en fase de implantación.

### 3 Implicaciones sociales del uso de las tarjetas de crédito y búsqueda de soluciones correctoras

Dentro de las prácticas de vigilancia podemos distinguir dos tipos básicos. La *vigilancia de acumulación*, como aquella que tiene como objetivos el “inocente” acopio y recolección de datos, falto de intencionalidad concreta (aun considerando que el hecho de la acumulación y almacenamiento de datos es per se bastante intencionado). Frente a ésta definiremos *vigilancia de supervisión* como aquella que recolecta los datos persiguiendo objetivos concretos. Dentro de este tipo de vigilancia, por ejemplo, encuadraríamos las informaciones de transacciones bancarias, los datos fiscales, las listas negras de morosos, de trabajadores ‘problemáticos’, etc.

Con la introducción de los ordenadores, ambas prácticas de vigilancia caen bajo la *dataveillance*, término creado por un ingeniero de computadores llamado R. Clarke. Como indica su composición etimológica *data* (datos) y *surveillance* (vigilancia), se utiliza para designar todo tipo de vigilancia que se realice o sustente sobre medios informáticos. La datavigilancia “destaca las modalidades en que la convergencia de las nuevas tecnologías de la información y la comunicación han enfrentado a las sociedades avanzadas con rápidos cambios en la cantidad, cuando no en la calidad, de la vigilancia”[6]. La datavigilancia permite, dada la actual situación, la vigilancia de masas con costes bastante limitados e incluso, como ahora explicaremos, generando beneficio.

Actualmente, en las sociedades modernas observamos un paulatino asentamiento y aplicación de las lógicas de mercado a todos los niveles y, particularmente, en las prácticas de vigilancia. Ya que aparentemente todo es mercado y todo se puede comprar o vender, las prácticas de marketing tienen muy en cuenta la información que pueden aportar unos extensos y exhaustivos sistemas de vigilancia, como son, en el caso que nos ocupa, aquellos basados en las tarjetas de crédito.

En la constatación de este hecho es donde hay que situar el origen de lo que Oscar Gandy llama el *panoptic sort* (la clasificación, el tipo o la marca, **panóptica**<sup>2</sup>). “El tipo *panóptico* es una tecnología de discriminación compleja. Es panóptica en la me-

<sup>2</sup> **Panóptico**: Sistema arquitectónico en forma de círculo con una torre central cuyas paredes eran celosías, ideado por Bentham en el siglo XVIII y diseñado de forma que unos pocos vigilantes pudieran tener un control absoluto, día y noche, de todas las actividades y tareas de los internos sometidos a vigilancia. Posteriormente, Foucault, filósofo francés del 68, teorizó sobre la aplicación social de esta estructura y actualmente es una conceptualización recurrente en los estudios sobre vigilancia, control social y Sociedad de la Información. Son muchos los autores que teorizan sobre la existencia o no, de un *panóptico electrónico*.

dida en que considera **toda** la información sobre el status o conducta individual potencialmente útil para producir elementos de valoración sobre el potencial económico de una persona. Y decimos que es una tecnología discriminatoria porque se usa para clasificar a la gente en categorías construidas sobre estas estimaciones” [4].

Así, el mercado tiene una necesidad de generar evidencias dignas de crédito sobre la identidad de los individuos con los que se pretende hacer negocios. Y aunque en un principio los objetivos de identificación se asociaban a cuestiones de seguridad y protección de intereses, tanto del cliente como del vendedor, actualmente nos encontramos con unos procesos de demanda de identificación que no responden necesariamente a los criterios de seguridad. Por contra, responden al objetivo de aumentar las bases de datos sobre cada consumidor (nombre, dirección, hábitos de consumo, capacidad de endeudamiento, número de teléfono, número de identificación personal, etc.).

En suma, este modelo panóptico abarca no sólo a los sistemas informáticos y de telecomunicaciones que facilitan la recolección, almacenamiento, procesamiento y comparación de la información personal, sino que también incluye las técnicas de análisis que seleccionan objetivos, diferencian, clasifican y segmentan individuos y grupos sobre las bases de los modelos, suposiciones y orientaciones estratégicas que demandan la optimización del beneficio económico y la minimización del riesgo.

Así, haciendo uso de los sistemas telemáticos, se han establecido prácticas cuyos objetivos se centran en *Identificación, clasificación y evaluación*, en los que los ciudadanos son reducidos a la categoría de potenciales consumidores, y su vida diaria y privada es reducida a una variable que es necesario conocer, clasificar y prever. Actualmente, una de las fuentes principales de las que se extrae esta información son las tarjetas de pago, tanto de crédito, como de débito.

La extensión de este tipo de prácticas conlleva cambios cualitativos importantes en la relación entre vigilancia y privacidad. En épocas anteriores cuando “la mayor parte de las informaciones concernientes a una persona estaban conservadas todavía en su domicilio, cada uno era dueño de sus datos personales, y sólo una vigilancia física podía amenazar la vida privada y atentar al derecho de ser ‘dejado en paz, al abrigo de la mirada del otro’ como afirma la Declaración Universal de los Derechos del Hombre”[17]. Sin embargo, el desarrollo de la informática ha cambiado esta perspectiva, ya que el sujeto es juzgado en base a informaciones sobre las que habitualmente no existe el derecho de réplica (generalmente el sujeto es desposeído de la propiedad de esa información) e incluso siendo las más de las veces nada consciente de su existencia.

Las consecuencias perniciosas de este tipo de prácticas de tipo panóptico son múltiples, pudiendo señalar en la evaluación de nuestra potencialidad como consumidores la denegación injusta de créditos: en EEUU cerca del 70% de los informes de crédito contienen errores ‘más o menos graves, de los cuales un tercio son errores graves’; delitos imaginarios o referencias a cuentas bancarias que no pertenecen al sujeto investigado<sup>3</sup>.

---

<sup>3</sup> Encuesta realizada en Estados Unidos. ‘Mistakes Do Happen: Credit Report Errors Mean Consumer Lose’, Grupo de Investigaciones de Interés Público (PIRG), Washington DC, 12 de marzo de 1998.

La sustitución de tarjetas de crédito convencionales por tarjetas inteligentes operando en red, no soluciona en absoluto este problema sino que lo magnifica: el futuro uso masivo de tarjetas inteligentes para gran cantidad de actividades de la vida diaria representa un peligro tanto más acusado cuanto mayor sea el número de situaciones en las que se utilicen. Frente a esta orientación, la inclusión de servicios de anonimato puede representar un conjuro contra la pesadilla de vigilancia y totalitarismo que algunos investigadores sociales advierten en las tendencias actuales [5], [6] y [18].

Algunos investigadores encuadrados en el campo de la criptografía y la seguridad de la información como Chaum [7] y el propio Diffie [8] se han considerado concernidos por el análisis y búsqueda de soluciones ante el enorme problema social de la vigilancia social y de la preservación de la privacidad de los ciudadanos.

Como respuesta a este problema se hace necesario la búsqueda de soluciones que resuelvan este problema. Proponemos que ello se aborde desde un enfoque multidisciplinar: utilizando las técnicas de Seguridad en Redes para la búsqueda de soluciones viables y los métodos de la Sociología para la predeterminación de las condiciones y requisitos que han de cumplir los sistemas, el análisis de las consecuencias de su implantación y la evaluación de su hipotética aceptación por parte de los ciudadanos.

Esta ponencia está en línea con otros trabajos de los autores que tratan de centrarse en los análisis de los problemas desde el punto de vista de los ciudadanos, procurando detectar cuales son sus necesidades y apuntando a los remedios que las satisfagan. Desde esta perspectiva definimos la Seguridad Cívica como el conjunto de algoritmos, mecanismos de seguridad, protocolos, servicios, determinación de riesgos y, en suma, políticas de seguridad y métodos de trabajo que son necesarios usar para establecer comunicaciones seguras sobre redes telemáticas, *teniendo en cuenta las necesidades de la vida diaria de los ciudadanos normales*, permitiéndoles el ejercicio de los derechos cívicos que les son reconocidos en otros ámbitos convencionales de comunicación, mejorando (respecto de esos mismos ámbitos) los niveles de independencia y privacidad actualmente existentes.

La utilización de mecanismos criptográficos avanzados puede servir para la provisión de servicios de anonimato en los que, en determinadas circunstancias, la identidad de la persona que realiza una determinada operación telemática permanezca oculta ante algunos actores presentes en esa operación. Esto es lo que se consigue con las Tarjetas de Crédito Anónimas.

## 4 Tarjetas de Crédito Anónimas (ACCs)

### 4.1 Anonimato en los medios de pago

El dinero metálico siempre es anónimo. Por ello, cualquier proyección digital de los mecanismos de pago debería preservar el anonimato del comprador. Existen muchas propuestas de Comercio Electrónico en las que esta condición no se garantiza, lo cual puede dar lugar, según se ha comentado, a una situación de control social y vigilancia de masas. Para evitar este tipo de escenarios podemos distinguir al menos ocho ca-

racterísticas que sirven para catalogar un sistema anónimo de pago usando dinero digital:

1. **Verificabilidad** (*verifiability*). Todo participante en una transacción monetaria digital debe de ser capaz de verificar el valor del dinero recibido, la entidad financiera emisora y su autenticidad.
2. **Seguridad** (*security*). El dinero digital no puede ser copiado, o rehusado por el mismo comprador. Tanto el comprador como el vendedor tienen serias dificultades para perpetrar un fraude.
3. **Anonimato** (*anonimity*). La identidad del comprador debe de ser protegida. Esta característica ha sido ampliamente discutida en apartados anteriores.
4. **Irrastreabilidad** (*untraceability*). Nadie puede rastrear o detectar la relación entre el consumidor y los bienes adquiridos.
5. **Pago sin conexión** (*off-line payment*). Los protocolos de venta se llevan a cabo entre el consumidor y el comerciante sin necesidad de que el punto de compra establezca una conexión directa con cualquier banco o agencia financiera.
6. **Transferibilidad** (*transferability*). El dinero recibido puede a su vez ser utilizado por el vendedor para realizar él mismo otras compras o transacciones.
7. **Divisibilidad** (*divisibility*). Quien recibe una cantidad de dinero electrónico está capacitado para transferir a terceros el total, o solamente una parte.
8. **Devolución de cambio o vuelto**. Un comprador puede entregar al vendedor una cantidad de dinero superior al valor del bien adquirido y recibir del vendedor una transferencia monetaria correspondiente a la diferencia.

Estas ocho características pueden servir para evaluar las diversas propuestas y alternativas se han venido realizando para abordar esta cuestión. Existen propuestas, claramente insuficientes, que no utilizan mecanismos criptográficos para la implantación de los protocolos. Otras proponen utilizar algoritmos criptográficos clásicos, si bien sus soluciones no proveen servicios de anonimato, cosa que consideramos absolutamente inservible.

Entre las soluciones que sí contemplan el anonimato cabe destacar la propuesta de Chaum y Pedersen [9] sobre dinero digital (*digital cash*), que plantea un modelo “off-line” que incluye la posibilidad de que las monedas sean transferibles entre varios usuarios antes de que lleguen de nuevo al banco, de forma que el proceso sea irrastreable. Otras propuestas [10] plantean sistemas con distintos grados de anonimato, dependiendo de la autenticación empleada. Algunas propuestas, [11] entre otras, recogen la idea de utilizar distintas firmas según sea el valor de la moneda puesta en juego (que ha sido asumida en las propuestas que se presentan en los siguientes apartados) aunque requieren la existencia de cuentas anónimas (de dudosa viabilidad).

Casi no existen referencias dignas de destacar en lo que se refiere a propuestas sobre tarjetas de crédito anónimas, a excepción de la realizada por Low y otros [12], que plantean un modelo en el que participan varios bancos y en el que no se requiere el uso de mecanismos criptográficos especiales. El cliente mantiene una cuenta en un banco C, en la que se controla el saldo pero no las operaciones y otra cuenta anónima,

en otro banco BS<sup>4</sup>, donde se identifica al cliente por un seudónimo P y sí se recogen las operaciones que realiza. La tarjeta de crédito es expedida por BS y mediante la interacción de estos bancos a través de una entidad mediadora, que actúa como un dispositivo anonimizador, se consigue el efecto buscado. El problema es que la legislación de muchos países prohíbe (con razón) la existencia de cuentas anónimas.

## 4.2 Trabajos y experiencias sobre ACCs

Durante los últimos años, los autores de la presente ponencia han estado involucrados en una serie de trabajos exploratorios [13], [1] y [2] sobre las implicaciones sociales y las posibilidades tecnológicas del uso de tarjetas inteligentes para soportar servicios de anonimato. Además, como resultado de diversos trabajos en los que han participado estudiantes (realizando su Proyecto Fin de Carrera) del Departamento de Ingeniería y Arquitecturas Telemáticas de la UPM, se han especificado dos modelos distintos de Tarjeta de Crédito Anónima, ACC, y se han desarrollado demostradores simplificados que permiten evaluar la validez de las soluciones aportadas.

Se ha optado por abordar, al menos en un principio, solamente el tema de las ACCs por tres razones:

- a) El problema de pérdida de privacidad y vigilancia de masas asociado a las tarjetas de crédito ha sido analizado y evaluado de forma exhaustiva por los investigadores sociales como una cuestión de primera magnitud que requiere, cuanto antes, de respuestas correctoras.
- b) El empleo de tarjetas inteligentes resistentes a fraude (*tamper-resistant*), dotadas de capacidad para ejecutar algoritmos criptográficos, facilita enormemente la búsqueda de soluciones técnicas que satisfagan los requisitos exigidos.
- c) Los requisitos exigibles a las ACCs son más fáciles de satisfacer que los asociados al uso de dinero digital a través de la red (que puede ser abordado posteriormente).

En efecto, atendiendo a las ocho características que antes seleccionamos como asociadas al dinero digital anónimo, solamente las cuatro primeras (*verificabilidad, seguridad, anonimato e irrastreabilidad*) son imprescindibles para disponer de una ACC.

Así, en las soluciones abordadas se ha descartado totalmente la característica número 5 (operación *off-line*) porque, además de complicar enormemente los protocolos, consideramos más interesantes los sistemas conectados en red. Además, cabe observar que en el uso actual de tarjetas de crédito convencionales los puntos de ventas están mayoritariamente conectados telemáticamente con las entidades bancarias.

Por tratarse de esquemas en los que el cliente se relaciona sólo con el vendedor y con la entidad financiera, la característica número 6 (*transferibilidad*) no se ha tenido en cuenta, excepto en la operación mediante la cual el vendedor recibe del banco el importe del bien o servicio que ha cedido. En cuanto, a las características 7 y 8 (*divisibilidad y devolución de cambio*) son usadas en alguna de las soluciones sólo como

---

<sup>4</sup> Este banco es denominado “Banco Suizo” en referencia a que es posible abrir allí cuentas anónimas, tan del gusto de tantos dictadores, mafias internacionales y otros delincuentes de cuello blanco.

mecanismos internos de astucia para ocultar operaciones y dificultar la **datavigilancia**, antes que como emulaciones digitales de la devolución de cambio o vuelto que se produce en las operaciones de compra con dinero en metálico. Así una sola operación de compra puede ser enmascarada bajo varias transacciones monetarias entre la tarjeta y el punto de venta, dificultando su rastreabilidad.

Los dos modelos especificados a los que se hacía referencia más arriba, que, para simplificar, denominaremos aquí ACC#1 y ACC#2 respectivamente, comparten muchos elementos comunes, diferenciándose solamente en lo que se refiere al número de agentes telemáticos que han de participar en la comunicación y en la complejidad del protocolo.

Un elemento arquitectural común en ambas propuestas ha sido el considerar la presencia de un agente telemático en los puntos de venta ante el cual un cliente comparece en persona, portando su tarjeta inteligente. Este agente, denominado Punto de Venta Anónimo (PVA<sup>5</sup>) debe poder conectarse con el banco cuando el protocolo lo requiera. Se ha dejado para futuros trabajos el estudio del acceso remoto a estos puntos de venta vía Internet.

En el siguiente apartado se describe muy brevemente el modelo aquí denominado ACC#1( que se corresponde con [14] con ligeras simplificaciones, variaciones, y retoques) en el que la tarjeta puede ser utilizada indistintamente como de crédito o de débito y, en algunas circunstancias, también como tarjeta-monedero<sup>6</sup> anónima. La ACC#2 [15], en cambio, funciona solamente como una tarjeta de crédito con comportamiento global más parecido a las actuales tarjetas de crédito, lo que conlleva una reducción de las operaciones *on line* en el momento de realizar la compra. Otra diferencia entre ambas soluciones es que la opción ACC#1 necesita del concurso de una Tercera Parte de Confianza (TTP) conectada en línea, mientras la ACC#2, no necesita de ese tipo de ayuda. Por contra, en esta última los protocolos son más complicados y las operaciones criptográficas que han de realizarse en la tarjeta son más complejas. Por razones de espacio y de oportunidad (la ACC#2 requiere aún de trabajos de depuración y de evaluación) se ha decidido presentar aquí solamente la ACC#1.

---

<sup>5</sup> En la presente ponencia, para simplificar, se ha optado por recoger solamente en español el nombre y las siglas que se han asignado a los distintos elementos que constituyen el sistema, excepción hecha del término ACC por considerar que éstas son ya unas siglas reconocidas como tales en inglés.

<sup>6</sup> Se suele denominar tarjeta-monedero a aquella que una vez cargada en un cajero automático o dispositivo *ad hoc*, permite ir haciendo uso de ese dinero hasta su finalización.

## 5 Una propuesta de Tarjeta de Crédito Anónima

### 5.2 Algo más sobre la tarjeta inteligente que la soporta

En el apartado 2 se introdujeron, de forma resumida, algunas de las características principales de las tarjetas inteligentes sobre las que se configurarán las ACCs. Añadiremos ahora algunas otras que ayuden a entender mejor su funcionamiento.

Una característica de capital importancia de las tarjetas inteligentes es su robustez ante ataques que pretendan leer o modificar el contenido de su memoria. Están dotadas de mecanismos de protección tanto físicos como lógicos que las protegen contra acciones no autorizadas. Si una tarjeta es extraviada o le ha sido sustraída a su legítimo propietario, no es técnicamente posible leer los datos en ella contenidos o realizar modificación o copia de éstos.

Las protecciones físicas garantizan que aunque la tarjeta sea destruida o violentada físicamente, no sea posible acceder por medios electrónicos al contenido de la memoria del chip. Esta propiedad de defensa antifraude o antifalsificación, que en inglés se denomina *tamper-proof* o *tamper-resistant*, será uno de los pilares en que se apoya la seguridad de la ACC que presentamos. Cuando es emitida, la tarjeta estará adecuadamente personalizada y contendrá el conjunto de claves y de algoritmos que determinan su funcionamiento, y estará homologada de forma que el terminal del sistema en el que se introduzca reconozca si esa tarjeta es válida o no.

La tarjeta inteligente especificada responde básicamente a la estructura y características recogidas en la norma ISO/IEC 7816 [16] sobre la que se han definido nuevos ficheros y nuevas funcionalidades. La estructura lógica de la memoria consiste en un conjunto de ficheros organizados jerárquicamente en forma de árbol en los que se almacenan las claves y los datos necesarios para el funcionamiento global. En cuanto a las protecciones lógicas cabe decir que estas tarjetas tienen posibilidad de autenticar a su propietario bien mediante un PIN o mediante otro tipo de identificadores biométricos, como pueden ser la huella dactilar o la forma del iris del ojo. Además, existen unos niveles de seguridad que regulan el acceso de entidades externas a los distintos ficheros, estableciéndose un intercambio de información en el que entran en juego números aleatorios generados dinámicamente a tal efecto y claves previamente establecidas.

Además de estas características estándar, la ACC presenta otras específicas y diferenciales que se irán presentando en la descripción que sigue. La más novedosa de ellas es que el chip que opere en su interior debe asumir funciones similares a las de las tarjetas de telefonía móvil (denominadas SIM) que operan en sistemas tipo GSM.

### 5.2 Billetes digitales

Para conseguir la no rastreabilidad de las operaciones realizadas se ha optado por incorporar un concepto inherente al dinero en metálico ( y por tanto al dinero digital

que lo emule) que no está presente en la concepción que comúnmente se tiene de las tarjetas de crédito: la utilización de billetes o monedas digitales.

En efecto, supongamos que en una fecha concreta se ha realizado una compra de combustible en una gasolinera por valor de 30,12 Euros. Aunque el sistema garantice, como luego se tratará de demostrar, que la operación es anónima (en el doble sentido de que no se sabe ni quién ha hecho la reserva de dinero ni desde dónde, con lo que el banco desconoce en ese momento incluso la identidad del vendedor de la mercancía), si el banco tiene voluntad de rastrear los apuntes realizados, no sería muy difícil diseñar programas que comparasen reservas de dinero realizadas por el cliente con operaciones de cobro realizadas por parte de los vendedores, llevadas a cabo en horas próximas, con lo cual, una cantidad tan específica como es 30,12 sería fácilmente relacionable con ambas operaciones.

Para neutralizar este riesgo, lo que el comprador va a solicitar del banco son billetes digitales suficientes para pagar el importe de lo que está adquiriendo. Además, como más tarde se detalla, nunca pedirá la cantidad exacta de billetes necesarios para la operación (es decir, no pedirá 20 Euros, más 10 Euros, más 10 céntimos, más 2 céntimos) sino una cantidad redondeada que le permita enmascarar la operación.

Un billete bancario convencional de una moneda de curso legal consta de una cantidad, un número de serie válido, una firma y un diseño material que hagan que sea muy difícil copiarlo o falsificarlo. En teoría sería factible rastrear la circulación de billetes si se anotasen los números de serie, pero, en la práctica, esto es totalmente inviable (recuérdese la solicitud de “billetes antiguos y sin numeración contigua” que hacen los secuestradores en las películas).

De forma análoga, la plasmación digital del billete que se usa en la ACC tiene un identificador con una estructura bien definida, que denominaremos Número de Identificación del Billeto (NIB). El valor monetario del billete está determinado por la clave privada monetaria con que lo haya firmado el banco. En efecto, el banco dispone de un conjunto de tantos pares de claves (pública y privada) como valores de billetes sean puestos en juego. Así, se dispondrá de billetes de 1 Euro, 2 Euros, 5, Euros, etc. y sus correspondientes valores centesimales. Es conveniente anotar que los valores monetarios aquí seleccionados no tienen porqué coincidir con los valores puestos en circulación por el banco central correspondiente, ya que se trata de un simple artificio interno.

Los NIB son generados por una agencia externa que sea de confianza para las distintas partes involucradas en el proceso de compra. Aquí la hemos denominado, a falta de mejor nombre, Agencia de Protección de la Privacidad (**APP**) y actuará como una Tercera Parte de Confianza, TTP, en el proceso. Generará rstras NIBs constituidos por una cabecera específica donde se indique la fecha de caducidad, seguida de un número hexadecimal constituido por de un número suficientemente elevado de bits (100 han sido definidos en una primera aproximación, aunque estos valores podrían aumentarse e incluso estudiar la posibilidad de que el tamaño dependiese de franjas de valores, para adaptar la seguridad al riesgo que conlleva).

Esta lista de NIBs disponibles se la hará llegar la APP al banco (que la guardará ordenada) e irá distribuyendo estos números, bajo demanda y de forma aleatoria, a las ACCs que se los soliciten, marcando como utilizados los que vaya entregando. El tamaño del número debe ser grande para evitar que se agoten durante un determinado

periodo de vigencia, y para que sea muy pequeña la probabilidad de que alguien invente, con fines maliciosos, un número que coincida con el de uno de los NIBs creados. Aunque, como veremos más adelante, el acertar con un NIB válido no le reportaría especial beneficio al presunto estafador, en tanto que engañar al banco con un NIB inexistente sólo reportaría beneficios para el banco y pérdida de dinero para él.

El establecimiento de la APP habría que hacerlo al amparo de la normativa legal existente orientada a la protección de los datos y la privacidad de los usuarios (o la que se crease o modificase para asumir este tipo de demanda de los ciudadanos). En el caso de España, podría constituirse al amparo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD) dirigida a tal fin y concorde con las directivas europeas en esta materia.

### 5.3 Escenario de comunicación

Las entidades de comunicación presentes en el escenario diseñado para llevar a cabo el adecuado funcionamiento de las operaciones con la tarjeta son las siguientes:

1. **Cliente.** Es la persona a cuyo nombre se ha expedido la Tarjeta de Crédito Anónima. Deberá contar con una cuenta corriente en el Banco que sirva de respaldo a las operaciones de compra que se lleven a cabo.
2. **ACC.** Es la tarjeta de crédito propiamente dicha, configurada sobre una tarjeta inteligente. Contiene la clave privada del cliente, las claves públicas monetarias, las claves que regulan el acceso de entidades externas y todos los datos y algoritmos necesarios para la ejecución de los protocolos. Una característica específica y diferencial de la ACC es que el chip que opere en su interior debe asumir, además, funciones similares a las de las tarjetas de telefonía móvil (denominadas SIM) que deberán tener asignado un número telefónico específico como si de un teléfono móvil tipo GSM se tratase.
3. **PVA.** El punto de venta anónimo es el terminal homologado instalado en los puntos de venta donde sea operativa la ACC. Estará dotado de un lector de tarjetas para operar en conjunción con la ACC. Las comunicaciones que establezca con el banco se llevarán a cabo desde la circuitería residente en el PVA pero con la información contenida en la tarjeta, de forma que es la tarjeta la que se conecta con el banco desde el PVA. De esta manera se consigue que el banco no pueda saber desde dónde le está llamando la tarjeta cuando le solicite billetes digitales.

Los dispositivos y programas que gobiernan el almacenamiento de información y las comunicaciones del PVA son también resistentes a fraude (*tamper-resistant*) bien porque aprovechen las funcionalidades de una tarjeta inteligente especialmente diseñada para el Vendedor, bien porque utilicen componentes intrínsecamente seguros como pueden ser microprocesadores especiales que le permitan espacios de almacenamiento de información muy superiores a los que se pueden conseguir con las tarjetas inteligentes. (Este aspecto concreto no ha sido todavía objeto de diseño en los trabajos realizados).

4. **Vendedor.** Es el propietario de la tarjeta inteligente que permite el acceso y gobierno de PVA.

5. **Banco.** Es la entidad que emite la ACC y la entrega al Cliente, la que envía los billetes digitales a la ACC cuando ésta se lo solicita y la que ingresa los fondos correspondientes en la cuenta del Vendedor cuando éste le entrega billetes digitales válidos.
6. **APP.** Es la Agencia de Protección de la Privacidad a que hemos hecho referencia en el epígrafe anterior.

#### 5.4 Comportamiento global del sistema

A continuación se presenta una descripción simplificada de los distintos pasos que conlleva la operación de compra con la ACC. Con objeto de hacer más fácil su entendimiento, se han omitido ciertos detalles de importancia secundaria. Asimismo, en la descripción que sigue se ha omitido la referencia a que todas las informaciones que se intercambian están firmadas por la entidad emisora con objeto de garantizar su autenticidad y su integridad. Una vez concertada la compra y llegado el momento de abonar el importe de la mercancía adquirida, los pasos a seguir pueden resumirse en los siguientes:

- a) El cliente se autentica ante la tarjeta introduciéndola en el PVA.
- b) El Vendedor teclea el importe, que es comunicado por el PVA a la ACC.
- c) La ACC analiza el número de billetes que posee y los NIBs que tiene almacenados y calcula cuantos de estos necesita. Si tiene almacenados, procedentes de una operación anterior, suficiente número de billetes como para poder satisfacer la compra, salta al paso g). Caso contrario averigua cuantos billetes necesita y si tiene suficientes NIBs disponibles.

El algoritmo para calcular los billetes que necesita solicitar al banco es una pieza fundamental del sistema para garantizar el anonimato y la no rastreabilidad. Se ha denominado *Algoritmo de Redondeo Inteligente* y consiste en determinar, contando con el resto que ya tiene, una cantidad de billetes que exceda en algo a la que realmente necesita. De esta forma, cuando el Vendedor ingrese en el Banco los billetes digitales que ha recibido, este importe nunca coincidirá con el solicitado por la ACC, evitando así el cotejo de datos. Además, el disponer de un ligero saldo de billetes almacenados en la tarjeta puede dar lugar a que en operaciones de poco valor no sea necesario establecer comunicación con el Banco.

- d) Si la ACC no tiene suficiente cantidad de NIBs se los solicita a la APP y los almacena en memoria. A continuación realiza ante el banco, apoyándose el PVA, una petición firmada de billetes anónimos, proporcionándole los NIBs suficientes para que sean firmados por el banco con la firma privada monetaria que corresponda a cada valor. Antes de enviarlos les incorpora un factor de opacidad de tal forma que el banco nunca sepa el número de identificación contenido en los NIBs recibidos.
- e) El banco comprueba la disponibilidad de fondos del cliente y realiza una firma ciega sobre los NIBs opacos recibidos, cada uno con la clave privada monetaria que le corresponda. Y anota la operación en la cuenta del Cliente (que se ha autenticado adecuadamente y de forma robusta).

Si el contrato establecido entre el Cliente y el Banco es en forma de débito o pago inmediato, lo descuenta directamente de su cuenta corriente. Si el contrato es en forma de crédito anota la operación, que le será facturada a fin de mes o en la fecha previamente pactada.

El Banco envía a la ACC los billetes con la firma opaca.

Obviamente, si el Cliente no tiene fondos (de uno u otro tipo) el banco rechaza la operación y la venta queda interrumpida.

- f) La ACC, tras verificar que lo recibido se corresponde con su petición (dispone de las correspondientes claves públicas monetarias), almacena los billetes recibidos junto los que ya tuviese almacenados, sin retirarles el factor de opacidad.
- g) La ACC selecciona exactamente los billetes que necesarios para satisfacer el precio de la mercancía que está adquiriendo, les retira el factor de opacidad y se los entrega a Vendedor a través del PVA.
- h) El PVA hace una primera comprobación del formato de los billetes verificando las firmas del banco y comprobando las fechas de caducidad. Comprueba, consultando su base de datos, que esos NIBs no han sido ingresados antes en este PVA. No puede saber si los NIBs son correctos antes de consultarlo con el Banco.
- i) Si las anteriores comprobaciones resultan favorables, el PVA envía al banco una solicitud de ingreso de billetes. Para ello, el PVA accede desde su propia dirección y le entrega al banco los billetes que ha recibido del Comprador.
- j) El Banco verifica la validez de los billetes comprobando que han sido firmados con las claves privadas monetarias correspondientes y que los NIBs no han caducado. Comprueba también que esos NIBs están en la lista de NIBs válidos remitida por la APP y que no han sido usados previamente, y si todo es correcto, los marca como usados con la identidad del Vendedor, y transfiere a su cuenta corriente la cantidad total resultante. A continuación informa al PVA del resultado de la operación.
- k) Si el resultado es favorable, el PVA avisa al Vendedor para que entregue la mercancía al Cliente y le entrega a la ACC un comprobante firmado de la operación, dando por finalizado el proceso.

### 5.5 Posibles fraudes y reclamaciones

La APP podría actuar como árbitro en caso de reclamaciones por desacuerdo con el contenido de los extractos bancarios que puedan recibir tanto el Vendedor como el Cliente. Dada la existencia de piezas de información cifradas y firmadas no resultará difícil organizar los procesos de comprobación correspondientes.

En cuanto al fraude, cabe decir que al ser tanto la tarjeta como el PVA dispositivos “tamper-resistant”, programados conforme a las especificaciones antes descritas, resultará muy difícil practicar las violaciones que se suelen tener en cuenta en estos casos: la duplicación del dinero digital por parte del Cliente o por parte del Vendedor. Una tarjeta o un PVA falso o manipulado sería fácilmente detectable por la otra parte, con lo que se interrumpiría el proceso de compra.

No obstante, aún en el supuesto de que esa manipulación fuese posible y no detectable en primera instancia, pocos resultados favorables podrían obtener los usuarios defraudadores. Si un cliente consiguiese entregar un billete ya usado anteriormente en el mismo PVA que usó la primera vez, éste lo detectaría tras realizar la comprobación en su base de datos. Si ese billete ya usado lo entregase en otro PVA distinto, el proceso prosperaría hasta llegar al Banco que detectaría que había sido ya cobrado por otro comerciante, con la posible punición que eso conllevaría. Si el que consigue enviar al Banco un billete usado es el mismo Vendedor a través de su PVA, el banco detectaría inmediatamente que es él quien está tratando de cometer fraude.

Es evidente que si un usuario le envía al banco un NIB falsificado (eso es muy sencillo porque el banco espera un dato oscurecido y cualquier cosa del tamaño esperado le resulta válida) lo que consigue es que el banco le descuente el dinero y posteriormente no ser capaz de pagar nada con ese billete.

Rizando el rizo, y suponiendo que dos vendedores se pongan de acuerdo en violentar sus sistemas para fastidiar a un comprador, se puede dar el caso de que un Vendedor pase a otro un billete ya usado y que éste lo entregue en el banco: se estaría acusando falsamente al Cliente de haber cometido fraude. Incluso esta alternativa se podría resolver complicando un poco el protocolo.

No obstante, consideramos que estos sistemas están pensados para transacciones corrientes en las que intervienen ciudadanos corrientes, en cuyo ámbito no parece probable que se produzcan situaciones de este tipo. Lo que sí se procura con esta propuesta de ACC es resolver un problema nada imaginario ni fantasioso: la vigilancia de las vidas de los ciudadanos que en la actualidad se lleva a cabo a través de las tarjetas de crédito.

Serán, precisamente, los ciudadanos normales, cuando se percaten de la gravedad del problema de la vigilancia y de la viabilidad de soluciones técnicas que pueden resolver la mayor parte de los problemas detectados, los que exijan la implantación de sistemas con características similares a la ACC aquí presentada.

## Referencias

1. Carracedo J. and Carracedo J.D. *Use of Security Protocols for Privacy and Anonymity Protection in the Internet Communications*. En *Exploring Cyber Society*, Armitage, J. & Roberts J., Editors. University of Northumbria at Newcastle Press, 1999
2. Carracedo Gallardo, J.A. y Carracedo Verde, J.D. *Telemática y Sociología. Apuntes para una Investigación Multidisciplinar: Tarjetas de Crédito Anónimas y Democracia Electrónica*. I Congreso Iberoamericano de Telemática, Cartagena de Indias, Colombia, Agosto de 2001
3. Castells, M. *The information Age. Economic, Society and Culture*. Vol I. Oxford. Blackwell Publishers, 1996-1997
4. Gandy, Oscar, 'Coming to terms with the panopticon sort'. In *Surveillance, Computers and Privacy*, (ed) Lyon D. y Zureik, E. University of Minnesota Press, 1996.
5. Marx, G. T. (1986) *The iron fist in the velvet glove*. En *The Social Fabric*. Short, J. Sage, 1986  
Marx, G.T. *Undercover: Police Surveillance in America*. Berkeley. University of California Press, 1988.

6. Lyon, D. (1994). *The Electronic Eye. The rise of the Surveillance*, Society. Polity, 1994.
7. Chaum, D. *Security Without Identification. Transaction system to make Big Brother obsolete*, Communication of the ACM, v. 28, n. 10, Oct 1985, pp 1030-44., 1985
8. Diffie, W y Landau, S.(1998). *Privacy on the Line. The politics of wiretapping and Encryption*, MIT Press,1998
9. Chaum, D. and Pedersen, T.: *Transferred Cash Grows in Size*, CWL, Netherlands, 1993
10. Bürk, H. and Pfitzmann, A. *Digital Payment Systems Enabling Security and Unoservability*, Karlsruhe Univerdity, 1989
11. Camensch, L., Piveteau, J.M. , Stadler, M.: *An Efficient Electronic Paypent System Protecting Pryvacy*. Computer Security- EXOTERIC'94, Springer-Verlag,1994
12. Low, SH., Maxemchuck, NF and Paul, S.: *Annoymous Credit Cards*, Proceeding of the Second annual ACM Conference on Computer and Communication Security, ACM Press, 1994
13. Carracedo, JD.: *To what extent is the scheme of panopticism useful in the age of global electronic communication to make sense of the concepts of power, discourse and surveillance*, En *Exploring Cyber Society*, Armitage, J.& Roberts J., Editors. University of Northumbria at Newcastle Press, 1999
14. De Diego Toral, J.: *Servicios de Anonimato para redes seguras. Tarjetas de Pago Anónimas*. Proyecto Fin de Carrera. EUIT de Telecomunicación, Universidad Politécnica de Madrid. Abril de 2000
15. Gómez Espansandín, P.: *Servicios de Anonimato para redes seguras. Tarjetas de Crédito Anónimas*. Proyecto Fin de Carrera. EUIT de Telecomunicación, Universidad Politécnica de Madrid. Octubre de 2000.
16. ISO/IEC 7816-3: *Information technology – Identification Cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocols*.
17. O'Neil, M. *Internet como riesgo para la vida privada*. Le Monde Diplomatique. Septiembre-Octubre. Madrid L. Press. 1998.
18. Lyon, D. *Surveillance Society. Monitoring everyday life*. Open University Press. 2001.