SEGURIDAD EN REDES TELEMÁTICAS

Justo Carracedo Gallardo
Universidad Politécnica de Madrid

CAPÍTULO

11

SERVICIOS DE ANONIMATO PARA LA SOCIEDAD DE LA INFORMACIÓN

En anteriores capítulos hemos ido tratando los distintos servicios de seguridad sin entrar a describir las aplicaciones concretas (correo, transferencia de ficheros, servidores de información, etc.) que hacen uso de ellos. El análisis detallado de cada aplicación concreta podrá abordarse apoyándose en el estudio que aquí hemos realizado sobre estos servicios básicos. De forma semejante, en este capítulo se acometerá de forma genérica el estudio de los elementos principales que conforman el servicio de anonimato, haciendo referencia al tipo de aplicaciones que hacen uso de las facilidades que este servicio proporciona.

Consecuentemente, abordaremos en este capítulo la aplicación del anonimato en los medios de pago, en el voto a través de redes telemáticas y, de forma más genérica, en los sistemas que sirven de soporte a la democracia digital. Las aplicaciones emergentes que los soportan están todavía lejos de convertirse en estándares de facto o de jure; por eso abordaremos aquí diversos esquemas genéricos que puedan servir de pauta y comparación para analizar y evaluar las distintas aplicaciones que con el tiempo vayan surgiendo.

Ya en el Capítulo 2 se presentaron las características principales de las tarjetas inteligentes y a lo largo de los distintos capítulos hemos estado haciendo reiterada referencia a sus múltiples aplicaciones y usos. No obstante esto, hemos considerado conveniente hacer una descripción algo más detallada de este tipo de dispositivos en el presente capítulo, ligándolas al estudio del anonimato, debido a que consideramos que las aplicaciones que servirán para el desarrollo de la democracia digital en sus múltiples facetas se apoyarán en gran medida en tarjetas inteligentes, bien sean del mismo tipo que las que están actualmente normalizadas, bien sean resultado del desarrollo de una nueva generación de tarjetas que ofrezcan más posibilidades en sus conexiones externas y mayor capacidad de procesamiento y de memoria.

11.1. CRIPTOGRAFÍA AL SERVICIO DEL ANONIMATO

Ya en el epígrafe 5.6, dentro del apartado «*Otros mecanismos criptográficos*», hicimos referencia a una serie de mecanismos criptográficos que pueden servir de apoyo para conseguir el anonimato en algunas transferencias de información. Solemos denominarlos *mecanismos criptográficos avanzados* porque no se requiere su empleo para la provisión de los servicios de seguridad básicos a los que hemos venido dedicando nuestra atención en los anteriores capítulos.

El hecho de que los utilicemos como soporte de los servicios de anonimato no quiere decir que estos mecanismos sean de uso exclusivo en aplicaciones que proveen este tipo de servicios, sino que pueden también ser utilizados para construir protocolos seguros en otros esquemas de comunicación especiales en donde puedan ser de interés para los fines allí pretendidos. De igual modo, tampoco pretendemos en estos apartados hacer un estudio exhaustivo de todos los mecanismos criptográficos que pueden ser utilizados en la provisión de servicios de anonimato (para lo cual se usan también los mecanismos convencionales antes estudiados), sino que analizaremos solamente aquellos que consideramos más significativos. Fijaremos, por tanto, nuestra atención en tres de ellos:

- *Firma opaca* o *firma a ciegas.*
- *Secreto dividido.*
- *Secreto compartido.*

FIRMA A CIEGAS SIN TERCERA PARTE

La *firma opaca* o *firma a ciegas* (en inglés, *blind signature*) se caracteriza porque la entidad firmante no puede adquirir conocimiento alguno sobre el documento que está firmando. Posteriormente, la firma obtenida podrá ser verificada como válida por el propio firmante o por cualquier entidad que disponga de la información pertinente para ello, pero el firmante no puede establecer ninguna relación con las circunstancias en que realizó la firma.

En este apartado estudiaremos el escenario más sencillo y al mismo tiempo más robusto de firma opaca: aquel en el que solamente intervienen la entidad *A* peticionaria de la firma y la entidad *B* firmante, sin intervención de tercera parte alguna que haga de árbitro o de juez en ese proceso.

Para adquirir una aproximación intuitiva de lo que representa este mecanismo podemos poner un ejemplo de comunicaciones mediante papel * que puede servirnos de ayuda. Podemos suponer que la relación entre ambas entidades es la siguiente:

1. *A* prepara un documento impreso en un papel con la intención de que *B* lo firme. *A* guarda ese documento junto con un trozo de papel carbón en un sobre que cierra adecuadamente y se lo entrega a *B*. De esta forma «oculta» el contenido del documento. En el sobre está impresa una cuadrícula indicando el sitio exacto en el que *B* debe estampar su firma caligráfica.
2. Si *B* acepta lo que se le propone, firma el sobre, por ejemplo con un bolígrafo, de forma que su firma se estampe, mediante el papel carbón copiativo, en el

* En [Schn96] se propone este esquema para explicar los procedimientos que pueden seguirse en la obtención de dinero anónimo.

documento preparado por *A*. *B* ha firmado sin adquirir ningún conocimiento acerca del contenido del documento. *B* devuelve el sobre firmado.

3. *A* abre el sobre, retira el trozo de papel carbón y se queda con el documento original firmado por *B*.

A partir de ese momento *A* puede presentar ese documento firmado ante cualquier otra persona exhibiendo la firma estampada por *B*. En realidad, este esquema sólo funcionaría si se aceptase un documento firmado a través de papel carbón (lo cual es mucho suponer), pero como ejemplo nos puede servir.

Para la plasmación de este mecanismo en el ámbito de los procedimientos criptográficos nos apoyaremos en el esquema inventado por Chaum [Cha83] utilizando el algoritmo de cifrado asimétrico RSA. Como hemos dicho, en este proceso intervienen sólo dos entidades:

a) Entidad peticionaria *A* que dispone de un mensaje *m* que quiere que *B* firme a ciegas.
b) Entidad firmante *B* que realizará la firma. La clave pública de *B* es conocida en el dominio de seguridad donde se lleva a cabo la comunicación:

$$kP_B = (e, n)$$

El procedimiento necesario para que *A* obtenga la firma opaca, por parte de *B*, de un mensaje *m* es el siguiente:

1. *A* genera un valor aleatorio (*k*) que denominaremos *factor de opacidad* y que debe estar comprendido entre 1 y *n*, tal que *k* y *n* sean primos entre sí. Debido a ello, este número *k* posee un inverso, k^{-1}, en el conjunto de números comprendidos entre 1 y *n*. A continuación, la Entidad peticionaria *A* oculta (opaca) el mensaje *m* calculando $x = mk^e \bmod n$ y se lo envía a *B*:

$$A \rightarrow B\text{: } x = mk^e \bmod n$$

2. *B*, recibiendo *x*, no es capaz de conocer el valor de *m*. *B* cifra el mensaje opacado *x* con su clave privada, $kS_B = (d, n)$, obteniendo la firma opaca o firma a ciegas:

$$x^d = (mk^e)^d \bmod n = m^d\, k^{ed} \bmod n = m^d\, k \bmod n$$

A continuación *B* le envía a la entidad peticionaria la firma opaca:

$$B \rightarrow A\text{: } \quad x^d = m^d\, k \bmod n$$

3. *A* «desopaca» el mensaje opacado firmado por *B*, x^d, dividiendo éste por *k* (multiplicándolo por su inverso k^{-1}), obteniendo:

$$s = x^d \cdot k^{-1} \bmod n = m^d\, k\, k^{-1} \bmod n = m^d \bmod n$$

Es decir, *A* obtiene:

$$s = m^d \bmod n = B_S(m)$$

que es el mensaje *m* cifrado con la clave privada de *B*, es decir, lo que podemos llamar la «firma simple» de *B*.

A partir de ese momento, la entidad *A* podrá presentar ese mensaje «firmado» (*m* más *s*) ante cualquier instancia, pudiendo demostrar que la firma la ha realizado

la entidad *B* porque ella y sólo ella es poseedora de la clave privada $kS_B = (d, n)$. Del mismo modo, la entidad *B* tiene que reconocer su autoría aunque no será capaz de relacionar el documento firmado que se le presenta con ninguna circunstancia de tiempo ni de origen que le permita averiguar cuándo y a petición de quién realizó la firma.

Lo que acabamos de describir es el procedimiento que se seguiría caso de que *B* acepte firmar algo que a priori no puede conocer. En el escenario de comunicación en el que se esté proporcionando un servicio de anonimato que utilice este mecanismo de firma opaca será necesario establecer las garantías necesarias para que *B* adquiera la confianza suficiente en que lo que está firmando no perjudica ni su seguridad ni sus derechos. Estas circunstancias serán las que se evalúen cuando se presenten, en epígrafes posteriores, algunos esquemas de voto telemático y de anonimato en los medios de pago.

Conviene darse cuenta de que en este caso la «firma» que obtiene *A* está realizada sobre el mensaje *m* completo y no en base al resumen $h = H(m)$ como es el caso del *mecanismo de firma digital* RSA o DSA.

No obstante, si *m* es muy grande, la entidad *A* podría pasarle a la entidad *B* el resumen *h* del mensaje y obtendría como resultado de desopacar la firma a ciegas:

$$s = B_S(h)$$

que coincide con lo que en los capítulos 5 y 8 hemos denotado como firma *f* en el mecanismo de firma digital RSA. Es decir, en ese caso *A* podría presentar el documento firmado (m, f) como si se tratase de una firma sobre resumen bajo algoritmo de firma RSA.

Existen muchas otras propuestas de algoritmos para la obtención y verificación de firma a ciegas, alguno de los cuales comentaremos en el siguiente apartado. El propio Chaum ha desarrollado otros esquemas y ha registrado las correspondientes patentes. En la página web personal de este autor puede encontrarse información detallada sobre ese asunto.

Si nos ceñimos a un esquema de comportamiento equivalente al que hemos descrito antes, podemos generalizar el procedimiento y utilizar una nomenclatura simplificada.

Para indicar que una entidad ha opacado un documento *m* **para** *B*, podremos denotarlo como:

$$O_B(m)$$

Para indicar que una entidad *B* ha generado una firma a ciegas sobre un documento *m* opacado, podremos denotarlo como:

$$B_{bsig}[O_B(m)]$$

En realidad, esta nomenclatura que proponemos (el subíndice procede de *blind signature*) es algo redundante, porque si lo que se firma es algo opacado ya se sabe que se trata de una firma a ciegas. Para evitar esa redundancia, podríamos haber decidido reflejar la firma ciega simplemente como $B_{sig}[O_B(m)]$. Pero ello tendría el inconveniente de utilizar una nomenclatura confundente, ya que en anteriores capítulos, cuando representábamos $X_{sig}(m)$ nos estábamos refiriendo a la firma *f* obtenida por *X* mediante un *mecanismo de firma digital* RSA o DSA basado en el resumen, $H(m)$, del mensaje. Por todo ello, aun asumiendo la redundancia, emplearemos B_{bsig}

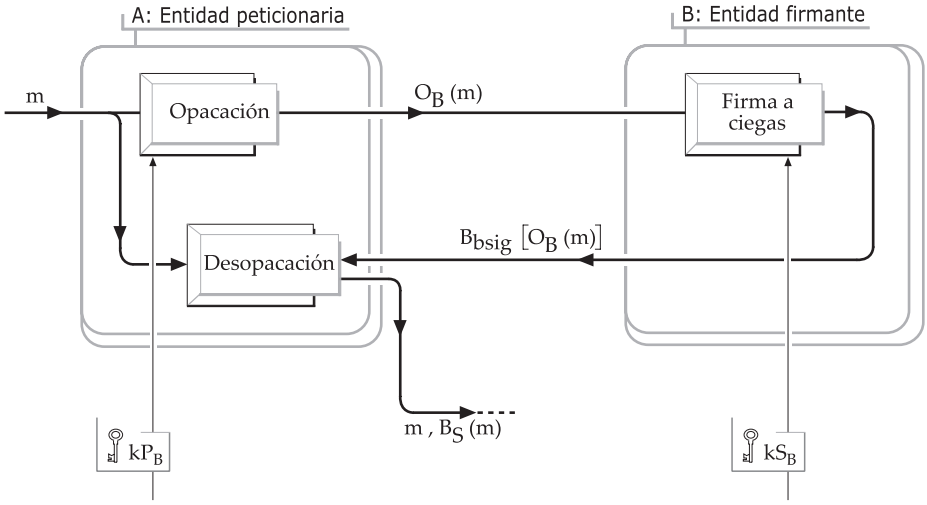

Figura 11.1. Esquema de firma a ciegas.

$[O_B\ (m)]$ para recalcar que lo que se firma es un documento opacado y que el algoritmo de firma será uno **específico** de firma a ciegas.

En la Figura 11.1 se representa este comportamiento generalizado que podemos describir abreviadamente de la manera siguiente:

1. *A* oculta (opaca) el mensaje *m* utilizando la clave pública de *B* (kP_B) calculando $O_B\ (m)$ y se lo envía a la entidad *B*:

$$A \rightarrow B: \quad O_B\ (m)$$

2. *B*, con la información recibida, no es capaz de conocer el valor de *m*. *B* cifra el mensaje opacado utilizando su clave privada (kS_B) mediante un algoritmo específico de firma a ciegas:

$$B_{bsig}\ [O_B\ (m)]$$

A continuación *B* le envía a la entidad peticionaria la firma opaca:

$$B \rightarrow A: \quad B_{bsig}\ [O_B\ (m)]$$

3. *A* «desopaca» el mensaje opacado firmado por *B* obteniendo **una firma** del documento *m* cuyo formato dependerá del algoritmo de firma a ciegas utilizado, pero que, en todo caso, servirá como prueba robusta ante cualquier otra entidad de que *B* ha firmado el documento *m*. Si se trata de un esquema equivalente al de Chaum antes estudiado, será $B_S\ (m)$ el valor de esa firma (situación que se recoge en la Figura 11.1).
4. La entidad *A* está en condiciones de enviar el mensaje firmado, *m,* más la firma de *m* realizada por *B*, a cualquier otra entidad perteneciente a ese dominio de seguridad (en la figura se ha representado este paso como un flujo de datos que se «sale» del marco representado).

Un procedimiento de firma tal que este podría ser vulnerado utilizando el método denominado «ataque mediante texto elegido» que ya comentamos en el Capítulo 5 al hablar de la fortaleza del RSA. Como consecuencia de ello el atacante podría conse-

guir falsificar la firma o incluso obtener la clave privada de *B*. Para contrarrestar este riesgo se han diseñado algunas mejoras y añadidos al algoritmo antes descrito, aunque, como ya hemos dicho, se puede usar este mismo procedimiento simplificado con tal de garantizar que en el escenario de comunicación en el que se esté proporcionando un servicio de anonimato se hagan las cosas de tal forma que se garantice que *B* sólo firme documentos que no perjudiquen su seguridad.

FIRMA A CIEGAS: ALGO MÁS QUE FIRMAR SIN VER

Conviene que fijemos nuestra atención en que la firma a ciegas se realiza por la entidad firmante *a petición de part*e, es decir, esta entidad firma algo que no es capaz de ver y que se le envía para que lo firme. El esquema de comportamiento es, por tanto, totalmente distinto al que se presenta cuando una entidad firma un documento «suyo» con la intención de garantizar su autoría en la generación o distribución de determinada información.

Si pensamos en el comportamiento de una Autoridad de Sellado de Tiempo (Figura 11.2) ante una solicitud que recibe, podemos observar que, según describimos en el epígrafe 7.9, la entidad peticionaria lo que le envía es, además de algunos datos complementarios, el *hash* del mensaje que pretende sellar. La TSA debe generar el sello de tiempo firmando parte de esos datos con el añadido de la fecha y hora en que realiza la operación. El motivo de no mandarle el mensaje *m* completo es evitar que la TSA pueda andar cotilleando acerca del contenido del mensaje, cosa que no es de su incumbencia, porque su único cometido es garantizar que dicho documento existía antes de determinada fecha y hora.

Es decir, en cierto modo, podemos considerar que una TSA firma «bastante a ciegas» la información que recibe, porque no es capaz de conocer el contenido de *m*. Sin embargo, la situación es totalmente diferente a la que se recoge en la Figura 11.1, ya que, a posteriori y en caso de conflicto, la TSA puede reconocer con toda claridad los sellos de tiempo por ella emitidos y relacionarlos con la entidad que realizó la correspondiente petición. Eso no tiene nada que ver con la firma a ciegas.

Veamos, para terminar, otra situación ficticia, representada en la Figura 11.3, en la que se imita el procedimiento de firma a ciegas recogido en la Figura 11.1. En este

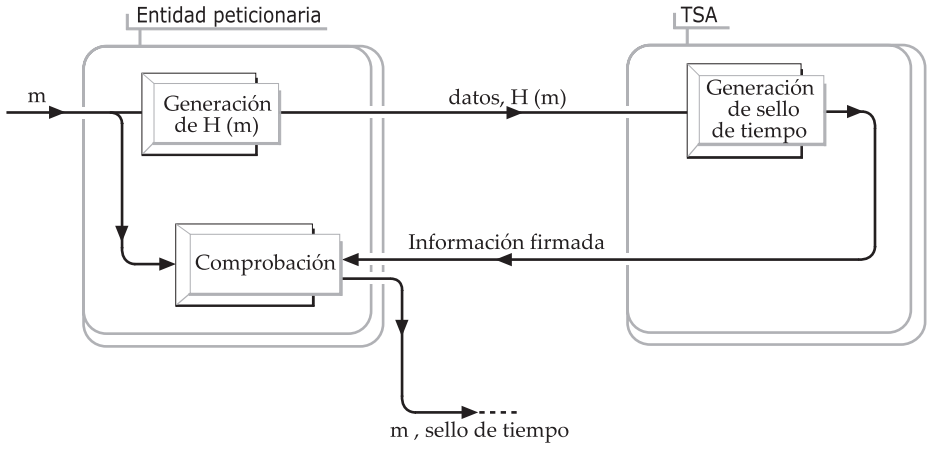

Figura 11.2. Firmado de un sello de tiempo.

caso, lo que la entidad peticionaria envía no es el mensaje opacado sino el resumen H(*m*) del mensaje. Si la entidad *B* acepta cifrar H(*m*) con su clave privada, la entidad peticionaria podría generar y distribuir el mensaje *m* firmado por *B* conforme al mecanismo de firma digital RSA. Una situación como esta puede que tenga algún sentido para implementar un esquema local de generación de firmas con dos módulos internos que cooperan entre sí, pero no se corresponde con las características de la firma a ciegas. Veamos por qué:

Si con este esquema estuviésemos tratando de sustituir a un verdadero esquema de firma a ciegas, apreciaríamos que, ciertamente, la entidad *B* firma H(*m*) sin poder adquirir ningún conocimiento acerca del mensaje *m*, pero en otro momento posterior sí que tendría elementos de reconocimiento. En efecto, si en el esquema de la Figura 11.1 la entidad *B* estuviese firmando a ciegas distintos mensajes que le van enviado de tiempo en tiempo distintas entidades peticionarias, y si además pudiese conocer la identidad de esas entidades (cosa totalmente razonable de cara a que pueda adquirir confianza en la operación que está realizando), podría ir generando un registro donde anotase la entidad peticionaria, la hora y la pieza de información O_B (*m*) que va firmando. Trabajo inútil, porque, posteriormente, cuando se encuentre los documentos firmados y desopacados, no tendrá pista alguna para relacionarlos con las anotaciones que en ese registro ha ido llevando. Por contra, si un registro similar lo llevase la entidad *B* en un esquema como el de la Figura 11.3, sí que podría relacionar sin género de duda los H(*m*) que ha ido firmando con los que aparezcan después en los documentos firmados que *A* distribuya.

Es decir, para que exista firma opaca o firma a ciegas no basta con que la entidad firmante no sea capaz de ver lo que firma en el momento en que lo firma, sino que la entidad firmante no pueda establecer ninguna relación entre el documento firmado que se distribuya y las circunstancias en que se realizó la firma.

FIRMA A CIEGAS ARBITRADA

El esquema de firma a ciegas estudiado en los precedentes apartados es el que se utiliza con mayor frecuencia en las aplicaciones que, en mayor o menor medida,

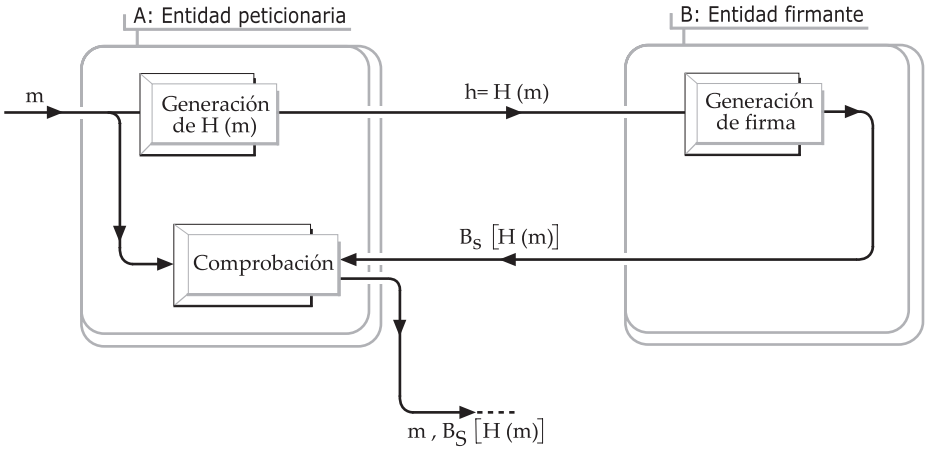

Figura 11.3. Falsa firma a ciegas: firmado del resumen del mensaje.

ofrecen algún servicio de anonimato. No obstante, existen otras propuestas que conviene conocer, siquiera sea de forma genérica, porque puede ser conveniente tenerlas en cuenta en algunos escenarios especiales.

Algunas de estas propuestas incluyen la presencia de una TTP que ayude a la consecución de los objetivos propuestos. En los párrafos que siguen destacaremos dos de estas configuraciones, cada una de las cuales utiliza la TTP con una intencionalidad distinta. El uso de la TTP como ayuda para configurar la firma opaca es una de ellas. La otra consiste en usar la TTP como una especie de juez o árbitro para «romper» lo que puede considerarse excesivo blindaje de la firma a ciegas basada en el esquema de Chaum.

Vayamos por partes y analicemos someramente el primero de esos dos esquemas. En este caso de lo que se trata es de conseguir una firma a ciegas por parte de la entidad firmante aunque para garantizar su validez sea necesario recurrir al dictamen de una TTP en la que confíen los hipotéticos receptores del mensaje firmado. En la Figura 11.4 se representa simplificadamente una posible plasmación de este esquema. El hecho de contar con la TTP, que comparte secretos tanto con la entidad peticionaria como con la entidad firmante, permite emplear algoritmos de generación de firmas menos complejos [1] que los puestos en juego en el esquema con solo dos entidades que analizamos en apartados anteriores.

La fortaleza de los algoritmos utilizados debe ir en consonancia, tanto en este como en otros casos, con el riesgo que represente la vulneración de la protección que ofrecen. No será lo mismo garantizar rotundamente que el voto sea secreto (que no se sepa quién ha emitido determinado voto) que, por ejemplo, mantener el anonimato de un ciudadano que accede a la web de una administración pública para manifestar, de forma anónima, su opinión o su queja sobre tal o cual asunto. En el primer caso, la ruptura del secreto supondría la invalidación total del proceso de votación que se esté realizando, mientras que en el segundo no parece razonablemente probable esperar

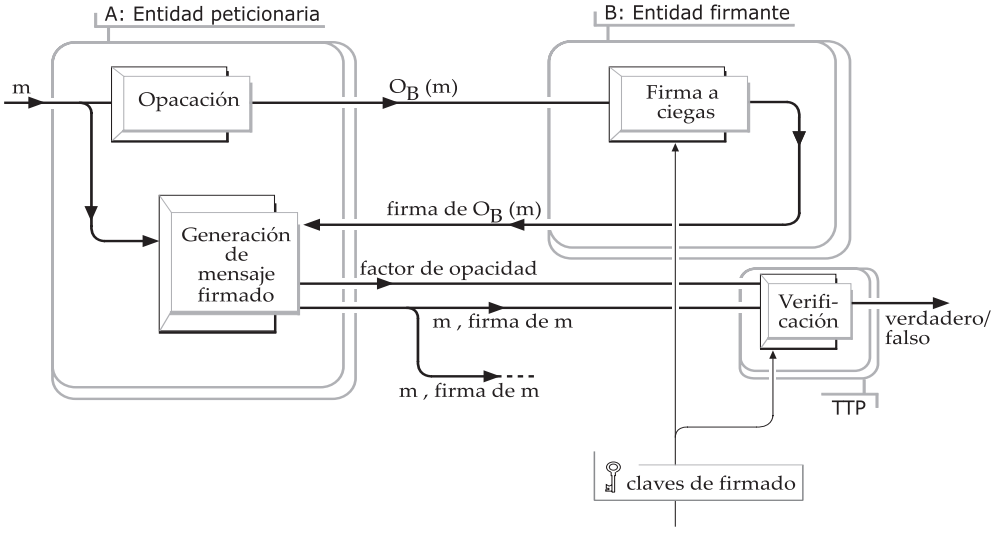

Figura 11.4. Generación y verificación de firma a ciegas con ayuda de una TTP.

que haya alguien interesado en poner en juego la suficiente energía como para conseguir romper el anonimato del opinante. Consecuentemente, si estuviésemos utilizando en ambos casos un mecanismo de firmas opacas, los algoritmos que sería necesario utilizar en cada uno de ellos no tendrían por qué ser de la misma fortaleza.

Volviendo al modelo propuesto en la Figura 11.4, vamos a suponer que en este esquema las claves secretas que usa la entidad *B* para generar la firma a ciegas son también conocidas por la TTP que va a realizar posteriormente la verificación de esa firma.

El proceso podemos describirlo como sigue:

a) La entidad *A* peticionaria, utilizando un factor de opacidad, opaca el mensaje *m* y se lo envía a la entidad firmante *B*. En la figura se ha representado este mensaje opacado como $O_B(m)$ para cubrir el caso en que la opacación sea distinta en función de la entidad que se desea que firme a ciegas (como ocurre en el esquema de Chaum). Caso de que (como ocurre en otros algoritmos) la opacación no fuese específica de la identidad de la entidad firmante, el mensaje opacado se podría representar simplemente como $O(m)$.
b) La entidad firmante *B* genera la firma opaca de $O_B(m)$ y se la envía a la entidad *A*.
c) *A* realiza las comprobaciones que sea capaz de hacer (no está capacitada para verificar la firma que ha generado *B*) y:
    1. Envía a la TTP verificadora el factor de opacidad utilizado en el paso a).
    2. Genera el mensaje firmado: *m* más la firma de *m* realizada por *B*. Esta firma debe ser una pieza de información calculada a partir del valor de la firma que ha recibido de *B* (para evitar que esta entidad pueda posteriormente reconocerla).
d) La entidad *A* envía ese mensaje firmado a cualquier otra entidad destinataria o, antes de distribuirlo, a la TTP para que verifique la corrección de la firma.
e) Cualquier entidad que reciba el mensaje firmado (*m* más la firma a ciegas) si quiere verificar la validez de la firma tendrá que dirigirse a la TTP verificadora para conocer su veredicto sobre la validez o falsedad de la firma realizada por *B*, ya que *B* no puede realizar ese reconocimiento.

La gracia del asunto está en que la TTP conoce tanto el factor de opacidad generado por *A* como las claves utilizadas por *B* para la generación de la firma. Es evidente, por tanto, que la TTP debe ser de absoluta confianza para garantizar el funcionamiento de la firma a ciegas, ya que, si quiere, en cualquier momento puede desvelar los secretos bajo los que se sustenta.

Este esquema de funcionamiento puede extenderse a múltiples entidades peticionarias y varias entidades firmantes. En este caso, para garantizar la verificabilidad de la firma sería necesario incluir algunos identificadores en los intercambios de información descritos en los pasos anteriores.

El segundo de los dos esquemas que anunciábamos al principio de este apartado no se basa en incorporar una TTP para facilitar las operaciones sino en incluirla dentro del escenario para que actúe como juez o árbitro para deshacer la opacidad de la operación en caso de que se sospeche que alguna de las partes involucradas en el proceso actúa maliciosamente para obtener un provecho ilícito de la utilización del mensaje firmado a ciegas.

En la Figura 11.5 se representa un esquema en el que están presentes la entidad solicitante (se supone que pueden existir varias entidades de este tipo), la entidad

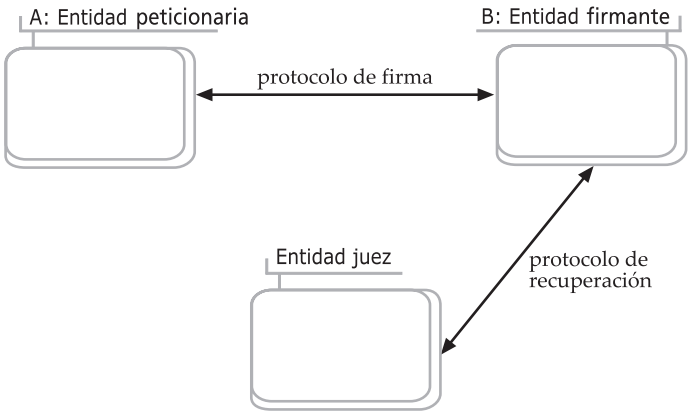

Figura 11.5. Esquema de firma a ciegas arbitrada por una entidad juez.

firmante y una entidad de confianza que actúa como juez. Entre estas entidades se establecen dos protocolos que pueden actuar de forma coordinada:

a) Un protocolo *de firma* en el que sólo intervienen la entidad peticionaria y la entidad firmante.
b) Un protocolo de *recuperación del vínculo* que relaciona a la entidad firmante con la entidad que actúa como juez.

Mediante el primero de ellos la entidad peticionaria obtiene la firma opaca robusta de un mensaje con las características que ya resaltamos al estudiar la firma a ciegas sin tercera parte. Es decir, de tal manera que la entidad firmante no puede relacionar la información que obtiene al ejecutar el protocolo con la pareja mensaje-firma que la entidad peticionaria distribuirá posteriormente.

Mediante la ejecución del protocolo de *recuperación del vínculo* la entidad firmante puede recibir información del juez que le permita relacionar la información que obtuvo al ejecutar el protocolo de firma con la pareja mensaje-firma producida por la entidad peticionaria. Para ello, durante la ejecución del protocolo de firma, la entidad peticionaria debe enviar cierta información que sólo el juez puede leer y la entidad firmante debe ir pasándole a la entidad juez la información suficiente para que ésta esté en condiciones posteriormente de ayudarle a recuperar el vínculo antes referido. Se supone que esta última revelación de datos sólo se pone en marcha cuando existen sospechas justificadas en relación con la utilización indebida de la opacación de la firma (en un entorno real debería ponerse en marcha mediante autorización judicial).

En [SPC95] se recoge un escenario de este tipo en el que se define un modelo genérico similar al representado en la Figura 11.5 que acabamos de comentar. En esta propuesta[2] se recogen, además de varias realizaciones concretas de estos protocolos, dos esquemas distintos para la obtención de la firma opaca que se distinguen entre sí dependiendo de la información que la entidad juez recibe de la entidad firmante durante la ejecución del protocolo de *recuperación del vínculo.*

Como puede apreciarse, la TTP que opera en el esquema representado en la Figura 11.4 participa de oficio en el procedimiento de verificación de la firma a ciegas, mientras que la TTP presente en el esquema mostrado en 11.5 no es de por sí imprescindible para la creación y verificación de la firma. La funcionalidad de esta TTP consiste en observar el proceso y adquirir información sobre él para, llegado el caso

de un comportamiento presumiblemente indebido, desvelar lo que la firma a ciegas oculta. Es evidente, no obstante, que la TTP del primer esquema también puede actuar, si las circunstancias lo requieren, bajo esta segunda funcionalidad.

SECRETO DIVIDIDO

A veces resulta interesante mantener una información secreta repartida entre varias entidades comunicantes con objeto de asegurar que la recomposición del secreto se realiza solamente si coinciden en la voluntad de reconstruirlo todas las partes entre las que aquél se había dividido.

Un ejemplo no telemático de una situación de este tipo podría ser el caso de la caja fuerte de un banco que para abrirla se requiriese la presencia de tres empleados, cada uno provisto de una llave distinta, que previamente le ha sido confiada para su custodia. Para poderla abrir hace falta la presencia de los tres y la voluntad colectiva de aportar el componente que cada uno posee. En este caso, lo que es definitivo no es la identidad de los empleados sino la posesión de la correspondiente llave.

Para emular lo que ocurre en las votaciones convencionales mediante papeleta, en un entorno de voto electrónico podríamos pensar en que para abrir la urna electrónica podría ser necesario que coincidiesen cinco personas, cada una de las cuales tuviese almacenada una información en un testigo de seguridad (por ejemplo una tarjeta inteligente), de tal manera que la urna estuviese programada para que sólo se abriese (mostrase su contenido) cuando esas cinco personas hubiesen aportado su información secreta (hubiesen introducido su tarjeta inteligente en un lector) y, como resultado de la adición de todas ellas, se reconstruyese un determinado secreto global.

El paso previo debería haber sido, por tanto, la división de un secreto (*secret splitting*) en tantas partes como individuos se quiere que participen en su reconstrucción. Cada uno de los fragmentos de por sí no tienen ningún valor: el secreto se reconstruye cuando se junten todos ellos. Además el secreto global puede reconstruirse sin que ninguno exhiba ante los demás el fragmento que le corresponde. Convendremos en denominar *secreto dividido* al caso en el que la partición del secreto se haga de forma que para reconstruirlo sean necesarias todas y cada una de las partes.

Un esquema sencillo [Schn96] para conseguirlo (ya planteado en los inicios de la criptografía moderna) consiste en aplicar un algoritmo basado en la utilización de la operación *OR exclusivo*, que tiene la propiedad de que dadas dos cadenas binarias M y N del mismo número de bits y una cadena 0 con todos sus bits a cero, se cumple que:

$$M \oplus M = 0$$
$$M \oplus 0 = M$$
$$(M \oplus N) \oplus N = M$$

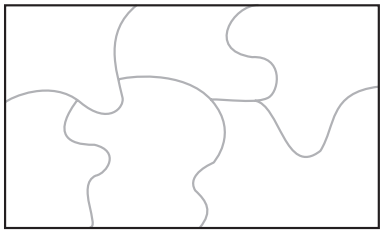

Figura 11.6. Secreto dividido. Para reconstruirlo son necesarias todas las partes.

Supongamos que existe un secreto *S*, por ejemplo la clave privada de la urna electrónica mediante la cual pueden leerse los datos contenidos en ella. Consideremos que el secreto *S* puede estar representado por una cadena de bits (1.024, por ejemplo). Si se tratase de dividirlo en solamente dos partes, un procedimiento sencillo para conseguirlo podría ser que la Autoridad de Seguridad que vaya a generar la partición del secreto *S* realice lo siguiente:

a) La Autoridad de Seguridad genera de forma aleatoria una cadena de binaria, *S1*, del mismo número de bits que el secreto *S*.
b) A continuación, la Autoridad de Seguridad, a partir de *S* y de *S1* genera una nueva cadena aleatoria mediante la operación *OR exclusivo*:

$$S2 = S1 \oplus S$$

c) La Autoridad de Seguridad reparte las cadenas *S1* y *S2* entre dos entidades distintas, *A* y *B,* que serán las que custodien la parte del secreto que se les ha confiado.

En cualquier momento posterior, si *A* y *B* se ponen de acuerdo y se realiza la operación *OR exclusivo* entre sus partes del secreto, se obtiene:

$$S1 \oplus S2 = S1 \oplus (S1 \oplus S) = S$$

A pesar de su sencillez, la operación *OR exclusivo* es muy robusta (ya vimos su empleo en los criptosistemas de secreto perfecto), de forma que, si las cadenas se han generado de forma bastante aleatoria, será bastante difícil romper un esquema de comportamiento como el antes descrito.

Conviene percatarse de que para recomponer el secreto cada entidad aporta su información al sistema donde se está realizando la operación de suma sin que ello implique que la otra entidad adquiera conocimiento acerca del valor de esa parte del secreto (ni del secreto global, por supuesto). Es decir, se puede reconstruir el secreto sin que ninguna de las entidades participantes averigüe la información secreta que posee la otra.

Este esquema de comportamiento puede extenderse sin ninguna dificultad a un mayor número de partes. Si, como en el ejemplo de la urna electrónica que vimos antes, son cinco las partes en las que hay que dividir el secreto, la forma de proceder sería la siguiente:

a) La Autoridad de Seguridad genera de forma aleatoria **cuatro** cadenas de binarias (*S1*, *S2*, *S3* y *S4*) del mismo número de bits que el secreto *S.*
b) A continuación, la Autoridad de Seguridad, a partir de *S* y de las cuatro cadenas *S1* a *S4* genera una nueva cadena aleatoria mediante la operación *OR exclusivo*:

$$S5 = S1 \oplus S2 \oplus S3 \oplus S4 \oplus S$$

c) La Autoridad de Seguridad reparte las cadenas *S1* a *S5* entre cinco entidades distintas.
d) En cualquier momento posterior, si las cinco entidades depositarias de una parte del secreto se ponen de acuerdo y se realiza la operación *OR exclusivo* entre esas cinco cadenas, se obtiene:

$$S = S1 \oplus S2 \oplus S3 \oplus S4 \oplus S5$$

Todo depende de la Autoridad de Seguridad que es, en definitiva, la responsable del correcto funcionamiento del sistema. Las entidades depositarias del secreto dividido no tienen forma alguna de comprobar la corrección de la cadena que se les está entregando. Si la Autoridad de Seguridad, a la hora de generar y distribuir las cadenas, actúa maliciosamente, las entidades implicadas no pueden percatarse de ello hasta el momento en el que quieran reconstruir el secreto y no sean capaces. Y lo que es peor: pueden pensar que la culpa de ese fallo es de una de las entidades participantes que ha podido cambiar el valor de la cadena que le han confiado.

Es evidente, por tanto, que este tipo de solución sólo sirve en el caso de que todos los participantes confíen de forma absoluta en la Autoridad de Seguridad y que las partes del secreto estén almacenadas en un testigo de seguridad no manipulable.

El inconveniente grave de un esquema como el que acabamos de ver es que para reconstruir el secreto es necesaria la concurrencia de todas y cada una de las partes en las que se ha dividido. Si, en el ejemplo de la urna electrónica, una de las cinco personas necesarias para iniciar el proceso de apertura de la urna se ausenta del sitio en el que esa concurrencia debe tener lugar, bien porque las encuestas que se han realizado a pie de urna la hayan sumido en una fuerte desmoralización, bien porque la jornada de confraternización interpartidaria le haya resultado insufrible e insoportable, todo el proceso final de recuento se vería bloqueado. La solución que se plantea en el apartado siguiente trata de resolver esta dificultad.

SECRETO COMPARTIDO

Un planteamiento más general (del que el caso anterior sería un caso particular) consiste en compartir o repartir el secreto (*secret sharing*) entre varias partes de forma que para reconstruirlo no sea imprescindible reunir todas las porciones en que ha sido dividido sino solamente un número mínimo de ellas. Un esquema de este tipo de repartición del secreto es el que podemos denominar esquema umbral p sobre q, o esquema (p, q), donde tanto p como q son enteros mayores que uno y p es menor o igual que q. En este esquema, a partir del secreto S se construyen q muestras o «sombras» (*shadows*) que se reparten entre distintas entidades, de tal suerte que se puede reconstruir el secreto reuniendo cualquier combinación de p de ellas.

En la Figura 11.7 se representa un ejemplo de esquema umbral (4,7), en el que se han extraído siete sombras o muestras del secreto y para reconstruirlo solamente se necesitan cuatro cualesquiera de ellas. Es decir, tres muestras serían insuficientes para reconstruir el secreto, cualquier combinación de cuatro de ellas sería suficiente, y si se reúnen cinco o seis también puede reconstruirse, aunque sobradamente.

Existen distintas propuestas de algoritmos para plasmar un esquema de este tipo, casi todas ellas bastante antiguas y relativamente sencillas de entender. El algoritmo que aquí explicaremos es el propuesto por Shamir [Sham79] basado en la interpolación de polinomios definidos en un campo finito (recuérdese lo visto en el Capítulo 3). El esquema umbral (p, q) se definiría de la siguiente forma:

A partir del secreto S, se elige un número primo n (de tal suerte que tanto p y q como el secreto S sean números inferiores a él) y se construye un polinomio de grado $p-1$ tal que:

$$y = f(x) = (S + a_1 x + a_2 x^2 + \ldots + a_{p-1} x^{p-1}) \bmod n$$

Los coeficientes a_1, a_2, ... a_{p-1} se eligen de forma aleatoria de entre números también menores que n. El secreto S es el valor que adquiere y para $x = 0$ y las distintas

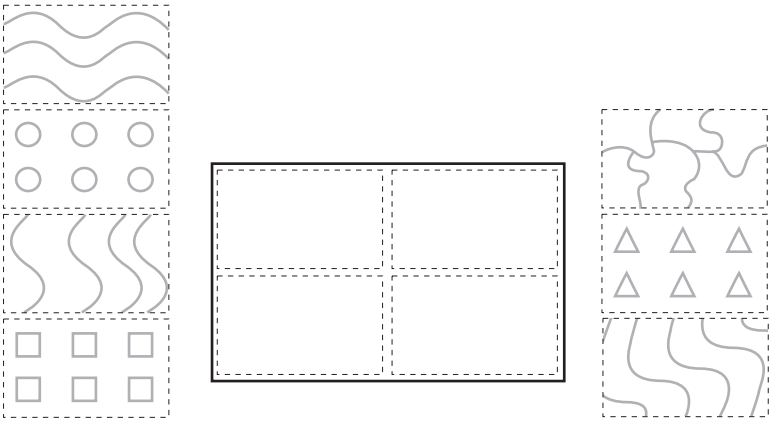

Figura 11.7. Secreto compartido: para reconstruirlo son necesarias cuatro de las siete muestras.

muestras o sombras se obtendrían dando valores arbitrarios, distintos de cero, a la variable *x*. Cada muestra estará constituida por uno de esos pares (x_i, y_i) que se hayan formado. Pueden construirse tantas *q* muestras como se deseen y es fácil demostrar que reuniendo solamente *p* de ellas puede calcularse el secreto *S*.

Para entenderlo fácilmente, veamos un ejemplo muy sencillo en el que *p* es igual a dos y el número *n* que acota el campo es muy pequeño. Supongamos que el polinomio es:

$$y = (9 + 4x) \bmod 11$$

Es decir, el secreto *S* que se quiere repartir es 9 y 4 es el coeficiente del término lineal que se ha elegido al azar. Si representamos $y = 9 + 4x$ en dos ejes de coordenadas, saldría una línea recta que quedaría perfectamente determinada por dos puntos. Por tanto, conociendo solamente dos puntos de esa recta se conocería el punto en el que corta al eje *y*, esto es, el valor del secreto *S*. Aunque la representación en el plano de la gráfica resultante teniendo en cuenta que los valores han de calcularse módulo 11 no sería una sola recta, las conclusiones respecto a la determinación del secreto son las mismas: como $p = 2$, son necesarias solamente dos muestras para reconstruir el secreto. El número de muestras, *q*, que pueden obtenerse sólo está limitado por el valor del módulo.

Por ejemplo, quien repartiese el secreto podría generar tres muestras que se podrían distribuir entre otras tantas personas:

a) $(x = 1, y = 2)$, dado que $y = (9 + 4) \bmod 11 = 2$.
b) $(x = 3, y = 10)$, dado que $y = (9 + 12) \bmod 11 = 10$.
c) $(x = 4, y = 3)$, dado que $y = (9 + 16) \bmod 11 = 3$.

Es inmediato comprobar que a partir del polinomio $y = (S + a_1 x) \bmod 11$, con solamente dos de esas tres muestras o sombras se podría generar un sencillo sistema de dos ecuaciones con dos incógnitas del que se deduciría el valor $S = 9$.

Obviamente, para que sea muy difícil averiguar *S* sin contar con al menos dos muestras sería necesario disponer de números muchísimo más elevados que los que se han supuesto en el ejemplo, cuya única virtud es facilitar el seguimiento de las ope-

raciones mostradas. Por otra parte, el grado $p - 1$ del polinomio dependerá del número mínimo de muestras necesarias para reconstruir el secreto.

Volvamos al ejemplo de la urna electrónica planteado en el apartado anterior. La urna sólo se abre (muestra el contenido de las «papeletas» de votación) cuando los encargados de abrirla son capaces de reconstruir el secreto *S,* que en este caso está representado por los 1.024 bits de su clave privada. En el apartado anterior utilizábamos para ello el *secreto S dividido* en cinco partes, de tal manera que para ser capaces de reconstruirlo sería necesaria la presencia de todas y cada una de las partes. Y vimos también el problema que puede acarrear la exigencia de esta comparecencia unánime.

Utilizando el paradigma del secreto compartido podríamos desarrollar un esquema umbral (4,5), es decir, la Autoridad de Seguridad generaría cinco muestras o sombras y se las entregaría a cada una de las personas miembros de la Mesa Electoral encargada de abrir la urna: un Presidente o Presidenta, un Secretario o Secretaria y tres vocales. Ahora no es imprescindible la presencia de los cinco: con que sólo cuatro de ellos aporten su muestra del secreto, la urna podrá ser abierta.

El número mínimo de muestras necesarias, $p = 4$, determina el orden del polinomio, que en este caso será:

$$y = f(x) = (S + a_1 x + a_2 x^2 + a_3 x^3) \bmod n$$

donde S es el secreto y los coeficientes a_1, a_2 y a_3 serán elegidos al azar entre números menores que n. A partir de aquí, para obtener las cinco muestras no queda sino dar cinco valores arbitrarios a x (distintos de cero, que se corresponde con el valor asignado a S) y obtener los correspondientes cinco pares (x_i, y_i). En este caso, aunque uno de los miembros de la mesa se niegue a colaborar, la apertura se podrá realizar con todas las garantías.

Si bien, como hemos dicho, p determina el grado del polinomio, el número q de muestras a repartir es ampliable sin modificar el polinomio de partida. Si el esquema anterior lo quisiésemos convertir en un esquema umbral (4,7), como el representado en la Figura 11.7, sólo tendríamos que generar dos pares (x_i, y_i) más para tener las siete muestras necesarias. Llegados a este punto, la Autoridad de Seguridad podría decidir distribuir las muestras de forma que le entregase dos muestras a la persona que ostente la presidencia, otras dos muestras a quien lleve la secretaría y una muestra a cada uno de los vocales restantes.

Bajo una situación como esta, para reunir cuatro muestras y ser capaces de abrir la urna, podrían ser suficientes el presidente y dos vocales, o el secretario y dos vocales, o el presidente y el secretario sin presencia de vocales. Pero no podrían abrirla los tres vocales si no colabora o el presidente o el secretario.

Es decir, la repartición de un secreto mediante un esquema umbral (p, q) permite el establecimiento de reglas muy variadas y muy flexibles.

No obstante, estas soluciones de compartición de secreto siguen teniendo las mismas limitaciones que comentamos al describir el secreto dividido (al fin y al cabo son dos variaciones de una misma forma de proceder). Esta limitación estriba en que todo depende de la Autoridad de Seguridad porque las entidades depositarias de las muestras o sombras del secreto no tienen forma alguna de comprobar que lo que se les ha entregado es correcto. Si la Autoridad de Seguridad actúa maliciosamente las entidades involucradas no tienen forma de percatarse de ello hasta el momento en el que quieran reconstruir el secreto y no sean capaces.

Por todo ello, conviene insistir en que este tipo de soluciones son de interés sólo en el caso de que exista una confianza total en la autoridad que genera el reparto y, además, las entidades involucradas dispongan de dispositivos resistentes a manipula-

ción (*tamper resistant*) para almacenar su parte del secreto sin que ellas mismas sean capaces ni de leerlo ni de modificarlo.

11.2. TARJETAS INTELIGENTES AL SERVICIO DEL ANONIMATO

A lo largo de los capítulos precedentes, en multitud de ocasiones hemos venido haciendo reiteradamente referencia a la utilidad que podría representar el uso de tarjetas inteligentes en muy diversos escenarios.

En realidad, una tarjeta inteligente no es más que un dispositivo físico que permite almacenar información de seguridad de forma fiable que, además, debido a que tiene un microprocesador incorporado, puede gobernar tareas de entrada/salida y ejecutar algunos algoritmos criptográficos. Ello posibilita, entre otras muchas cosas, que pueda almacenar la clave privada de su titular y cifrar datos con ella. Pero muchos otros dispositivos podrían responder a esta breve descripción y, sin embargo, no han merecido tanta atención por nuestra parte. Luego debe haber algo más.

En efecto, hay, al menos, tres cosas más que hacen que las tarjetas inteligentes presenten para nosotros tanto interés. Su portabilidad (el aspecto externo es similar a una tarjeta de plástico convencional) y su bajo precio son dos de ellas. La otra es que están fabricadas de forma que los datos en ellas almacenados no se pueden leer ni alterar de forma fraudulenta.

Por todo ello, en las aplicaciones telemáticas seguras que interesan a los ciudadanos es frecuente encontrar que las tarjetas inteligentes son unos testigos de seguridad que ayudan grandemente a diseñar escenarios de comunicación complejos al tiempo que sirven para preservar la privacidad de los participantes.

Alguna limitación o inconveniente habrán de tener. Así es en efecto: debido a su reducido tamaño, la capacidad de proceso y, sobre todo, de almacenamiento es limitada. Pero aun así esta es una restricción que va siendo menor a medida que van evolucionado las tecnologías de fabricación. Por eso es acertado aventurar que las tarjetas inteligentes, u otros dispositivos de similares características que se desarrollen en un futuro, van a seguir jugando un papel muy relevante en el desarrollo de esas aplicaciones que protegen la privacidad de los ciudadanos.

De lo dicho hasta aquí se deduce que las tarjetas inteligentes son de utilidad para la provisión de **todos** los servicios de seguridad y no sólo para la provisión del servicio de anonimato. El hecho de que en el título del presente epígrafe hagamos hincapié en este último servicio es debido a la constatación, antes comentada, de su presencia en los escenarios de comunicación que servirán de soporte a la Sociedad de la Información. Por ello, más que hablar de las tarjetas inteligentes al servicio del anonimato, en este epígrafe lo que realmente haremos es hablar de las tarjetas inteligentes al servicio de las aplicaciones que posibilitan la seguridad y la privacidad en las comunicaciones.

En entornos más profesionales, por ejemplo en la gestión de claves de una CA, se dispone de otros dispositivos físicos de tamaño y grosor no mucho mayores que los de una tarjeta inteligente, que también son resistentes a manipulaciones (*tamper proof*), pero con mucha mayor capacidad de proceso y de almacenamiento. El conexionado que les permite entrar en contacto con el exterior es diferente al normalizado para las tarjetas inteligentes, por lo que no existe posibilidad de compatibilizar su uso a través de un mismo periférico de lectura-escritura. Estos dispositivos no serán objeto de atención en el presente epígrafe, orientado a evaluar las posibilidades que ofrecen las tarjetas inteligentes a los usuarios finales.

Para entender mejor en qué medida son interesantes las tarjetas inteligentes vamos a estudiar de nuevo el comportamiento de estos dispositivos. Ya en el Capítulo 2, cuando planteamos una visión general de los conceptos y elementos presentes en la Seguridad en Redes Telemáticas, adelantamos cuáles son las características principales de las tarjetas inteligentes tradicionales, es decir, aquellas se que se ajustan estrictamente a la norma ISO 7816. Ahora ampliaremos algunos detalles acerca de su estructura y funcionamiento para poder analizar con mayor conocimiento de causa el tipo de aplicaciones en las que pueden ser utilizadas.

Además, analizaremos someramente las características y posibilidades de uso de una nueva generación de tarjetas no comentadas en el Capítulo 2. Se trata de las tarjetas que operan con pequeñas aplicaciones (*applets*) codificadas en Java: las denominadas *Java Cards* o *Tarjetas Java*. La experiencia demuestra que este tipo de componentes ofrece mayores posibilidades a los desarrolladores de aplicaciones.

ESTRUCTURA INTERNA DE LA TARJETA «CLÁSICA»

Las dimensiones externas de la tarjeta de plástico en la que se inserta el circuito integrado están perfectamente normalizadas (ISO 7816) para conseguir la compatibilidad de los dispositivos de lectura a través de los cuales se comunica con el mundo externo (habitualmente se comunicará con otro computador desde el que se regula su utilización).

Como ya hemos venido diciendo, una tarjeta inteligente es un minúsculo microcomputador contenido en un circuito integrado o *chip* que posee (Figura 11.8) la correspondiente Unidad Central de Proceso (CPU), un elemental sistema de entrada/salida y un espacio de memoria para almacenar datos y programas.

Para reforzar la eficacia del microprocesador que opera como CPU, las tarjetas más potentes disponen de un coprocesador matemático que facilita la ejecución de los algoritmos criptográficos. La mayor limitación en la potencia de las tarjetas inteligentes viene dada por lo reducido del espacio de memoria de que disponen, aunque la mejora de los procedimientos de fabricación consigue que éste vaya siendo cada vez mayor.

Cuando se diseña una aplicación concreta para operar en conjunción con una tarjeta inteligente, lo primero que se decide es qué parte de esa aplicación correrá fuera de la tarjeta y cuál dentro. Otro tanto puede decirse en relación con las estructuras de datos que se manejen.

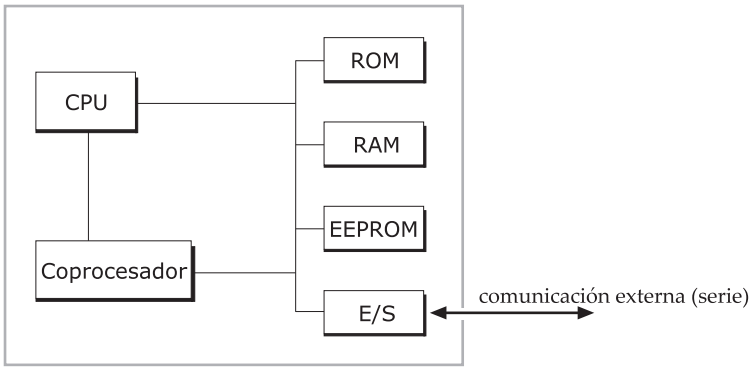

Figura 11.8. Elementos constitutivos de una tarjeta inteligente.

En lo que se refiere a la parte de los programas y los datos que residan dentro de la tarjeta, el pequeño sistema operativo que gobierne su funcionamiento y los programas que se consideren más estables irán grabados, desde el mismo proceso de fabricación, en la memoria de sólo lectura (ROM). Esta información es inalterable, lo que supone que una posible modificación motivada por una mejora o corrección de su comportamiento conllevaría desechar esa tarjeta y construir una nueva.

También, para guardar datos y estados que varíen durante la ejecución del programa, las tarjetas inteligentes disponen de un espacio de memoria de lectura-escritura y acceso directo (RAM). Por lo general, en este tipo de tarjetas, el tamaño de la memoria RAM es reducido (menos de mil octetos), lo que limita el tipo de operaciones que pueden llevarse a cabo a través del programa almacenado.

La memoria EEPROM* servirá para almacenar aquellos datos y programas que pueden verse modificados durante el tiempo de vida de la tarjeta. Esta memoria puede borrarse y regrabarse externamente por parte de personas que conozcan suficientes detalles sobre la aplicación concreta que se ha diseñado para esa tarjeta. De los ocho posibles contactos mediante los cuales la tarjeta se comunica con la unidad de lectura y escritura (ULE o CAD, *Card Acceptance Device*) existe uno de ellos, conocido como V_{pp} (Figura 11.9), que sirve para suministrar a la tarjeta el voltaje necesario (entre 12,5 y 21 voltios, según los casos) para poder regrabar esta EEPROM.

La forma, posición y cometido de estos ocho contactos está, como ya se ha dicho, perfectamente especificada en la norma ISO 7816. Aparte del ya mencionado V_{pp}, existen otros cinco contactos con la siguiente funcionalidad: a) V_{cc} para suministrar la tensión de cinco voltios necesaria para su funcionamiento; b) CLK para la entrada de reloj; c) un contacto GND para masa; d) un contacto RST de rearranque; y e) un solo contacto (I/O) para la comunicación de entrada/salida. Los otros dos contactos restantes (RFU) están reservados para otras posibles funciones.

Para evitar el desgaste de los contactos provocado por el uso, se han desarrollado tarjetas sin contactos que se comunican con el exterior mediante ondas electromagnéticas[3]. Este tipo de tarjetas son útiles en control de tránsito o medios de transporte en los que conviene evitar el trámite de insertar la tarjeta en el lector, aunque, debido a lo reducido de la potencia de emisión puesta en juego, es necesario que la tarjeta se aproxime mucho al dispositivo a través del cual se comunica.

Volviendo al esquema convencional de comunicación mediante contactos directos, el diálogo entre la tarjeta y lector se inicia cuando éste aplica una tensión de cinco voltios entre el punto V_{cc} y masa. A continuación, a través del contacto CLK introduce

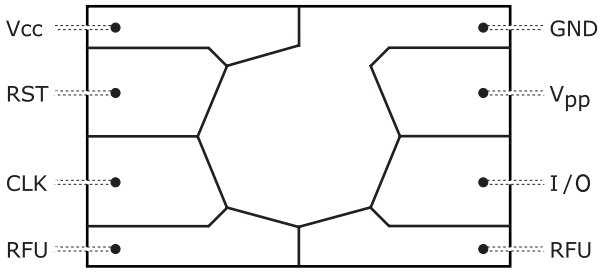

Figura 11.9. Los ocho contactos externos del microcomputador.

* Como es sabido, EEPROM es el acrónimo de *Electrically Erasable Progamable Read-Only Memory*.

la señal de reloj y activa el contacto de rearranque. Como respuesta a estos estímulos la tarjeta emite una respuesta (denominada ART) mediante la que comunica al mundo exterior los protocolos de transmisión que admite y los parámetros básicos [Dieg00] acerca de cómo ha de ser la comunicación (detalles sobre el reloj, lógica utilizada, etcétera). A partir de ahí será el lector el que lleve la iniciativa enviando peticiones a las que la tarjeta deberá responder.

Para posibilitar esa comunicación entre el lector y la tarjeta se han definido un conjunto de protocolos de transmisión (ISO 7816-3) en los que se especifica con detalle la estructura de las TPDUs intercambiadas (unidades de datos del protocolo de transmisión). Aunque hay definidos hasta 15 protocolos distintos, los más usados son el T=0 y el T=1. El primero de ellos realiza una transmisión semidúplex asíncrona de caracteres, y el segundo es similar aunque opera con bloques (de forma similar a un protocolo de nivel de enlace) en vez de con caracteres aislados. El hecho de que solamente se disponga de una línea serie limita bastante las posibilidades de la comunicación que puede establecerse.

Sobre este nivel de transmisión se define (ISO 7816-4) un protocolo de aplicación que regula la comunicación entre la tarjeta y el computador al que está conectado el CAD. Las unidades de dato de este protocolo de aplicación, APDUs, se intercambian de forma bidireccional alternada en forma de preguntas o comandos que genera el computador y respuestas de la tarjeta.

PROTECCIONES, FICHEROS Y AUTENTICACIONES

Para garantizar que sea muy difícil falsificar o manipular la tarjeta inteligente mediante ataques externos es necesario establecer protecciones tanto físicas como lógicas. Entre las primeras podemos destacar el hecho de que el microcomputador dejará de funcionar si alguien lo extrae de la tarjeta con la intención de analizarlo microscópicamente. Para ello, cuando el sistema integrado que contiene el microcomputador se introduce en la tarjeta, se somete a una presión mecánica permanente de forma que, detectando esta presión, el chip puede conocer si ha sido extraído o no.

Aunque el chip está protegido contra la luz ultravioleta y otras radiaciones, algún atacante podría intentar borrar algunas celdas de memoria. Por ello existen bits centinela distribuidos aleatoriamente en la memoria que serán comprobados por el microprocesador cada cierto tiempo y que, caso de que se borren, servirán de aviso para que el sistema deje de funcionar. Asimismo, otras posibles protecciones consisten en la ejecución de operaciones fingidas para evitar que se rastreen y averigüen las secuencias de instrucciones midiendo el consumo de energía.

Además de este tipo de protecciones, la tarjeta inteligente posee mecanismos que le permiten autenticar los datos que recibe y las entidades con las que se comunica. Los datos contenidos en la tarjeta están organizados (ISO 7816-4) según una estructura jerárquica en forma de árbol en cuya raíz se encuentra un denominado *Fichero Maestro*, o *MF*. La estructura puede contar con varios niveles y ficheros especializados en distintas tareas de administración o de almacenamiento de datos de usuario. El siguiente nivel jerárquico lo ocupa el *Fichero Dedicado*, o *DF*. Sólo existe un *MF* pero puede haber uno o varios *DFs* dependiendo de él (véase Figura 11.10) y pueden existir varios niveles jerárquicos de *DFs*. Por último, está normalizada la existencia de varios tipos de *ficheros elementales*, *EFs*, que son los verdaderos ficheros de datos y, como se refleja en la figura, pueden depender de cualquiera de los antes citados.

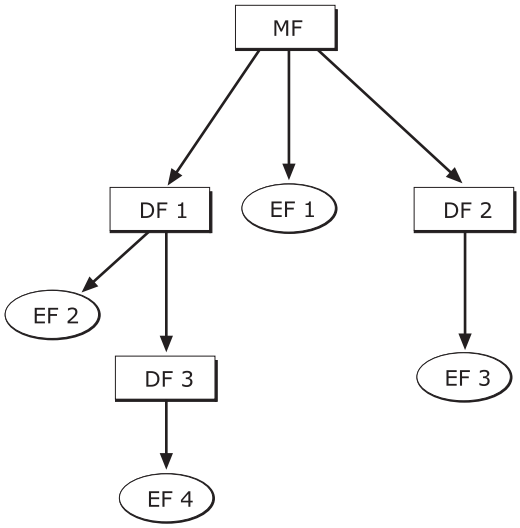

Figura 11.10. Sistema de ficheros en una tarjeta inteligente «clásica» o tradicional.

Sobre cada fichero se pueden realizar múltiples acciones (la norma enumera hasta 21) entre las que se encuentran las de selección, lectura, escritura, búsqueda, invalidación, etc., todas ellas llevadas a cabo mediante intercambio de PDUs. Cada fichero posee unas condiciones de acceso distintas, conforme a determinados niveles, para cada operación. El nivel más elemental consiste en que la entidad que pretende el acceso tiene que suministrar a la tarjeta un PIN o contraseña. Un nivel de acceso más riguroso se produce cuando para determinados ficheros se requiere que la entidad que accede (que se denomina «autoridad administrativa») comparta con la tarjeta inteligente una clave secreta cuya posesión tiene que demostrar, mediante un mecanismo de reto, para que se le permita el acceso.

En este último caso se produce un diálogo entre la tarjeta y la entidad externa que consiste, aproximadamente, en lo siguiente:

a) La tarjeta genera un número aleatorio y se lo envía a la entidad.
b) La entidad cifra ese número aleatorio con la clave secreta que comparte con la tarjeta.
c) La tarjeta verifica el cifrado y autoriza o deniega el acceso.

La autenticación del usuario ante la tarjeta se consigue mediante la introducción de un PIN secreto que sólo debe conocer la persona que es su legítima propietaria. Más adelante discutiremos las circunstancias en que se puede aplicar este mecanismo de autenticación y las ventajas que aporta el uso de controles biométricos.

Como medidas de seguridad complementarias se utilizan determinadas restricciones en la autenticación de entidades externas consistentes en limitar el número de intentos fallidos en una misma sesión y exigir nuevos procesos de autenticación en el caso de que se produzcan anomalías en la alimentación o en las señales que se aplican en otros contactos.

Es decir, las tarjetas inteligentes tradicionales ofrecen bastantes posibilidades para garantizar un nivel de seguridad bastante razonable de cara al tipo de aplicaciones

sobre las que estamos centrando nuestro interés en el presente capítulo. No obstante, en cuanto a las posibilidades de introducir programas dentro de su memoria para que sean ejecutados internamente por su propio microprocesador, presentan grandes limitaciones que se pueden solventar utilizando una nueva generación de tarjetas inteligentes: es la generación de las *Tarjetas Java* o *Java Cards*. A ellas dedicaremos el siguiente apartado.

ESTRUCTURA Y FUNCIONAMIENTO DE LAS TARJETAS JAVA

Como su nombre sugiere, una *Tarjeta Java* o *Java Card* es una tarjeta inteligente en cuyo sistema microcomputador pueden ejecutarse pequeñas aplicaciones, llamadas *applets* *, que operan y se programan conforme a la tecnología Java[4]. Estas *applets* se ejecutarán en la correspondiente Máquina Virtual Java, que en el caso de estas tarjetas recibe el nombre de JCVM (*Java Card Virtual Machine*).

El formato y las dimensiones externas de la tarjeta de plástico que les sirve de base son en todo compatibles con las que hemos denominado «clásicas» o tradicionales (aquellas que se ajustan a la norma ISO 7816 en sus siete partes). También la arquitectura del microcomputador contenido en el chip, así como la disposición y funcionalidad de los contactos que lo comunican con el mundo exterior, son conformes con dicha norma y responden al esquema representado en las Figuras 11.8 y 11.9 antes comentadas.

Esta compatibilidad se fundamenta en que las Tarjetas Java[5] son totalmente conformes con la norma ISO 7816 en sus partes 1, 2 y 3. Debido a ello, los protocolos denominados *de transmisión* o *de transporte* mediante los cuales se comunican la tarjeta y el CAD (dispositivo de lectura/escritura) son coincidentes con los que ya

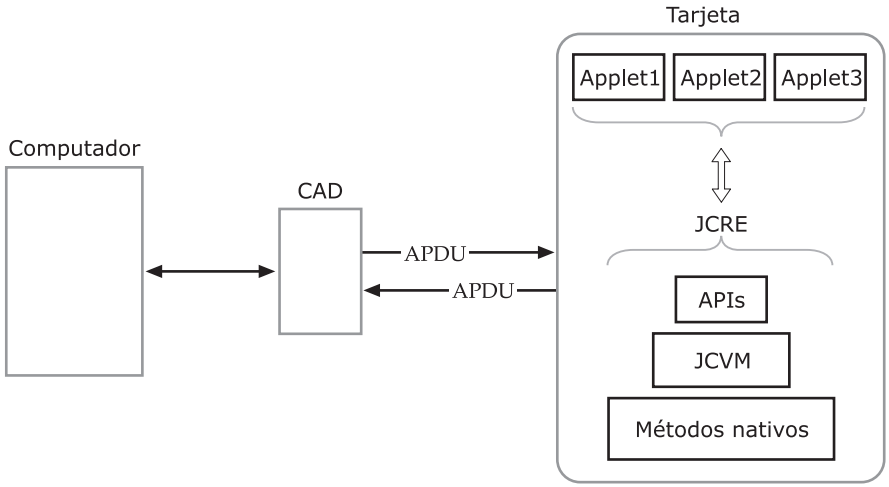

Figura 11.11. Estructura de la Tarjeta Java y esquema de comunicación.

* La palabra *applet* viene a significar «aplicacioncita» o «pequeña aplicación». Aunque en la jerga imperante en el mundillo de la programación es frecuente nombrarla en masculino, parece más razonable usarla en femenino, conservando el género de la palabra de la cual procede. En la versión en español del libro de Tanenbaum [Tane97] (un libro clásico sobre redes) se sigue este mismo criterio.

hemos referido. Por tanto, entre el CAD y la tarjeta existirá un intercambio de TPDUs (con una funcionalidad equivalente a la del nivel de enlace de los protocolos OSI), aunque en la Figura 11.11, que representa la estructura de una Java Card y el esquema de comunicación entre la tarjeta y el computador conectado a la red telemática, no se haya reflejado (por simplificar) este intercambio de PDUs.

En dicha figura sí se ha representado la existencia de unas APDUs, con semántica y funcionalidad propia, que se encastrarán, a efectos de la transferencia de información, en las correspondientes TPDUs.

La estructura lógica de la tarjeta se representa también, de forma muy simplificada, en la Figura 11.11 a la que venimos haciendo referencia. Como hemos dicho, los programas y los datos se alojarán en la memoria (materializada en componentes RAM, ROM y EEPROM) y las instrucciones de máquina serán ejecutadas por el correspondiente microprocesador (con ayuda, si existe, del coprocesador criptográfico). Cada fabricante podrá incorporar un microcomputador diferenciado con una arquitectura interna propia, de forma que, en último extremo, los programas deberán ejecutarse conforme a un conjunto específico de instrucciones de máquina. Debido a ello, en la parte inferior de la estructura lógica representada en la figura aparecen los *Métodos nativos* que se adaptarán a las características particulares de cada microcomputador y, además, servirán de soporte a la JCVM (*Java Card Virtual Machine*) y a otras clases del entorno de ejecución Java. Estos métodos serán los que proporcionen el acceso a los recursos físicos, protocolos de comunicación de bajo nivel, uso del coprocesador criptográfico, gestión de memoria, etc.

En la JCVM es donde se interpretan los códigos de bytes, y será la encargada de ejecutar las applets, garantizar la seguridad, gestionar objetos, organizar el reparto de memoria, etc. En un nivel inmediatamente superior se encuentra lo que hemos denominado con el nombre genérico de API, que englobaría las applets propias del sistema y las clases necesarias para proveer los distintos servicios soportados. Este bloque representa las funciones o tareas que pueden invocar las pequeñas aplicaciones de usuario (que se representan en la parte superior del diagrama), incluyendo los programas necesarios para cargarlas e instalarlas en la tarjeta.

El conjunto de estos tres bloques (métodos nativos, JCVM y APIs) constituye el entorno de ejecución de la Tarjeta Java o JCRE (*Java Card Runtime Environment*), que es el responsable global de la ejecución de los programas y de la gestión de todos los recursos. Es decir, se comporta, en la práctica, como el verdadero sistema operativo de la tarjeta.

Para adaptar la tarjeta inteligente a una aplicación concreta, las applets necesarias se programan cómodamente en un sistema informático convencional, se prueban y se depuran y después se instalan en la tarjeta. La tecnología Java permite al programador diseñar una applet sin tener en cuenta la plataforma física concreta sobre la que va a ejecutarse en la tarjeta, reduciendo los costes del desarrollo. Además, al trabajar con una programación orientada a objetos se facilita el diseño modular y la reutilización de los módulos.

Debido a que el programa se ejecuta mediante un intérprete, es posible probar las instrucciones antes de que se ejecuten, teniendo garantías de que la applet va a respetar los datos y los recursos de otras applets y no va a realizar operaciones indebidas. Esta característica es especialmente interesante cuando se requiere que en una tarjeta cohabiten varias aplicaciones o cuando se necesite ampliar la funcionalidad de una tarjeta añadiendo una nueva applet.

La limitación que tiene todo esto es que debido a la poca potencia del microprocesador que gobierna la tarjeta y a lo reducido del espacio de memoria en que pueden

residir los programas y los datos, la Java Card solamente soporta un subconjunto de los elementos * definidos en el lenguaje Java. Entre los elementos que no soporta cabe destacar:

- Tipos de datos primitivos y estructuras de datos que ocupan gran cantidad de octetos (*float, double, long, arrays multidimensionales*...).
- Hilos y sincronización.
- Clonación de objetos.

Es razonable que, dadas sus características, nunca pueda una tarjeta soportar definiciones de datos que ocupen gran cantidad de octetos, ni estructuras dinámicas complejas, pero también es cierto que la evolución de la tecnología hace que cada vez los microprocesadores sean más rápidos y que puedan implementarse memorias con mayor capacidad de almacenamiento. Por ello, es de esperar que, progresivamente, las limitaciones impuestas al lenguaje Java vayan siendo cada vez menores.

De lo que venimos diciendo acerca de la estructura lógica de una Tarjeta Java, donde el funcionamiento global está focalizado en la existencia de applets «independientes», cabe deducir que no tiene mucho sentido normalizar aquí un sistema de ficheros como el definido en la ISO 7816-4 para las tarjetas tradicionales (que se representa en la Figura 11.10). Consecuentemente con ello, en las Java Cards no está definida la autenticación que allí se hacía de entidades externas a la tarjeta (apoyándose en el intercambio de contraseñas o en la compartición de claves) para permitirles o denegarles el acceso a determinados ficheros.

En las Java Cards la autenticación de entidades externas (básicamente entidades clientes de una aplicación) se centra en la comunicación que dicha entidad desee establecer con una determinada applet. El primer paso en una comunicación entre la tarjeta y una entidad externa consiste en llevar a cabo una *autenticación mutua* entre ambas. Esto se realiza mediante un proceso de diálogo en el que se comparan unas claves, contenidas en un fichero, que deben ser las mismas en ambos extremos de la comunicación. La autenticación consiste en que la tarjeta comprueba que las claves que le presenta la entidad externa coinciden con las suyas propias y la entidad externa hace otro tanto con las claves que le presenta la tarjeta.

Una vez que la autenticación se ha llevado a cabo satisfactoriamente, se establece un canal seguro entre las dos entidades, apoyándose en el cual se intercambian las distintas piezas de información que constituyen los protocolos mediante los que se comunican.

Como dijimos más arriba al comentar la Figura 11.11, en las Tarjetas Java también están definidos los protocolos de transmisión y de aplicación y las correspondientes unidades de datos TPDUs y APDUs. No obstante, si bien en lo que se refiere al transporte las Tarjetas Java son totalmente conformes con la ISO 7816-3, en lo que se refiere a las APDUs normalizadas en la ISO 7816-4, esa conformidad sólo se produce en parte. Esto es así porque al no estar definido en esta nueva generación de tarjetas el sistema jerárquico de ficheros, todas las APDUs cuyo cometido era regular el acceso a los ficheros dejan de tener sentido. En contrapartida, será necesario definir nuevas APDUs que sirvan para establecer la comunicación entre las applets y el mundo exterior.

---

* El conjunto de elementos soportados está definido en la *Java Card Application Programming Interface Specification.*

A modo de resumen, podemos decir que ambos tipos de tarjetas, las Java Card y las que hemos dado en denominar tradicionales o «clásicas», tienen algunos elementos diferenciales en cuanto a la organización lógica de los datos y los programas residentes en el microcomputador, pero tienen bastantes elementos estructurales comunes: aquellos reflejados en la ISO 7816, partes 1, 2 y 3. Por esta razón, aquí no hemos utilizado el término *tarjetas ISO* para referirnos a las tarjetas convencionales que son conformes con la totalidad de la norma, y para diferenciar ambos tipos de tarjetas hemos huido, por tanto, de establecer el binomio *tarjetas ISO*/*Tarjetas Java*, porque ello induce a pensar que, por contraposición, el segundo tipo carece por completo de conformidad con la norma ISO. De forma que, para consumo interno, nos hemos despachado llamándole «clásica», así, entre comillas, a la tarjeta tradicional con microprocesador (que no es la misma que otra tarjeta más clásica todavía: la tarjeta de memoria sin microprocesador).

11.3. ANONIMATO EN LOS MEDIOS DE PAGO

Una de las actividades usuales en las sociedades organizadas es el intercambio de bienes y servicios a cambio de una prestación económica. Dentro de la Sociedad de la Información, este tipo de actividades han de tener su plasmación en el mundo de las Comunicaciones Mediante Computador (CMC). Es por ello que ya en la actualidad existe un elevado número de aplicaciones que podemos calificar bajo el nombre genérico de Comercio Electrónico, las cuales tratan de conjugar las ventajas indudables que ofrecen las comunicaciones telemáticas con las garantías que tradicionalmente ofrecen las operaciones comerciales convencionales.

La insuficiencia de esas garantías es lo que ha motivado que la implantación de este tipo de actividades en la Red haya sido, hasta el presente, más lenta (y menos lucrativa) de lo que algunos imaginaron frotándose las manos.

La firma electrónica es, por las razones que ya vimos en los capítulos en los que abordamos su estudio, uno de los pilares en que se sustentan esas garantías, por lo que es de esperar que cuando den fruto las iniciativas técnicas y legales que promueven su uso generalizado, ello generará un impulso en las actividades comerciales que se apoyan en redes telemáticas.

Otro aspecto que afecta de lleno a la implantación masiva de actividades de intercambio comercial en la Red es el relacionado con la pérdida de privacidad que puede representar el que determinados poderes económicos conozcan exhaustiva y pormenorizadamente cuándo y en qué los ciudadanos se gastan su dinero. Es decir, el efecto que causa la ausencia del necesario anonimato en determinadas operaciones de compraventa. Bien es verdad que este es un aspecto que, en principio, no preocupa a esos centros de poder económico (porque reporta un beneficio para ellos), pero sí es algo que preocupa a la ciudadanía por cuanto tiene de lesivo para sus derechos y libertades. Y por esa razón debería importar a los poderes públicos si, como proclaman, son garantes e impulsores de esos derechos cívicos.

En este contexto, existen en la actualidad (y es de esperar que aumenten en un futuro) numerosas propuestas acerca de Comercio Electrónico, con y sin servicios de anonimato incluido. En los párrafos que siguen no describiremos ni unas ni otras (como tampoco hemos descrito las aplicaciones convencionales de correo, web, transferencia de ficheros, etc.), sino que solamente nos centraremos en detectar los aspectos genéricos que afectan al anonimato, verdadero objetivo de este capítulo. Lo que sí haremos es hacer referencia a algunas partes de algunas propuestas existentes.

ESCENARIOS DE DINERO DIGITAL ANÓNIMO

Para la realización de compras de bienes y servicios a través de redes telemáticas será necesario emular los comportamientos existentes en el «mundo real». Tradicionalmente, los dos medios de pago (Figura 11.12) que han venido utilizándose han sido:

a) *Dinero en efectivo.* También llamado *dinero en metálico* o *dinero corriente*, es el constituido por monedas o billetes expedidos por un banco central de confianza para las partes que intervienen en una transacción.
b) *Dinero en forma de pagarés, cheques o tarjetas.* Al no tratarse de dinero a la vista, cuando se usa esta forma de pago, de alguna manera entra en juego la credibilidad y la solvencia de la persona que entrega ese dinero.

Por emulación, llamaremos genéricamente *dinero digital* o *dinero electrónico* a la plasmación en la Red de estos medios de pago. Por *dinero digital* podemos entender, por tanto, cualquier intercambio de piezas de información, en formato electrónico, del que resulte una transferencia de fondos entre dos o más partes. En una operación de compraventa el intercambio de esa pieza de información debe ofrecer garantías al vendedor de que obtendrá, directamente o a través de una entidad bancaria, una cantidad de dinero equivalente al precio de la mercancía que acaba de ceder.

Emular al dinero en metálico no es tarea sencilla. Es cierto que su uso resulta a veces incómodo y sujeto a múltiples limitaciones, pero es necesario resaltar que el dinero en metálico es un viejo mecanismo que permite mantener totalmente 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. Por otra parte, 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.

Los cheques o pagarés son propiamente documentos que se intercambian entre las partes que intervienen en la transacción, y nunca ofrecen anonimato (de ningún tipo), por lo que el análisis de su emulación en forma de dinero digital es algo que no nos interesa de cara a los objetivos que nos hemos planteado en este capítulo.

Caso aparte son las tarjetas. Por tres razones: a) porque en gran medida ya están de por sí integradas en las redes telemáticas (por lo que no ha lugar hablar de su «plasmación digital»); b) porque, generalmente, en su uso cotidiano no ofrecen anonimato (situación que no nos interesa emular); y c) porque nos interesa hablar de propuestas emergentes de tarjetas (soportadas en tarjetas inteligentes) que sean más seguras que las convencionales y además ofrezcan anonimato.

Es decir, en este caso no se trata de garantizar en la Red los derechos de los ciudadanos que ya garantizan las tarjetas, sino de evaluar propuestas que posibilitan la inclusión de servicios de seguridad que sirvan para que las nuevas tarjetas ofrezcan mayor privacidad que las convencionales.

Básicamente, en cuanto a su utilización como medios de pago, podemos considerar que existen tres tipos de tarjetas:

- Tarjeta-monedero. Suele denominarse así a aquella que una vez cargada en un cajero automático o dispositivo *ad hoc*, permite ir haciendo uso de ese dinero hasta su finalización. En el momento de la carga será deducido el importe de la cuenta corriente de su titular.

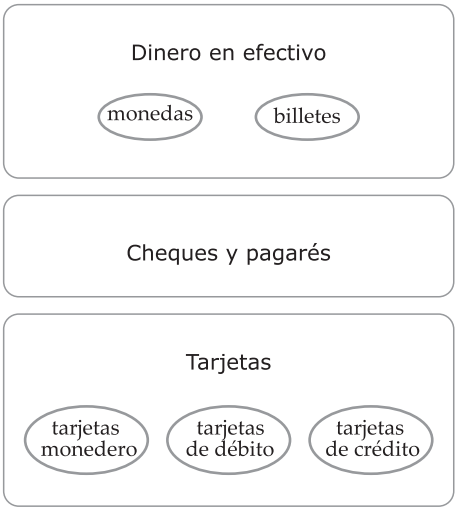

Figura 11.12. Medios de pago tradicionales.

- Tarjetas de débito. 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.
- Tarjetas de crédito. Son aquellas en las que el banco, tras comprobar que la persona titular de la tarjeta tiene crédito suficiente, anota la cantidad resultante de la compra efectuada y transcurrido un plazo de tiempo prefijado (generalmente un día concreto de cada mes) lo deduce de la cuenta corriente junto con el montante de otras compras realizadas.

De cara a su plasmación en escenarios de pago con anonimato, sólo nos interesan cuando son de propósito general, es decir, carece de interés para nosotros pensar en una tarjeta telefónica (aunque sí sean anónimas) que solamente sirve para llamar por teléfono. Por otra parte, a los efectos de lo que aquí nos interesa, no existen diferencias sustanciales entre ellas, ya que en lo único que se diferencian es en el momento en que se realiza el descuento de fondos. Debido a esto, cuando en los párrafos que siguen se haga alusión a las «tarjetas de crédito» debe entenderse que los razonamientos que se utilicen pueden extenderse a las tarjetas de los otros dos tipos. Evidentemente, en cada aplicación y en cada escenario concreto se definirá qué tipo de tarjeta se usa, pero esto no afecta significativamente al tipo de mecanismos criptográficos que se necesitan para conseguir el anonimato.

Ya en la actualidad se constata que, de forma creciente, un gran número de operaciones comerciales son llevadas a cabo por los ciudadanos mediante tarjetas de crédito. El uso masivo de tarjetas de crédito y los problemas de vigilancia que ello conlleva ha alertado a amplios sectores de la sociedad y atraído la atención de muchos investigadores sociales[6], que consideran este hecho como sumamente pernicioso para la conservación de la privacidad (entendida ésta, en el sentido que recogíamos en el Capítulo 1, como el derecho ciudadano a mantener protegido aquello que afecta a comportamientos sociales que sólo incumben a una persona o un grupo reducido de ellas).

Esto es así porque puede darse la situación, a medida que se vaya implantando la Sociedad de la Información, de que muchísimas de nuestras actividades, desde que nos levantemos hasta que nos acostemos, estén grabadas en registros informáticos. Frente a este peligro, la inclusión de servicios de anonimato en las transacciones puede suponer un conjuro contra esa pesadilla de vigilancia y totalitarismo que algunos investigadores sociales temen que pueda producirse con la introducción masiva de medios de pago electrónico.

Para ir centrando el tema, sin excluir el interés que, en general, puede tener el uso de tarjetas de crédito con soporte telemático e incluso con servicios de seguridad y de certificación (como puede ser el caso de SET, comentado en el Capítulo 7), de cara a la tipificación de escenarios de dinero digital anónimo, un primer aspecto que conviene anotar es que las **tarjetas de pago** que tienen mayor interés (y que serán, por tanto, en las que nos fijemos) serán aquellas que se materializan en **tarjetas inteligentes**.

(El solo uso de **tarjetas inteligentes**, sin servicios de anonimato, para configurar tarjetas de crédito o tarjetas de débito no sólo no resuelve el problema de la vigilancia social, sino que lo magnifica, debido a que facilitaría aún más el establecimiento de registros informáticos, con el enorme peligro que ello conlleva de pérdida de privacidad.)

Otro aspecto importante para caracterizar estos escenarios es el relacionado con la naturaleza de las partes que intervienen en las transacciones. Básicamente podemos considerar dos tipos:

a) Transacciones de compraventa en las que interviene una entidad *cliente* y una entidad *vendedora.*
b) Transacciones o transferencias de fondos entre ciudadanos.

A efectos de necesidades de anonimato, estas últimas no tienen ese requisito, ya que lo normal es que sean nominales. Aunque algunos sistemas, como es el caso de *Mondex* *, que utilizan tarjetas inteligentes como tarjetas de pago, contemplan esta posibilidad de intercambio de fondos entre tarjetas, aquí **nos centraremos en escenarios cliente-vendedor,** que es en los que tiene interés la provisión de anonimato.

Un tercer aspecto a tener en cuenta tiene que ver con la forma en que la entidad cliente accede a la red telemática en la que se sustenta el sistema de pago. Para el caso que nos ocupa, el cliente puede acceder:

a) Mediante una tarjeta inteligente especialmente adaptada a las necesidades del sistema que actúe ante él como un testigo de seguridad reconocible y resistente ante manipulaciones. En este caso, la tarjeta puede contener (además de la clave privada del cliente que le servirá de respaldo en las operaciones de firma digital) otras claves o datos de la aplicación e incluso determinados algoritmos específicos. La tarjeta inteligente puede facilitar grandemente la autenticación mutua entre la entidad cliente y el sistema global.
b) Directamente a partir de los sistemas informáticos de que disponga el cliente, de forma que las claves, los datos y los algoritmos que le permiten acceder al sistema están contenidos y programados en sus propios recursos computacionales y tanto la custodia como la exactitud de esa información está bajo su exclusiva responsabilidad.

---

* *Mondex* (http:www.mondex.com) es un sistema de pago en el que el dinero está almacenado en tarjetas inteligentes.

De la propia redacción de ambas opciones se deduce que, aunque la opción reflejada en segundo lugar es perfectamente válida, la alternativa más interesante es la de acceder con testigos de seguridad especializados, es decir, **acceder sistemáticamente mediante tarjetas inteligentes**. Podríamos hablar en ese caso de *tarjetas monedero anónimas* o de *tarjetas de débito anónimas* o de *tarjetas de crédito anónimas* o, de forma genérica, de *tarjetas de pago anónimas*. Lo que ocurre es que, debido a las posibilidades que ofrecen las redes telemáticas y los servicios de seguridad, estas tarjetas pueden tener, como veremos más adelante, un comportamiento mucho más parecido al dinero en metálico que el que pueden ofrecer las tarjetas tradicionales de las cuales, por evolución, proceden.

Otro aspecto también relacionado con el acceso, que podemos considerar como un desglose de la opción que acabamos de catalogar como a), es el relativo al terminal de acceso al sistema. Si partimos de que la persona que actúa como cliente lo hace mediante su tarjeta inteligente, será necesario, obviamente, que el terminal de acceso disponga de un dispositivo de lectura-escritura (CAD) para este tipo de componentes. No obstante, cabría contemplar dos alternativas:

a1) El terminal de acceso puede ser un computador cualquiera que disponga de un CAD para comunicarse con la tarjeta. En ese computador deberá residir el programa correspondiente a la Aplicación Cliente que se haya diseñado en ese sistema de pago.

a2) El terminal de acceso es un subsistema especialmente diseñado para servir de intermediario con la tarjeta inteligente del cliente. Lo razonable es que esté desarrollado sobre un computador de reducidas prestaciones pero de forma que sea resistente a manipulaciones (*tamper resistant*), es decir, que ni los programas ni los recursos que gobierna puedan ser alterados fraudulentamente.

Aunque la primera puede ser perfectamente válida, es fácil colegir que es la segunda alternativa la que ofrece más posibilidades a los diseñadores de la aplicación global. En efecto, si se dispone de un **terminal de acceso específico**, podrán asignársele algunas de las funcionalidades del sistema que, de forma conjunta, garantizan el anonimato y la seguridad del conjunto global.

Un último aspecto que vamos a tener en cuenta (dentro de muchos otros que sería posible considerar) es el referido a la «distancia» entre el comprador y el vendedor. Es un error bastante extendido el considerar que la principal aplicación de pago con dinero digital a través de redes telemáticas es la que se produce cuando el comprador se encuentra en un sitio remoto y separado, por tanto, del vendedor. Es decir, se trataría típicamente de una compra que se hace desde el domicilio a través de Internet. Esta acepción excluiría, o dejaría en un segundo plano, a las transacciones comerciales que se realizan *in situ,* es decir, en el propio establecimiento del vendedor.

Por contra, la mayoría de las operaciones que se realizan con las tarjetas de crédito, que tanto desasosiego y atención despiertan en los investigadores sociales, se realizan de forma «presencial» en los propios locales del vendedor. Si bien es cierto que determinados productos como libros, discos, material informático, etc., se prestan a la compra remota, la compra de muchos otros requiere (al menos dentro de la cultura en que nos hallamos) tener a la vista, y al tacto, la mercancía que se desea adquirir. (En este sentido, la experiencia de los Estados Unidos, con mucha costumbre previa de compra por correo y una mentalidad muy especial, no es transportable a otras latitudes.) Por todo ello, si se consiguiera sustituir las transacciones convencionales

mediante tarjetas de crédito por otras en las que se respetase el anonimato del comprador, se habría dado un paso de gigante de cara a respetar las garantías de privacidad de los ciudadanos.

De cara a la tipificación de escenarios que venimos abordando, la compra *in situ* facilitaría la implantación de **terminal de acceso específico** en los puntos de venta, en tanto que la compra remota a través de Internet lo dificultaría grandemente. No obstante, es factible concebir un sistema en el que todos los participantes afiliados dispongan de un terminal especialmente diseñado para ese sistema. Un sistema que contempla esta alternativa es el sistema *Mondex* antes citado, en el que se proporciona a sus miembros un pequeño terminal «de bolsillo» con lector de tarjeta, teclado y pantalla incluidos.

En resumidas cuentas, de lo que hemos venido comentando en los párrafos precedentes se deduce que, combinando distintas opciones para distintos aspectos, pueden establecerse escenarios muy diversos. No obstante, sin desdeñar ninguna otra alternativa, podríamos seleccionar lo que podríamos llamar un «escenario interesante» (conforme está representado en la Figura 11.13) cuya constitución sería de la siguiente forma:

- *Cliente*. Es la persona que desea realizar la compra. Deberá tener cuenta corriente o cuenta de crédito en el *banco* integrado en el sistema.
- *Tarjeta de pago anónima*. Es una tarjeta inteligente especialmente adaptada a las necesidades del sistema. Actúa ante él como un testigo de seguridad reconocible y resistente ante manipulaciones (*tamper resistant*). Además de la clave privada del Cliente, contendrá otras claves o datos de la aplicación y, en algunos casos, podrá ejecutar determinados algoritmos específicos.
- *Terminal de acceso al sistema*. Se trata de un terminal especialmente diseñado, instalado en los puntos de venta, que dispone del correspondiente CAD para establecer comunicación con la *tarjeta de pago anónima*. Tendrá asignadas algunas de las funcionalidades del sistema que ayuden a garantizan el anonimato y la seguridad del conjunto global. Estará desarrollado sobre un computador de reducidas prestaciones y será resistente a manipulaciones.
- *Vendedor*. Es el titular de la *tarjeta inteligente de punto de venta* con la que se tiene acceso y se gobierna el *terminal de acceso al sistema*, interactuando, llegado el caso, con la *tarjeta de pago anónima*.

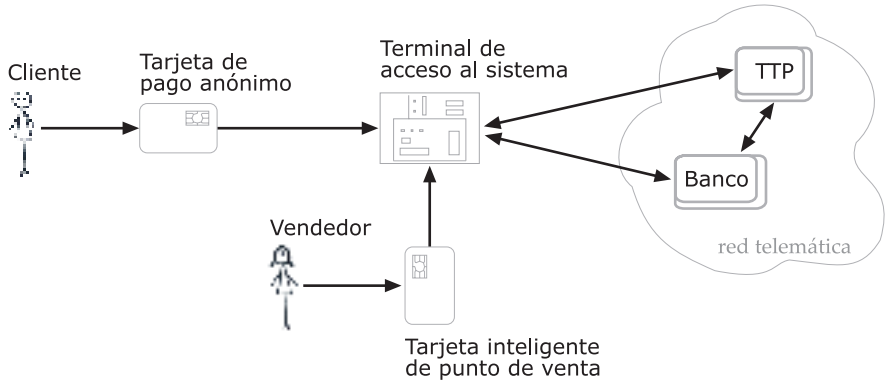

Figura 11.13. Un escenario «interesante» para dinero digital con anonimato.

- *Banco (o Central de Autorización)*. Es la entidad bancaria que reconoce el dinero digital manejado en el sistema y que está habilitada para deducir fondos de la cuenta del comprador e ingresarlos en la cuenta del Vendedor.
- *Tercera parte de confianza*. Es una entidad que puede aparecer de forma optativa. Caso de estar presente, puede servir para facilitar el comportamiento del sistema en cuanto a la provisión del necesario anonimato y/o actuar como garante en caso de un uso indebido del sistema.

Un escenario tal como este podría permitir, utilizando dinero digital, un comportamiento equivalente al que tiene lugar usando dinero en efectivo. De forma muy general, podríamos resumirlo diciendo que el banco *sabe cuánto se gasta* la persona que realiza las compras, pero *no sabe ni en qué ni dónde*, y el Vendedor sabe que *recibirá el dinero* equivalente al bien que cede, pero *no sabe quién es* la persona que compra ese bien. En el siguiente apartado trataremos de caracterizar más pormenorizadamente esta idea.

El escenario de la Figura 11.13 está adaptado al caso en el que la compra se realiza *in situ* y el terminal de acceso está ubicado en el punto de venta. No obstante, es adaptable de forma inmediata al caso en el que la compra sea remota y el terminal de acceso esté al lado del Cliente pero no al alcance del Vendedor. En este último caso no existiría la tarjeta inteligente del Vendedor como elemento que gobierna el terminal de acceso e interactúa, en algunos casos, con la tarjeta del comprador.

CARACTERÍSTICAS DEL DINERO DIGITAL ANÓNIMO

Como hemos dicho, el dinero en efectivo siempre es anónimo. Por ello, cualquier proyección digital de los mecanismos de pago debería preservar algún tipo de anonimato del comprador. Podemos distinguir al menos ocho características [Carr02] que sirven para catalogar un sistema anónimo de pago usando dinero digital:

1. **Verificabilidad** (*verifiability*). Todo participante en una transacción monetaria digital debe ser capaz de verificar el valor del dinero recibido y su autenticidad, lo que conlleva identificar a la entidad financiera emisora.
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 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. **Transferibilidad** (*transferability*). El dinero recibido puede a su vez ser utilizado por el Vendedor para realizar él mismo otras compras o transacciones, además de aquella que le permite el ingreso de esos fondos en su cuenta del banco.
6. **Divisibilidad** (*divisibility*). Quien recibe una cantidad de dinero electrónico está capacitado para transferir a terceros el total o solamente una parte de esos fondos.
7. **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.

8. **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.

De esas ocho características, que se corresponderían punto por punto con la plasmación en la Red del dinero en efectivo (*digital cash*), podemos afirmar que:

- Las cuatro primeras son imprescindibles para que el sistema pueda ser considerado de pago con anonimato.
- Las tres siguientes, *transferibilidad*, *divisibilidad* y *devolución de cambio*, son complementarias y útiles. Pero un sistema puede considerarse eficaz y robusto sin necesidad de soportarlas.
- La clasificada en octavo lugar, *pago sin conexión*, es menos importante. En algunos casos podría ser de utilidad porque es una propiedad que tiene el dinero en metálico. No obstante, no aparece recogida en el escenario que hemos considerado «interesante», el cual está focalizado al caso del uso de las redes telemáticas para realizar pagos mediante tarjetas inteligentes. Cabe observar, por otra parte, que, actualmente, en el uso convencional de tarjetas de crédito, los puntos de venta ya están mayoritariamente conectados telemáticamente con las entidades bancarias.

Entre las cuatro imprescindibles, la *irrastreabilidad* aparece diferenciada del *anonimato* porque puede que el banco, al expedir el dinero, no tenga forma de conocer dónde se ha gastado ese dinero (anonimato), pero sea capaz de buscar relaciones entre ambas operaciones. Por ejemplo, supongamos que en una fecha concreta a una hora concreta se va a realizar una compra de combustible en una gasolinera por valor de 50,12 euros. Cuando el comprador solicite ese dinero al banco, aunque el sistema garantice que la operación es anónima (el banco no podrá conocer ni la hora, ni la identidad del Vendedor, ni la mercancía que se compre con ese dinero), 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 50,12 sería fácilmente relacionable con ambas operaciones. Por tanto, para conseguir la *no rastreabilidad* será necesario diseñar las cosas para que una situación como la que acabamos de describir no sea factible. Una posible solución sería fraccionar las reservas de dinero o fraccionar los pagos.

En el escenario que se recoge en la Figura 11.13, la *transferibilidad* representaría que el dinero que paga el Cliente pudiera almacenarse en algún elemento del entorno del Vendedor, por ejemplo en su *tarjeta inteligente de punto de venta*, y que el Vendedor pudiera más tarde utilizarla como *tarjeta de pago anónima* ante otro Vendedor.

En ese mismo escenario, la *divisibilidad* significaría que cuando el Cliente, al comunicarse con el banco a través del terminal de acceso, obtuviese una cierta cantidad de dinero y la guardase, por ejemplo, en su *tarjeta de pago anónima*, tuviese la posibilidad de gastar solamente una parte de él reservando el resto para otra ocasión. De otra parte, la *devolución de cambio o vuelto* (que es una característica menos aprovechable que las dos antes descritas) lo que podría representar en ese escenario es que, por ejemplo, desde la *tarjeta de pago anónima* se pudiese pasar al entorno del

Vendedor una cantidad de dinero y desde este último se le pudiese hacer una transferencia de fondos en sentido inverso.

11.4. MECANISMOS Y PROTOCOLOS PARA CONSEGUIR DINERO DIGITAL ANÓNIMO

Como ya hemos dicho antes, el escenario representado en la Figura 11.13 es uno de tantos que pueden establecerse, aunque nosotros lo hayamos seleccionado por entender que reúne los elementos más interesantes de cara a la evolución que han de experimentar en un futuro los sistemas de pago con anonimato. A pesar de su falta de generalidad, nos ha servido hasta aquí para explicar las características de este tipo de sistemas y nos servirá en el presente apartado para discutir acerca de los mecanismos y protocolos que pueden establecerse para conseguir ese comportamiento.

Antes comentamos que no vamos a tratar de describir las distintas aplicaciones y propuestas que se han venido realizando acerca de los medios de pago anónimos. Del mismo modo, tampoco vamos a abordar aquí un análisis del estado del arte en relación con este tipo de propuestas [7].

Lo que sí haremos es analizar por partes los principales problemas que se presentan y tratar de ver cómo se solucionan en dos propuestas prácticas distintas [8], compatibles con el escenario representado en la Figura 11.13, que vamos a denominar respectivamente *Sistema1* y *Sistema2*. A medida que avancemos en la explicación iremos añadiendo alguna de las particularidades de ambos sistemas.

FORMATO DEL DINERO DIGITAL

Aunque es viable imaginar muchas formas distintas de representar el dinero digital que el Cliente necesita obtener del banco para realizar la compra, cabe seleccionar dos de ellas bastante diferentes entre sí. Una de ellas consiste en considerar este dinero como un documento digital en el que figura la cantidad total y está firmado por el banco: una especie de pagaré al portador. La otra es considerarlo descompuesto en un conjunto de billetes digitales firmados individualmente por el banco.

En el Sistema2 se trabaja con la primera de estas dos representaciones, más próxima al concepto de dinero manejado en las tarjetas de crédito o de débito. Para entendernos, a esa cantidad de dinero obtenido por el Cliente vamos a denominarla *autorización*. En principio, vamos a suponer que el formato que tendrá será el de un documento en el que figura un identificador único y la cantidad total de dinero, todo ello firmado por el banco. A ese identificador lo denominaremos Número de Identificación de la Autorización (NIA). Este número será elegido al azar por el Cliente y tendrá un número de bits suficientes como para garantizar que la probabilidad de repetición sea muy baja.

La segunda opción consiste en la definición de un conjunto de *billetes digitales*, cada uno representando un valor monetario distinto. Por ejemplo, 1 euro, 2 euros, 5 euros, 100 euros, etc., y sus correspondientes valores decimales. El valor monetario del billete está determinado por la clave privada monetaria con la que lo firme el Banco. Para ello, el Banco dispone de tantos pares de claves (pública y privada) como valores de billetes sean puestos en juego. En el Sistema1 será ésta la representación elegida y cada billete concreto será un documento digital con un valor monetario y con un identificador único al que denominaremos Número de Identificación del Billete

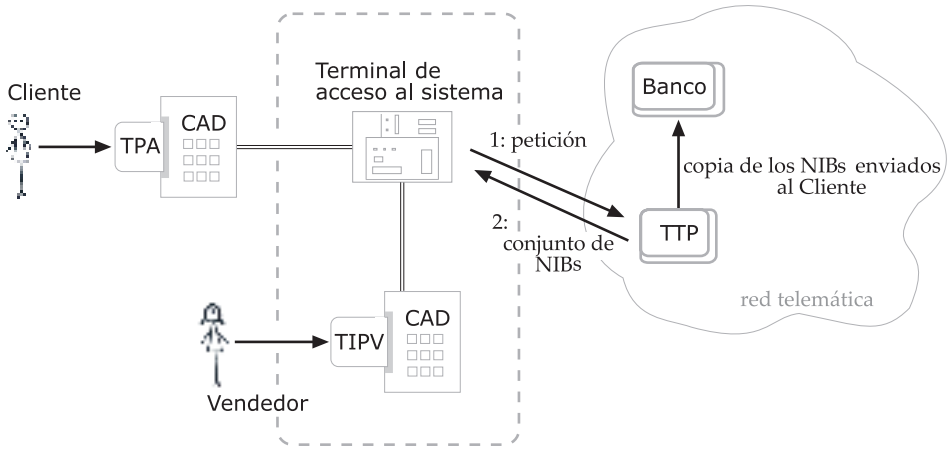

Figura 11.14. Solicitud de identificadores de billetes en Sistema1.

(NIB). Estos identificadores son generados por una TTP y entregados, a petición del Cliente, tanto a su *tarjeta de pago anónimo* (a la que, para abreviar, denominaremos TPA) como al Banco, en las condiciones que más adelante detallaremos.

En la Figura 11.14 se representa este intercambio de información. Como puede observarse, la TTP es parte imprescindible en el funcionamiento del Sistema1. Es como si lo que hiciese la TTP es enviar a la tarjeta billetes en blanco sin valor monetario y sin firmar, y al Banco le manda la relación de los identificadores que ha distribuido. En cambio, la estructura del Sistema2 sería casi igual a la representada en esta figura, pero sin la presencia de la TTP. Como veremos más adelante, el prescindir de la TTP simplifica el sistema pero obliga a que los protocolos sean más complejos.

LA FIRMA DEL DINERO POR PARTE DEL BANCO

El proceso de compra comenzaría de forma similar tanto si la operación se hace sobre el Sistema1 como si se hace sobre el Sistema2. Más o menos sería:

1. El Cliente elige una serie de productos.
2. El Cliente introduce su tarjeta (TPA) en el CAD. Se produce una autenticación mutua entre la TPA y el terminal de acceso al sistema.
3. El Cliente se autentica ante su TPA mediante un PIN o prueba biométrica.
4. El Vendedor a través del terminal le indica a la TPA la cantidad de dinero a pagar.

Esto es así suponiendo que todo vaya bien. Obviamente, si alguno de los pasos falla, se interrumpe el proceso. A partir de aquí, la tarjeta tendrá que comunicarle al Banco la cantidad a pagar y éste tendrá que firmar ese dinero para que posteriormente la tarjeta del Cliente se lo entregue al terminal de venta.

a) Hay que convencer al Banco para que firme

Como la representación del dinero es diferente en Sistema1 que en Sistema2, el proceso seguido para obtener la firma a ciegas del Banco no será igual en ambos.

Veamos cómo se comportaría el Sistema1:

1. La tarjeta TPA selecciona de entre los billetes en blanco que tiene almacenados la cantidad necesaria para hacer frente al pago.
2. La tarjeta incorpora un elemento de opacidad distinto en cada billete (véase apartado de firma a ciegas) para que los identificadores NIBs no sean visibles, y se los envía al Banco, indicándole, en claro, el valor monetario de cada uno de ellos.
3. El Banco comprueba la disponibilidad de fondos del Cliente y realiza una firma a ciegas sobre los NIBs opacados recibidos, cada uno con la clave privada monetaria que le corresponda. Descuenta el dinero de la cuenta del Cliente * y le envía los billetes firmados.
4. La tarjeta, tras verificar que lo recibido se corresponde con su petición y que la firma es correcta (dispone de las correspondientes claves públicas monetarias), retira la opacidad a los billetes y está lista para entregárselos al terminal del punto de venta.

Como veremos más adelante, el Vendedor, con la colaboración del terminal del punto de venta (con quien colabora la tarjeta inteligente del Vendedor), estará encantado de recibir estos billetes que puede reconocer como válidos, según detallaremos más adelante, verificando las firmas. Pero, ¿y el Banco? ¿Aceptará esta forma de proceder? Indudablemente, sí. Porque billete que firma, dinero que le descuenta al Cliente. Si la tarjeta del Cliente quiere engañar al Banco y en lugar de rellenar uno de los billetes en blanco (los NIBs) generados por la TTP le envía un número inventado, el Banco lo va a firmar igual (no puede ver el identificador) y lo va a descontar igual, pero será un billete inválido que el Cliente no podrá circular satisfactoriamente. Es decir, será una ganancia neta para el Banco porque le descuenta el dinero al Cliente y nadie podrá cobrar después ese «billete».

En el Sistema2, en cambio, la *autorización* (la cantidad de dinero que le va a pedir al Banco) va a llevar un número identificador que lo va a poner la propia tarjeta. Si le mandase al Banco la autorización opacada (de forma equivalente al punto 2 de la anterior secuencia) indicándole en claro el valor de esa cantidad de dinero, el Banco se negaría a firmar porque puede sospechar que la cantidad opacada sea superior a la cantidad de la que se le informa en claro.

¿Cómo convencerle? Una forma de hacerlo es asegurar que tanto la tarjeta del Cliente como el terminal del punto de venta están diseñados a prueba de manipulaciones (*tamper-proof*), por lo que la tarjeta va a seguir el algoritmo que tiene programado y, además, ninguna tarjeta puede ser falsificada y ninguna tarjeta falsa va a ser reconocida por el terminal. Este es un buen argumento que también vale para el caso del Sistema1, pero sería conveniente que introdujésemos un elemento primario de confianza basado en el protocolo seguido y en los mecanismos criptográficos.

---

* 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 lo descuenta de la cantidad de pago aplazado que tenga pactado y anota la operación, que le será facturada a fin de mes o en la fecha previamente acordada. En lo sucesivo, para simplificar, diremos que «lo descuenta» queriendo significar ambos casos.

Una forma de proceder podría ser la siguiente:

1. La tarjeta TPA genera n candidatos de autorización, todos ellos con la misma cantidad de dinero pero cada uno de ellos con un número de identificación (NIA) distinto.
2. La tarjeta incorpora un factor de opacidad distinto en cada candidato a autorización, y se los envía al Banco, indicándole, en claro, el montante de la cantidad pedida.
3. El Banco, que no puede ver ninguno de los candidatos opacados, selecciona al azar n –1 de ellos y se los devuelve a la tarjeta del Cliente, apartando uno de los candidatos recibidos.
4. La tarjeta del Cliente (TPA) le envía al Banco los factores de opacidad que utilizó para oscurecer esos n –1 candidatos.
5. El Banco retira la opacidad a esos n –1 candidatos y comprueba que todos ellos estaban generados con la misma cantidad de dinero (la que aparece en claro en la petición). Entonces, el Banco se fía de que el candidato restante también está generado por esa misma cantidad. El Banco comprueba la disponibilidad de fondos del Cliente y realiza una firma a ciegas sobre el candidato que permanece opaco. Descuenta el dinero de la cuenta del Cliente y le envía la autorización firmada.
6. La tarjeta, tras verificar que lo recibido se corresponde con su petición (dispone de la clave pública del Banco), retira el factor de opacidad de la autorización y está lista para entregársela al terminal del punto de venta.

A cambio de no usar una TTP hay que soportar el peso de un protocolo más complejo y con más intercambios de datos. Puede quedar la duda, razonable a primera vista, de que siempre existirá la probabilidad de que el Cliente engañe al Banco rellenando n – 1 candidatos con una cantidad pequeña y el restante con una cantidad sustancialmente mayor. Si tiene la suerte de que es ese candidato el que el Banco aparta, el fraude está servido. Según esto, para reducir esa probabilidad habría que elegir un valor de n razonablemente grande, con la carga que eso acarrea.

Analizado desde un punto de vista estrictamente «protocolario» así parece que son las cosas, pero una reflexión más detenida ayuda a matizar la cuestión. En efecto, supongamos que n es bastante pequeño, por ejemplo 5, lo que supone que existe un 20 por 100 de posibilidades de perpetrar el fraude. Pero aquí no estamos pensando en juegos criptográficos sino en sistemas que cumplan con las exigencias de lo que en el Capítulo 1 hemos caracterizamos como Seguridad Cívica, esto es, sistemas que sirvan para que los ciudadanos puedan tener en la Red razonablemente protegidos sus derechos y garantizada su privacidad. En el caso que nos ocupa, para poder realizar compras sin ser vigilado y clasificado.

Por eso, caso de implementarse este hipotético Sistema2 se haría limitando el valor máximo de las transacciones[9]. Entonces, caso de que un ciudadano se afilie a él y pague la correspondiente cuota de alta y desee usarlo regularmente y por mucho tiempo, el jueguito del fraude le costaría caro. Le costaría lo que cuesta falsificar la tarjeta (muchísimo) y la suerte le duraría poco porque la ruleta rusa del 20 por 100 iría estrechando los márgenes de la suerte cada vez que pruebe con una compra nueva, y la primera vez que sea descubierto se le expulsaría del Sistema2 para los restos, y se quedaría con su pequeño fraude, y perdería su cuota de afiliación, y se quedaría sin hacer lo que realmente quería: hacer pagos de forma anónima para que no lo vigilen los poderes económicos.

En resumen, tanto en el esquema de comportamiento del Sistema1 como en el del Sistema2, como en muchos otros existentes, es factible, con ingenio y estableciendo garantías, convencer al Banco para que firme un pagaré cuyo contenido no ve.

Una última cosa hay que comentar acerca de los sistemas que, como el Sistema2, no hacen uso de una TTP. Si el mecanismo de firma opaca es muy robusto y se sospecha que se está produciendo un uso del sistema para fines delictivos, no existe manera de descubrir al infractor. Para descubrir al infractor puede usarse un esquema de firma a ciegas arbitrada por una entidad juez como el representado en la Figura 11.5. En este caso se podría incorporar también una TTP al Sistema2 que no intervendría en el proceso normal del protocolo salvo que por decisión judicial (o bajo normas pactadas entre todos los afiliados al sistema) se decidiese romper el anonimato de la firma.

EL PROBLEMA DE LA REUTILIZACIÓN DEL DINERO

Uno de los problemas inherentes a los sistemas de pago con dinero digital es que pueda existir la posibilidad de utilizarlo más de una vez. No se olvide que este tipo de dinero está representado, de una u otra forma, en una pieza de información que se puede copiar cuantas veces se desee. A tenor de lo descrito hasta aquí, tanto el Sistema1 como el Sistema2 previenen de este doble uso aunque con alguna deficiencia.

b) Hay que evitar que el dinero firmado se use más de una vez

Veamos en primer lugar cómo continuaría el proceso de entrega de billetes en el Sistema1 una vez que se han recibido correctamente firmados en la tarjeta del Cliente (TPA). El proceso seguiría así:

a) La tarjeta, una vez comprobada la validez de los billetes recibidos, selecciona los billetes necesarios para satisfacer el precio de la mercancía que está adquiriendo y se los entrega al Vendedor a través del terminal del punto de venta.
b) El terminal hace una primera comprobación del formato de los billetes verificando la corrección de las firmas del Banco. No puede saber si los identificadores de billete (NIBs) son correctos antes de consultarlo con el Banco.
c) Si las anteriores comprobaciones resultan favorables, el terminal envía al Banco una solicitud de ingreso de los billetes que ha recibido del Comprador.
d) El Banco verifica la validez de los billetes comprobando que han sido firmados con las claves privadas monetarias correspondientes y que los NIBs están en la lista de NIBs válidos remitida por la TTP **y que no han sido usados previamente.** 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 terminal del punto de venta del resultado de la operación.
e) Si el resultado es favorable, el terminal avisa al Vendedor para que entregue la mercancía al Cliente y le entrega a la tarjeta TPA un comprobante firmado de la operación, dando por finalizado el proceso.

Es decir, el Banco detectará claramente el intento de cobro indebido de un billete usado pero no sabe si es que ha sido el Cliente (manipulando su tarjeta) el que ha

querido pagar dos veces con los mismos billetes o ha sido el Vendedor el que (manipulando el sistema del punto de ventas del Sistema1) ha conseguido rescatar billetes usados.

El comportamiento del Sistema2 para la entrega del dinero desde el Cliente al Vendedor es bastante similar al descrito para el Sistema1, y vamos a obviar su descripción. En este caso, en el paso equivalente al punto d) anterior, el Banco una vez que ha hecho el ingreso al Vendedor por importe de la autorización que le ha presentado, lo que hace es grabar el número de identificación de esa autorización usada en una lista. Y lo primero que hace cuando el terminal del punto de venta le presenta una autorización es cotejar su identificador para comprobar que no había sido utilizada anteriormente. Por esta razón, igual que el Sistema1, detectará el intento de doble uso, pero, también al igual que el Sistema1, no sabrá quién ha sido el responsable del intento.

Una mejora del Sistema1 podría consistir en que cuando la TTP genere los identificadores de billetes (los billetes en blanco) les añada una cabecera con una fecha de caducidad. Eso permitiría al terminal del punto de venta almacenar en una base de datos los identificadores que ha recibido con anterioridad para detectar si el Cliente quiere endosarle de nuevo un billete usado en ese mismo establecimiento. Para que esta base de datos pueda tener un tamaño manejable, el periodo de validez de los billetes no debe ser muy amplio (el cliente puede obtener nuevos NIBs de la TTP cuando le haga falta). De esa manera, todos los billetes pagados pero pasados de fecha pueden ser borrados de esa base de datos.

Conforme a esto, el comportamiento descrito anteriormente en el punto b), pasaría a ser el siguiente:

b) El terminal hace una primera comprobación del formato de los billetes verificando la corrección de las firmas del Banco y comprobando las fechas de caducidad. Comprueba además, consultando su base de datos, que esos NIBs no han sido ingresados antes en este terminal de punto de venta. No puede saber si los identificadores de billete (NIBs) son correctos antes de consultarlo con el Banco.

De esta forma, el Vendedor puede detectar si el Cliente trata de cometer fraude y rechazaría la venta, aunque no puede identificar al presunto estafador (aunque el terminal del punto de venta sí puede quedarse con su tarjeta y no devolverla hasta que se den determinadas circunstancias previamente pactadas). Por eso, si el que consigue enviar al Banco un billete usado es el mismo Vendedor a través de su terminal, el Banco detectaría la duplicación y le achacaría el intento de fraude. Si un Cliente consiguiese entregar un billete ya usado anteriormente en otro terminal de ventas distinto, el proceso prosperaría hasta llegar al Banco, que detectaría que había sido ya cobrado por otro comerciante, con la posible punición del Cliente que ello conllevaría.

Para trasladar una mejora equivalente al Sistema2 podría exigirse que cuando la tarjeta del Cliente genere el número de identificación de la autorización, le añada una cabecera con la fecha del día en que se hace la solicitud al Banco. De esa forma puede establecerse un periodo de validez limitado para las autorizaciones firmadas. También en este caso se dotaría al terminal de venta de una base de datos donde almacenase las autorizaciones que ha tramitado y las borrase cuando hayan caducado. Gracias a ello, de forma similar a lo que hace el Sistema1, el terminal podrá detectar el intento de doble uso (si ha sido en su mismo establecimiento) y el Banco, además de detectarlo, podrá atribuir al Cliente o al Vendedor la responsabilidad del intento.

EL PROBLEMA DE LA RASTREABILIDAD

Tal y como hemos descrito hasta ahora, del comportamiento tanto del Sistema1 como del Sistema2 se podrían establecer relaciones entre las operaciones de obtención de dinero (billetes en un caso, autorizaciones en el otro) y el pago de esa cantidad al Vendedor (recuérdese el ejemplo del pago de 50,12 euros en una gasolinera, que comentamos en el apartado *Características del dinero digital anónimo* al hablar de la *irrastreabilidad*).

c) Hay que evitar que los pagos sean rastreados

Para evitar ese riesgo, la solución, tanto en el Sistema1 como en el Sistema2, es no pedir nunca al Banco la cantidad exacta que se necesita pagar al Vendedor. Para eso la tarjeta del Cliente tiene que tener capacidad de almacenar dinero ya firmado y calcular qué cantidad debe solicitar para completar la suma requerida. En el Sistema2 lo que necesita la tarjeta es disponer de autorizaciones firmadas por valores intermedios y, en el momento de la compra, solicitar la cantidad necesaria para completar la cantidad exacta que tiene que entregarle al Vendedor.

En el Sistema1 esta operación es más fácil de llevar a cabo porque el dinero lo tiene dividido en billetes digitales. El algoritmo para calcular los billetes que la tarjeta necesita solicitar al Banco 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 tarjeta del Cliente, 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. Naturalmente, para incluir estos redondeos que evitan la rastreabilidad sería necesario cambiar el protocolo antes descrito, incluyendo nuevos pasos y modificando algunos otros.

d) Es necesario especificar muchos otros detalles

De lo antes descrito hemos podido conocer los elementos principales que están presentes tanto en Sistema1 como en Sistema2 para conseguir el anonimato de las operaciones de compra realizadas con la tarjeta de Cliente. Pero quedan muchos otros por aclarar. Por ejemplo, en el Sistema1 quedarían por discutir muchas otras cosas como puede ser la gestión de los identificadores, el almacenamiento de billetes para que se comporte como una tarjeta monedero, la posibilidad de obtener billetes en puntos específicos de carga además de los terminales dependientes de los vendedores, los mecanismos para evitar que el Banco conozca la dirección telemática desde la que se conecta la tarjeta del Cliente, y un largo etcétera.

Otro tanto podría decirse del que hemos denominado Sistema2 y de cualquier otro de los muchos sistemas que pudiésemos analizar. Además, quedaría por determinar las condiciones de seguridad (confidencialidad, integridad, etc.) en las que se lleve a cabo el intercambio de las PDUs que conforman los protocolos telemáticos que se establezcan a través de la red.

No obstante estas carencias, en los párrafos anteriores sí se han tocado los principales temas y los principales problemas presentes en el amplio y emergente asunto

de las transacciones comerciales de compraventa a través de redes telemáticas, en las que se considera conveniente mantener el anonimato del comprador para garantizar su privacidad.

11.5. VOTACIÓN TELEMÁTICA

Entre los pasos que se están dando de cara a la edificación paulatina de la Sociedad de la Información ocupan un lugar importante las propuestas relacionadas con procesos de votación a través de redes telemáticas. No es esta una tarea fácil porque los sistemas tradicionales de votación mediante papeletas, aunque adolecen de serios inconvenientes en cuanto a rapidez y flexibilidad, sí ofrecen unos mecanismos de salvaguarda y unos procedimientos organizativos muy seguros, que gozan, en general, de una valoración muy positiva por parte de los ciudadanos, lo que redunda en un nivel de confianza bastante alto. En su plasmación en entornos telemáticos será necesario no sólo emular las ventajas de estos sistemas sino superar tanto la seguridad como las prestaciones que pueden obtenerse. Y esto, desde un punto de vista tecnológico, no es tarea fácil.

Si bien es cierto que la existencia de votaciones no implica automáticamente la presencia de Democracia, sí que podemos afirmar que para la contribución a la Democracia mediante sistemas telemáticos (*Democracia Digital*) es imprescindible disponer de estructuras que posibiliten el voto en su doble acepción de elección entre alternativas predeterminadas y de participación de los ciudadanos en las decisiones colectivas. La primera de ellas, a imitación de los esquemas de votación construidos en los últimos siglos, consiste en la elección de representantes o en la decisión entre opciones alternativas previamente planteadas. La segunda servirá para dar soporte a modelos en los cuales los miembros de una comunidad estén capacitados para proponer, discutir y consensuar alternativas que afecten a la gestión y organización de recursos que les son comunes (ya sean de carácter político, económico, culturales, etc.).

El presente epígrafe y el siguiente estarán orientados al análisis y posibles soluciones de sistemas que den satisfacción a la primera de las dos acepciones de votación planteadas en el párrafo anterior, que es la que aparece más insistentemente en las propuestas planteadas actualmente (quizás por su carácter emulativo de procesos convencionales). La segunda de ellas será discutida de forma genérica en el epígrafe 11.8, al hablar de las plataformas que facilitan la Democracia Digital.

DEL VOTO ELECTRÓNICO AL VOTO TELEMÁTICO

Aunque las primeras referencias al término *voto electrónico* proceden de mediados de los años sesenta, que fue cuando por primera vez se utilizaron computadores para realizar ciertas tareas relacionadas con procesos electorales, ha sido en la década de los noventa cuando con más insistencia han aparecido propuestas y se han llevado a cabo experiencias que han merecido tal calificativo. No obstante, el término *voto electrónico* ha venido empleándose para identificar sistemas de votación de naturaleza muy diversa en los que las garantías de seguridad requeridas en los procedimientos de autenticación, emisión del voto y recuento son proporcionadas de muy diferentes formas [10]. Con objeto de clarificar adecuadamente toda esta gama diversa de sistemas, conviene hacer una tipificación [GoCa03] que nos permita distinguir las características principales de cada uno de ellos.

Conforme a esta clasificación, en el **primer nivel** estaría lo que podemos denominar el ***escenario clásico*** de votación con algunos elementos automatizados. En este escenario se englobarían tanto las votaciones mediante papeletas como aquellas que se sirven de tarjetas perforadas o de lectores ópticos. Estas experiencias no pueden ser consideradas como un sistema de voto electrónico propiamente dicho, pero hasta ahora han sido una referencia para los distintos escenarios electrónicos que se han propuesto.

En un **segundo nivel** se encontrarían los escenarios de votación que, basándose en la forma de operar del método convencional mediante papeletas, sustituyen alguno de sus elementos físicos y procedimientos manuales por algún tipo de sistema o de proceso electrónico. Estos sistemas serían los que podemos denominar propiamente como sistemas de ***voto electrónico***. Entre estos posibles sistemas tenemos aquellos que utilizan alguno o varios de los siguientes elementos: tarjetas magnéticas (para autenticar al votante o incluso para emitir el voto), urna electrónica (para la recepción y recuento de votos), pantalla (tablero) de votación (para seleccionar la opción de voto elegida), cabina electrónica (para depositar el voto), computadores con programas de distintos tipos (para el proceso de escrutinio).

En todos estos escenarios, de lo que se trata es de automatizar alguno de los procesos que se llevan a cabo en la votación convencional mediante papeleta. Podemos sintetizarlos en tres: el primero es el de la autenticación del votante, el segundo es el proceso de votar propiamente dicho y el tercero, todo lo relativo a la gestión y procesado del contenido de la urna electoral. Casi la totalidad de las experiencias y actuaciones gubernamentales encaminadas a la automatización de los procesos de votación en los distintos países democráticos se encuadran en este nivel.

Un **tercer nivel** más avanzado en la automatización del proceso de votación sería el determinado por los sistemas de votación que hacen uso de las redes telemáticas y de agentes telemáticos a los que se accede de forma remota. Al voto llevado a cabo bajo estos escenarios es al que podríamos denominar como ***voto telemático***. De esta manera, dejando el término de *voto electrónico* para designar a los sistemas que hemos clasificado en el segundo nivel, ganamos en claridad y en precisión. En los sistemas de voto telemático, la urna no se encuentra a la vista del votante (caso del voto electrónico antes citado), sino que es un agente telemático ubicado físicamente en un lugar remoto, al igual que el resto de los agentes que intervienen en la supervisión del sistema.

Aquí podríamos distinguir dos grupos: aquellos que utilizan las redes telemáticas (públicas o privadas) para la interconexión de los distintos colegios electorales, o bien los que proponen la votación desde casa (normalmente a través de Internet). En los escenarios del primer grupo, el elector tiene que desplazarse hasta lugares predeterminados (equivalentes a colegios electorales) para emitir su voto. El uso de redes telemáticas para la interconexión de esos «colegios electorales» por parte de un organismo encargado de la supervisión final (con un papel equivalente al que en España desempeña la Junta Electoral Central) permitiría una rápida recolección de los datos y la publicación de los resultados.

El segundo grupo, **votación desde casa** a través de Internet, es el más atractivo desde un punto de vista tecnológico, debido a los retos técnicos y de seguridad que plantea (venta de votos, coacción, monitorización clandestina, denegación abusiva del derecho a voto y entrega de resultados finales oficiales distintos de los verdaderos). Pero, a su vez, desde un punto de vista sociopolítico, plantea serios interrogantes debidos, en gran parte, al problema que representa el que no todo el mundo tenga las mismas oportunidades de acceso.

Para que las propuestas de sistemas de voto telemático lleguen a tener aceptación por parte de los ciudadanos deberán, al menos, ofrecer las mismas garantías que nos

brinda el sistema tradicional de voto, que, entre otras cosas, permite llevar a cabo un recuento visible de los votos y una revisión manual del proceso. No obstante, a la hora de diseñar nuevos esquemas de votación con soporte telemático es conveniente no limitarse simplemente a emular los procesos convencionales ni ceñirse a sus restricciones, sino aprovechar los recursos que nos brindan las nuevas tecnologías para conseguir sistemas aún más seguros, robustos y flexibles que sus precursores. De la determinación de los requisitos que deberían cumplir los sistemas de este tipo es de lo que trata el siguiente apartado.

DETERMINACIÓN DE REQUISITOS PARA LA VOTACIÓN TELEMÁTICA

En la Figura 11.15 se propone una estrategia para determinar adecuadamente cuáles son los requisitos necesarios para que un sistema de voto telemático cumpla con las demandas sociales, políticas y jurídicas exigibles a unos sistemas que pretenden cubrir actividades tan sensibles para la democracia como son aquellas que sirven para que los ciudadanos ejerzan su derecho al voto.

Huyendo de posturas tecnocéntricas, tan fáciles de encontrar en esta como en otras actividades relacionadas con el diseño de sistemas para la Sociedad de la Información, se propone aquí la colaboración multidisciplinar con el objetivo conjunto de diseñar sistemas que satisfagan las necesidades sociales de los ciudadanos y garanticen los derechos democráticos jurídicamente reconocidos.

En primer lugar se propone una actividad, a la que hemos denominado *Análisis teórico*, en la que se debería analizar qué se debe y qué se puede hacer desde un punto de vista tanto tecnológico como jurídico y sociopolítico. Para ello se partirá de la demanda concreta bajo la que surge el sistema que se quiere desarrollar y de los conocimientos previos que poseen las personas que llevan a cabo ese análisis. Como resultado, se deberá obtener una lista de requisitos exigibles al sistema. En esta actividad se deberán evaluar las posibilidades que ofrecen los protocolos y los mecanismos de seguridad en redes, así como los condicionantes jurídicos existentes (o las modificaciones legales que conllevaría asumir ciertos requisitos) y la determinación sociológica (preferentemente a través de estudios de campo) de las expectativas y temores que tiene la ciudadanía en relación con la implantación de este tipo de sistemas de votación.

En segundo lugar, a través de una *Investigación social*, esos requisitos previamente detectados deberían ser evaluados de cara a detectar la aceptación y la usabilidad del sistema. Ello permitiría matizar los requisitos previamente detectados, encontrar otros nuevos y evaluar la importancia relativa que la ciudadanía otorga a cada uno de ellos.

Teniendo en cuenta los requisitos así detectados y evaluados, se reduce el riesgo de que los ciudadanos presenten rechazos y temores una vez que se haya diseñado el sistema. En la Figura 11.15 se ha querido representar que la fase de diseño puede dar comienzo una vez se haya obtenido una primera relación de requisitos, aunque posteriormente deban ser tenidas en cuenta las mejoras y matizaciones derivadas de la investigación sociológica.

Por último, en el diagrama que estamos comentando, se ha recogido una fase de *Evaluación*, que preferentemente debería ser una demostración práctica del sistema con votantes reales, de la que se deduzcan defectos y se exploren nuevas posibilidades que deben ser incorporadas, de forma que se retoquen los requisitos que marcaron el diseño inicial, todo ello con objeto de obtener un sistema final más robusto y con mayor aceptación por parte de los ciudadanos.

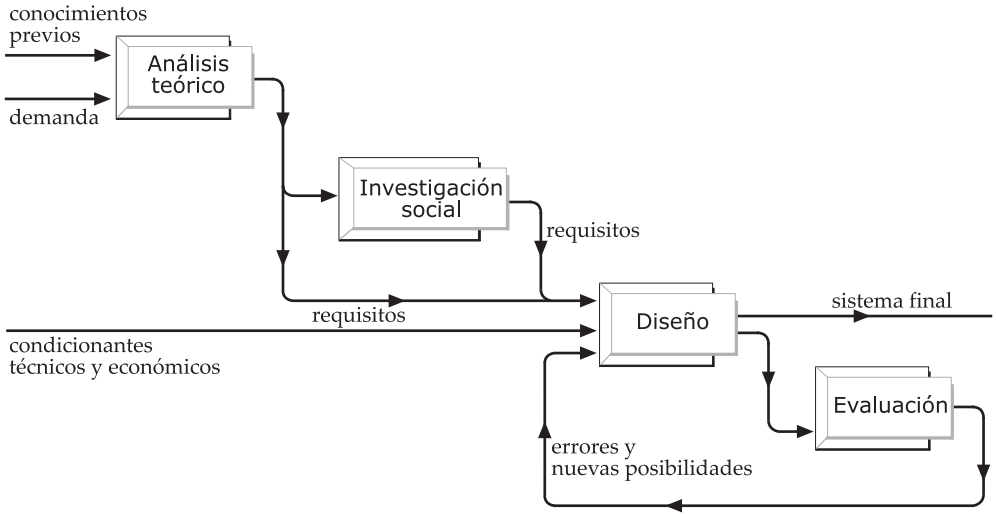

Figura 11.15. Determinación de requisitos para el diseño de un sistema de voto telemático.

Después de todo esto, es posible obtener una relación de requisitos que garantice, con bastante aproximación, que el sistema que los satisfaga cumplirá adecuadamente con todas las exigencias existentes y será bien aceptado por los ciudadanos. Apoyándonos en los resultados de una experiencia práctica realizada [11] bajo un esquema similar al recogido en la Figura 11.15, expondremos a continuación una *relación de requisitos* [CGMP02] exigibles a los sistemas de votación telemática. Es la siguiente:

1. ***Autenticidad*** o ***Autenticación***. Sólo los votantes autorizados pueden votar.
2. ***Acotabilidad*** o ***Singularidad*** (*Uniqueness*). El sistema tan sólo autentica la votación dentro de las reglas establecidas. Es decir, por regla general, cada votante sólo puede votar una vez.
3. ***Anonimato***. No se puede relacionar un voto con el votante que lo ha emitido.
4. ***Imposibilidad de coacción***. Ningún votante debe ser capaz de demostrar ante terceros qué voto ha emitido.
5. ***Verificabilidad individual***. Cada votante deberá poder asegurarse de que su voto ha sido considerado adecuadamente, de forma que pueda obtener una prueba palpable de este hecho. Podemos distinguir dos tipos de verificabilidad individual:

- Verificabilidad individual del contenido del voto emitido.
- Verificabilidad individual de que el voto ha sido tenido en cuenta adecuadamente. Se trataría de una prueba menos contundente que la requerida en el caso anterior. Si bien no puede conocer con puntualidad cuál de los votos contabilizados es el suyo, al menos deberá tener pruebas de que ha sido tenido en cuenta y, confiando en la corrección del sistema, confiar que lo haya sido a favor de la opción elegida (esto es lo que ocurre en la votación convencional mediante papeletas).

Definida de esta forma, en la verificabilidad individual puede aparecer una cierta contradicción con el requisito de imposibilidad de coacción. Cuanto más explícita es la verificación individual más riesgos de coacción pueden aparecer. En el sistema

convencional, el votante sabe lo que vota, y confía en que su voto será contabilizado correctamente cuando comprueba que es introducido en la urna. Además, si usa una cabina para cumplimentar su voto, no hay peligro evidente de coacción. Como puede intuirse, un estudio mínimamente riguroso del balance entre los requisitos de verificabilidad y coacción requeriría la inclusión y análisis de más parámetros, dependiendo de los distintos condicionantes sociales que aparecen en cada situación concreta.

6. ***Verificabilidad global***. Otra forma mediante la cual el votante puede asegurarse de que su voto ha sido considerado adecuadamente es que dentro del propio sistema existan mecanismos que permitan a los ciudadanos autorizados comprobar la validez del recuento final.

7. ***Fiabilidad.*** El sistema debe garantizar que no se produce ninguna alteración de los resultados, ya sea mediante ataques intencionados, fallos en el sistema o incluso si las autoridades del sistema se ponen de acuerdo para coludir.

- Fiabilidad en los procedimientos (*Reliability*). El sistema debe trabajar de forma robusta, incluso en el caso de numerosos fallos, incluyendo fallos masivos en las máquinas de votación o pérdida total de las comunicaciones.
- Exactitud en el recuento (*Accuracy*). El sistema debe registrar correctamente todos los votos. Todos los votos son tenidos en cuenta sin que sea posible cambiar, borrar o extraviar ningún voto. El sistema ha de proporcionar 100 por 100 de exactitud.
- Integridad de los datos (*Data Integrity*). Se garantiza que el contenido del voto u opinión es exactamente el que fue enviado, de tal forma que al texto original no le ha sido añadida, ni modificada ni sustraída alguna de sus partes.

8. ***Certificabilidad*** o ***Auditabilidad***. Durante el proceso de votación deberían registrarse las pruebas de voto y elementos de auditoría que permitieran a las personas autorizadas disponer de pruebas para comprobar que todo el proceso de votación es correcto (funcionamiento del sistema, programas, equipos, protocolos y demás elementos), todo ello sin comprometer la integridad de la elección o la privacidad y anonimato de los votantes. Se pueden distinguir dos tipos de auditabilidad:

- Auditabilidad al desarrollo y ejecución del sistema durante el proceso de votación.
- Auditabilidad global del sistema utilizando pruebas obtenidas durante el proceso de votación. Estas pruebas o registros deberán ser físicamente almacenables, recuperables y comparables una vez haya terminado el proceso de recuento y generación de resultados. Este requisito se puede considerar en sus objetivos bastante coincidente con el requisito de *verificabilidad* global, reseñado con el número 6.

9. ***Neutralidad***. No debe ser posible conocer resultados parciales hasta que no finalice el tiempo de la elección, para evitar que puedan influir en la libre decisión de los votantes.

10. ***Movilidad de los votantes***. El sistema debería permitir a los participantes que emitieran su opinión o voto desde cualquier *cabina o punto de votación*, eliminando la restricción actual de hacerlo en el centro de votación de la zona en la cual están censados.

11. ***Facilidad de uso***. El votante debe necesitar el mínimo de habilidades y conocimientos especiales para emitir el voto. De esa manera, se propicia la igualdad de oportunidades de todos los votantes a la hora de emitir su opinión.

12. ***Voto rápido***. El votante debería poder emitir el voto en un tiempo mínimo y razonable.

13. ***Voto nulo o de rechazo***. El sistema de votación telemática debería posibilitar que se emitiese un voto sin que fuese contabilizado como válido para ninguna de las candidaturas propuestas ni ser considerado dentro del bloque de los votos en blanco. En la votación convencional mediante papeletas existe esta alternativa, que puede usarse como muestra de rechazo ante la oferta de opciones que se presenta ante el votante.

14. ***Código abierto***. El código fuente de todos los programas que gobiernan el sistema debería ser conocido y verificable por los auditores que actúen en representación de los electores. La seguridad del sistema no debería estar basada, por tanto, en mantener este código secreto, sino en la fortaleza de los protocolos y de las claves de cifrado utilizadas en todas las fases del proceso de votación. Para garantizar el carácter abierto de los programas, el modelo de licencia más conveniente sería el comúnmente denominado *copyleft*.

15. ***Coste mínimo***. El coste del sistema de elección debería ser abordable y estar en consonancia con el coste de los sistemas convencionales mediante papeletas (o ser aún menor).

16. ***Utilización de una red dedicada***. Tanto si se vota a través de Internet como si se vota desde cabinas especializadas, la red telemática en la que se apoye el sistema deberá ser, desde un punto de vista lógico, totalmente cerrada, de forma que el acceso a ella sólo esté permitido a los agentes y actores contemplados en el sistema.

17. ***Compatibilidad con otros mecanismos de votación convencionales***. La implantación de los nuevos sistemas de votación telemática deberá hacerse de forma gradual, permitiendo que los ciudadanos puedan elegir entre este y el sistema tradicional mediante papeletas con «urna a la vista» (o voto por correo allí donde exista esta posibilidad).

18. ***Igualdad de oportunidades en la votación***. Todo ciudadano ha de tener acceso al equipamiento técnico y procedimientos organizativos a la hora de votar.

El acceso desde casa, quizás a través de Internet, plantea innumerables ventajas, pero, en la situación actual, conlleva unos riesgos capitales en lo relativo a lo que en sociología se conoce como Estratificación Digital. Se entiende por *Estratificación Digital* (en inglés *Digital Divide*) los trabajos que abarcan el estudio de los discursos y prácticas asociadas con las desigualdades y diferencias en el acceso a computadores, infraestructura de entrada a la red y adquisición de conocimientos, que se dan entre las distintas clases sociales, así como por etnia, género, nivel educativo, convicciones políticas o religiosas, etc.

La preocupación de los ciudadanos por este tipo de desigualdades ha sido fuertemente detectada en las investigaciones sociológicas que se han llevados a cabo. Un sistema de Democracia Digital necesariamente conlleva el derecho de acceso del conjunto de la ciudadanía: sería una proyección telemática del concepto de Sufragio Universal.

19. ***Flexibilidad física***. El equipamiento debe disponer de diferentes alternativas que hagan que pueda ser usado por gente con alguna discapacidad física.

20. ***Digno de confianza***. Al igual que los ciudadanos entienden, de forma genérica, la estructura y modo de operación del sistema convencional de votación mediante papeletas, deberán entender el proceso de votación telemática para fortalecer su confianza en el sistema y en las personas que lo gobiernan y lo supervisan.

Hasta aquí la relación de los requisitos detectados. Resulta evidente que esta no es una relación canónica sino que utilizando otros métodos de análisis se llegaría a otra relación diferente. Pero para los objetivos que aquí pretendemos nos va a servir como un punto de referencia a la hora de analizar las funcionalidades que

debe soportar un sistema de voto telemático (análisis que realizaremos en el siguiente epígrafe).

En algunos sectores se han realizado objeciones y críticas muy rigurosas de cara a la viabilidad de los sistemas de voto telemático. Las más significativas de ellas fueron recogidas por R. Mercuri [*] en su intervención en la Cámara de Representantes de Estados Unidos, y pueden resumirse en:

- Que es imposible superar aspectos tan críticos como son el riesgo de venta de votos, coacción, monitorización clandestina y denegación del derecho a voto.
- Que no hay forma de ofrecer al votante la seguridad de que el voto se ha registrado tal cual ha sido emitido, o que el recuento es el correcto.
- Que no ofrece control por parte de los partidos políticos.
- Que desde cualquier lugar del mundo se pueden atacar los sistemas telemáticos.
- Que los defectos del sistema pueden ser conocidos años después de la elección y que no hay elementos de auditoría.
- Que los mecanismos criptográficos se pueden romper tarde o temprano.

Como puede comprobarse, las cinco primeras objeciones que detectó Mercuri en los sistemas que analizaron han sido incluidas como requisitos en la relación antes expuesta, debido a lo cual será obligado que aquellos sistemas que cumplan esos requisitos queden a salvo de esas deficiencias. En cuanto a la última de ellas, será también necesario tenerla en cuenta a la hora de evaluar los procedimientos empleados por los sistemas de votación telemática que se nos presenten.

11.6. ESCENARIOS Y PROTOCOLOS DE VOTACIÓN TELEMÁTICA

Al igual que cuando analizamos los escenarios de dinero digital anónimo dijimos que no describiríamos las distintas aplicaciones existentes ni analizaríamos el estado del arte al respecto, tampoco ahora (por similares razones) abordaremos ni lo uno ni lo otro en lo relativo al voto telemático.

También ahora, para analizar por partes los principales problemas que se presentan en la votación telemática y la búsqueda de soluciones que **satisfagan los requisitos**, usaremos una estrategia pareja a la utilizada para el dinero anónimo: nos apoyaremos en la simplificación de dos propuestas prácticas [12] distintas que vamos a denominar, respectivamente, *SistemaA* y *SistemaB*. Con posterioridad, el lector estará en condiciones de aplicar los criterios obtenidos de ese análisis para evaluar los distintos sistemas de votación telemática que se le presentan en la actualidad y los que se le presentarán en un futuro.

Inicialmente haremos un breve comentario de una propuesta que ha supuesto un hito importante en la configuración de lo que nosotros denominamos voto telemático: se trata del esquema propuesto por Fujioka y otros [FOO93], cuya representación simplificada se muestra en la Figura 11.16, que contempla un escenario de comunicación en el que intervienen agentes telemáticos que se comunican a través de una red. Esta propuesta define distintos agentes participantes en el proceso de votación y pone el énfasis en el cumplimiento de los elementos básicos del proceso electoral tradicional. También hace la aportación de ofrecer al votante la posibilidad de ejercer cierto grado de control en el proceso.

---

* Mercuri R. *Testimony presented to the U.S. House of Representatives Committee on Science*, mayo 2001. http://www.house.gov/science/full/may22/mercuri.htm.

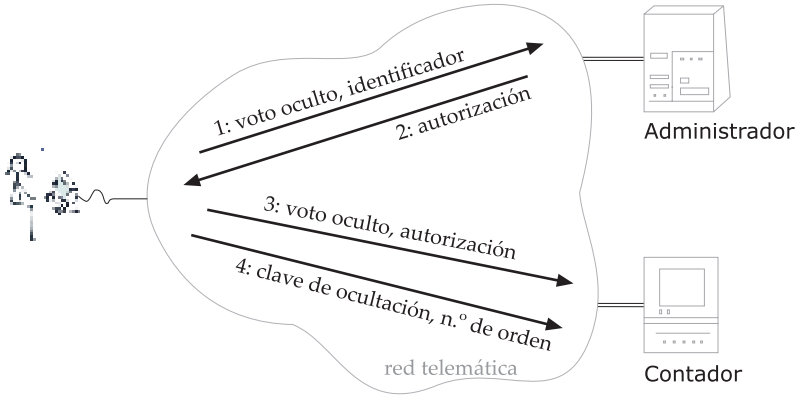

Figura 11.16. Esquema de votación en un entorno telemático (según la propuesta de Fujioka).

La votación se realiza en dos fases separadas en el tiempo. En la primera de ellas el votante selecciona el voto, lo oculta, lo firma con su clave privada y se lo envía al Administrador junto con su identificador personal (paso 1); si todo es correcto, el Administrador lo tacha de la lista y le devuelve una autorización consistente en el voto oculto firmado (paso 2). A continuación el votante envía esa autorización junto con el voto oculto al Contador (paso 3), el cual asigna **un número** a cada entrada que recibe. Cuando termina la votación y todos los votantes han realizado los pasos 1, 2 y 3, termina la primera fase y empieza la segunda. Tanto el Administrador como el Contador publican una lista con las informaciones recibidas. Consultándolas, el votante puede comprobar que su voto se ha tenido en cuenta y, extrayendo **el número** de orden que corresponde a su voto en la lista del Contador, se lo envía de nuevo al Contador (paso 4) junto con la clave que utilizó para ocultar el voto. Una vez que todos los votantes han cumplimentado la segunda fase, el Contador puede realizar el recuento de votos y publicar una lista en la que se muestra el voto en claro y los componentes criptográficos en base a los que se ha obtenido.

Como puede observarse, esta propuesta es muy interesante y muy completa, pero tiene el defecto de que requiere de dos fases diferenciadas (con todos los problemas de comunicación que ello acarrea y la ausencia del requisito de *rapidez*). Además, todo está demasiado a la vista, con lo cual existe el riesgo de *coacción* y *compra de votos*, así como el peligro que representa el hecho de que esas protecciones criptográficas (que ahora son irrompibles) transcurridos unos años dejarán de serlo, y los resultados de una votación pasada podrán ser conocidos de la A a la Z. Es decir, este sistema cumple perfectamente los requisitos elementales de anonimato en la entrega del voto; pero no hay que esforzarse mucho para comprobar, repasando la lista de requisitos que se recoge en el apartado anterior, que no cumple muchos de ellos. Aunque sea un recurso retórico algo manido, merece la pena recordar que una cadena es fuerte si son fuertes todos sus eslabones, pero basta que uno solo sea débil para que eso afecte a la robustez del conjunto.

Por todo ello, a partir de la visión global sobre el voto telemático que podemos extraer de esta propuesta pionera, pasaremos a desglosar las distintas tareas que son necesarias para culminar el proceso con las garantías necesarias.

AUTENTICACIÓN Y AUTORIZACIÓN DEL VOTANTE

En los procesos de votación convencionales, el primer paso que hay que dar es identificarse como votante ante la mesa electoral para así obtener la autorización necesaria para votar. Aunque, como ya hemos dicho, en los procesos de voto telemático no es conveniente limitarse a emular los procesos convencionales ni ceñirse a sus restricciones, valga esta comparación para entender mejor cuál es el objetivo de la fase que estamos analizando.

Es por ello que en los sistemas de voto telemático la primera fase del proceso sea también la de autenticar debidamente al votante y, caso de que sea elector, proporcionarle la correspondiente autorización para votar. Para analizar cómo se lleva a cabo esta fase en los sistemas que vamos a tomar de ejemplo, veamos inicialmente la estructura del primero de ellos: el SistemaA.

En la Figura 11.17 se presenta un esquema reducido del SistemaA en el que puede detectarse la presencia de los siguientes agentes telemáticos:

- *Puntos de Autenticación, PAs*. Se trata de un tipo de cabinas, dotadas de lector de tarjetas pero sin capacidades criptográficas, en las que el Votante inicia el proceso de votación. En la figura aparece uno solamente, pero pueden existir varios.
- *Puntos de Votación, PVs*. Se trata de cabinas, también sin capacidades criptográficas, dotadas de lector de tarjetas que ayudan al Votante a determinar y entregar el voto que desea emitir.
- *Un Administrador*. Es un sistema que sirve para la autenticación de los votantes.
- *Una Urna* que va recogiendo los votos.
- *Un Contador* que realizará el recuento de los votos una vez finalizado el periodo de recepción de los mismos.

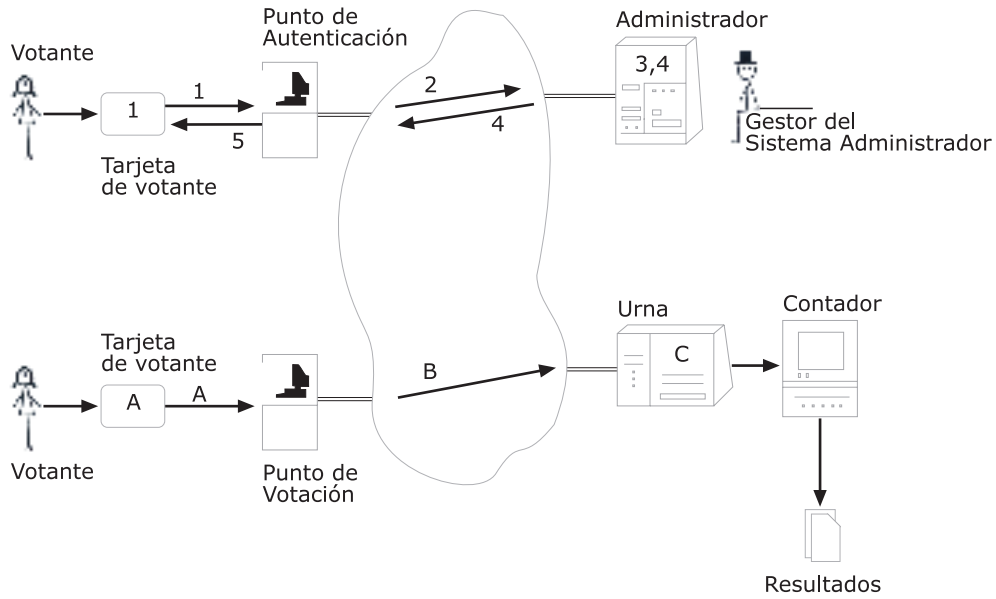

Figura 11.17. Esquema reducido del SistemaA.

Además, el sistema contempla la existencia de un conjunto de personas que intervienen de forma directa en el proceso de votación y recuento. En esta versión reducida son:

- *Votantes*. Cada Votante está en posesión de una Tarjeta inteligente de Votación, TV, que permite llevar a cabo múltiples operaciones criptográficas.
- Un *Gestor del Sistema Administrador* que también estará presente en «la apertura» de la Urna.
- Una *Autoridad de Elección.* Es la persona encargada de la supervisión general del sistema.

a) Hay que autenticar al Votante y autorizarle a votar una sola vez

Esta exigencia (como recordábamos en los requisitos 1 y 2 reseñados en el anterior apartado) es de las más elementales que deben plantearse. Analicemos si se cumple adecuadamente en el SistemaA.

El Votante se acerca a la cabina que contiene el Punto de Autenticación y procede de la siguiente forma:

1. El Votante introduce su tarjeta inteligente (TV) en el lector de tarjetas del PA. Se produce una autenticación mutua entre ambos.
2. El Votante se autentica ante su TV mediante un PIN o un mecanismo de identificación biométrico.

A partir de aquí se lleva a cabo, ante el sistema, el proceso de autenticación propiamente dicho, que podemos describirlo (véase Figura 11.17) en los cinco pasos siguientes:

1. La Tarjeta de Votante, TV, genera una clave de solicitud de autorización, k_A. La TV contiene un par de claves (pública y privada) identificativas del Votante. La tarjeta genera un factor de opacidad y opaca k_A para el Administrador. La TV le entrega al PV la clave opacada $O_{Ad}(k_A)$ y el identificador del Votante, todo ello firmado con su clave privada.
2. El PV genera una APDU con los datos recibidos de la TV y se la envía al Administrador.
3. El Administrador lee la APDU. Luego deberá comprobar si el identificador de votante recibido es correcto. Es decir, comprueba que el identificador está dentro de la lista de identificadores válidos, que la firma del Votante que realiza la solicitud es correcta y que no se ha recibido (y por tanto firmado ya) una clave opacada $O_{Ad}(k_A)$ asociada a dicho identificador (es decir, que esa tarjeta no ha realizado previamente la autenticación). En caso contrario se rechaza lo recibido.
4. Una vez comprobado que el identificador de votante recibido es válido, el Administrador firmará **a ciegas** la clave opacada de solicitud de autorización, $O_{Ad}(k_A)$. Esta firma opaca $A_{bsig}[O_{Ad}(k_A)]$ representa la autorización que el Administrador emite a favor del Votante.

   Todo ello lo volverá a cifrar con la clave pública del Votante, tras lo cual lo enviará (mediante una APDU) al Punto de Autenticación. De esta forma tan sólo la TV podrá leer esa información (confidencialidad de los datos) y además, gracias a la firma opaca, la tarjeta tendrá la garantía de que fue el Administrador quien le devolvió la autorización.

5. El Punto de Autenticación entrega a la Tarjeta del Votante los datos contenidos en la APDU que ha recibido del Administrador. La TV elimina el cifrado que los protege haciendo uso de la clave privada del Votante.

   A continuación la TV elimina el factor de opacidad de la autorización recibida obteniendo la clave de autorización k_A firmada por el Administrador [esa firma será $Ad_S(k_A)$ si se ha usado un algoritmo equivalente al de Chaum] (véase el apartado correspondiente a la firma opaca en el epígrafe 11.1). A continuación verifica que la firma del Administrador es correcta. Si es así, el Votante ha finalizado el proceso de autenticación y de obtención de autorización para votar.

Esta k_A **firmada** por el Administrador constituye la verdadera *autorización* para votar.

Visto en su conjunto, el proceso no es muy complicado. Consiste en que el Votante, a través de su tarjeta inteligente, envía su identidad más una clave de solicitud de autorización (k_A) opacada. El Administrador lo tacha de la lista de votantes y le firma de forma ciega la clave opacada que le envió. El Votante (su tarjeta) retira el factor de opacidad y obtiene la k_A firmada por el Administrador. Cualquiera que conozca la clave pública del Administrador podrá verificar que, en efecto, el Administrador ha sido quien le ha firmado esa autorización. El Administrador sabe que el Votante ha obtenido la autorización para votar, pero no tiene ni idea del valor real de esa k_A que ha firmado.

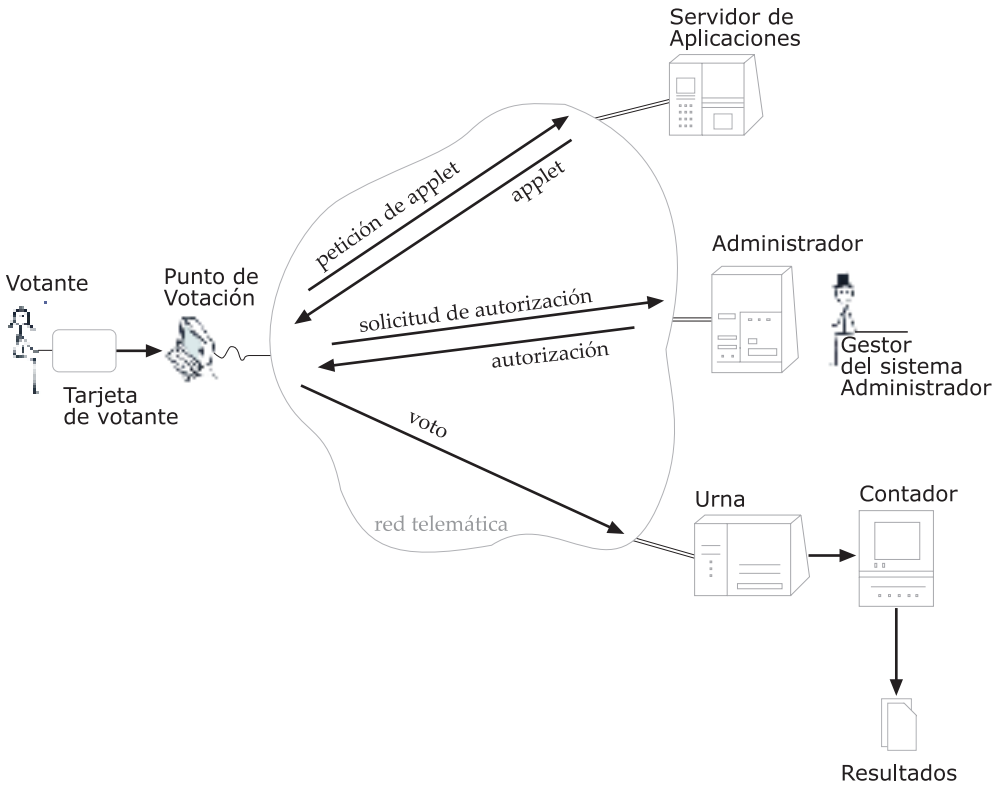

Figura 11.18. Esquema reducido del SistemaB.

Piénsese que aquí, a diferencia de lo que ocurría con el Banco en la firma a ciegas de pagarés digitales, el Administrador no se juega nada firmando a ciegas. Suponiendo que un votante se saltase la protección de la tarjeta y falsificase los programas y enviara en lugar de k_A un valor mal configurado, lo único que ganaría sería ser tachado de la lista y (como veremos más adelante) no poder votar.

En resumen, todo parece indicar que la exigencia de *autenticidad* y *acotabilidad* que estamos comentando se cumple en el SistemaA. Veamos si ocurre lo mismo con el SistemaB.

Una simplificación de la arquitectura del SistemaA la constituye el hipotético sistema que hemos denominado SistemaB, cuya configuración (a su vez reducida) se muestra en la Figura 11.18. A diferencia del esquema anterior en el que los Puntos de Votación (y los de Autenticación) son máquinas con periféricos y programas específicos, sin capacidades criptográficas, diseñadas exclusivamente para la aplicación de voto, los Puntos de Votación en el SistemaB son computadores personales convencionales dotados de lector de tarjeta y con capacidad de acceso a través de Internet. Además, como se aprecia en la figura, este mismo computador sirve tanto para la autenticación como para la emisión de voto. Así pues, el escenario de comunicación del SistemaB se diferencia del que ya hemos visto para el SistemaA en que:

- Las dos cabinas se sustituyen por un Punto de Votación constituido por un computador convencional conectado a la red telemática.
- Aparece un nuevo agente: el Servidor de Aplicaciones.

La primera parte del proceso de autenticación consiste en que:

i) El Votante introduce su tarjeta inteligente (TV) en el lector de tarjetas del computador.
ii) El Votante se autentica ante su TV mediante un PIN (o un mecanismo de identificación biométrico).
iii) El computador que actúa como Punto de Votación se conecta con el Servidor de Aplicaciones e invoca a la *applet* que reside en él. La *applet* se carga en el computador que actúa como Punto de Votación. A partir de ese momento es esa *applet* o *aplicación cliente*, que sí tiene capacidades criptográficas, la que gobierna todo el proceso de votación.

En el SistemaB la TV tiene menos competencias que las que tiene asignadas la TV del SistemaA. Por esa razón, puede ser una tarjeta inteligente más elemental, en cuyo caso no soportaría adecuadamente los mecanismos de autenticación biométrica, lo que supondría menos fortaleza en la autenticación del Votante. Además, al tratarse de un computador convencional, no es posible ofrecer las mismas garantías de resistencia ante manipulaciones que pueden implementarse en el PA y PV del SistemaA y no puede implantarse el reconocimiento mutuo entre el terminal y la tarjeta, con el riesgo que supone que una tarjeta pirata intente hacer tonterías.

En cuanto a los cinco puntos restantes, el comportamiento es muy similar al que ya hemos visto para el SistemaA salvo que aquí las tareas de cifrado y verificación se reparten entre la tarjeta y la applet que reside en el computador de acceso. No obstante, la generación de claves y el firmado con la clave privada del Votante han de realizarse obligatoriamente en la tarjeta inteligente del Votante.

Aunque la applet que se carga estará firmada por el Servidor de Aplicaciones para evitar que realice tareas indebidas, siempre será posible crear applets ficticias que

averigüen el valor de algunos de los datos que son manejados desde ella. En el SistemaA, sin embargo, todo lo que se procesa dentro de la tarjeta y no sale fuera de ella es computacionalmente impracticable conocerlo.

En resumen, también el SistemaB cumple bastante aceptablemente la exigencia de *autenticidad* y *acotabilidad* que estamos comentando, aunque de forma menos robusta que el SistemaA. Por contra, el SistemaB tiene un aspecto más atractivo, ágil y «moderno» que el sistema «padre» del que procede.

ENTREGA DEL VOTO A LA URNA

El Votante, una vez que ha completado con éxito el proceso de autenticación y que ha obtenido la autorización, se dirige a un Punto de Votación para proceder a la entrega del voto. Nuevamente cabe recordar el paralelismo que esto tiene con los procesos convencionales de votación: una vez que la persona que va a votar se ha identificado ante la mesa electoral y su nombre es tachado de la lista correspondiente, se le permite que el sobre que contiene su papeleta sea introducido en la Urna.

b) El voto debe entregarse de forma anónima y sin coacciones

Fijemos nuestra atención de nuevo en el SistemaA para analizar si cumple esta exigencia (números 3, 4 y parte del 7, según la relación de requisitos). Antes, cuando contamos que la tarjeta generaba la *clave de solicitud de autorización* (k_A), no contamos toda la verdad. Lo que genera realmente es un par de claves asimétricas de votación (k_{dV}, k_{cV}), tipo RSA, que se almacenan de forma que ni el propio Votante pueda leerlas (las dos son secretas). La *clave de cifrado de voto* (k_{cV}) se utilizará para cifrar el voto en claro y, como su nombre también señala, la *clave de descifrado de voto* (k_{dV}) servirá para leer el voto cifrado. Esta segunda clave k_{dV} es la que se utiliza para solicitar la autorización y es a la que en la fase anterior denominamos k_A. Es decir: $k_A \equiv k_{dV}$. Y la *autorización firmada* (si se usa un algoritmo equivalente al de Chaum) es: $\mathrm{Ad}_S(k_A) \equiv \mathrm{Ad}_S(k_{dV})$.

A partir de ahora, para mejor entendimiento de las operaciones, vamos a utilizar para esta clave el nombre y el símbolo de *clave de descifrado de voto*. Dicho esto, digamos que el Votante se dirige al Punto de Votación e introduce su tarjeta en el lector correspondiente, llevándose a cabo un proceso de autenticación del Votante ante su tarjeta y de la tarjeta ante el PV, que es en todo igual al que ya describimos como preámbulo de la fase de autenticación.

A partir de ahí el proceso se divide en tres pasos (Figura 11.17), de la forma siguiente:

A) El Punto de Votación solicita al Votante su voto mediante un diálogo interactivo en el que, a través de texto e imágenes, se facilita al Votante la elección de la opción deseada. En la Tarjeta de Votante se cifra con k_{cV} (*clave de cifrado de voto*) el voto a entregar. Ello implica que el voto sólo podrá ser descifrado usando la clave k_{dV} (*clave de descifrado de voto*) pareja de la anterior.

   Mediante un proceso de diálogo entre el PV y la Tarjeta, ésta crea una pieza de información con el voto cifrado, la clave k_{dV} y la *autorización firmada* (la clave k_{dV} firmada por el Administrador). A continuación se «guarda»

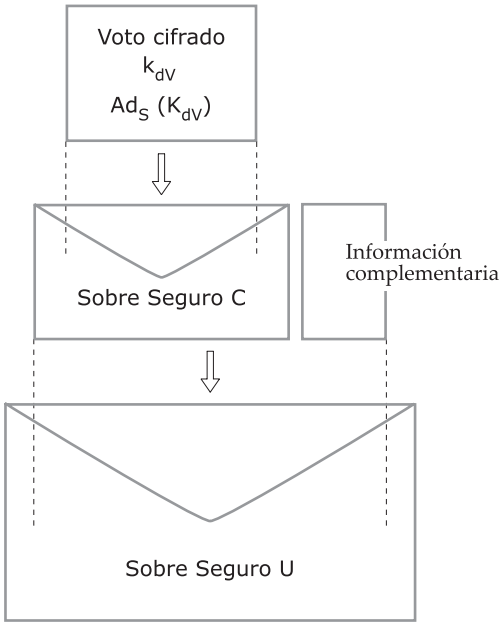

Figura 11.19. *Sobre Seguro C* dentro de *Sobre Seguro U.*

esta pieza de información en un *Sobre Seguro* * *C* entre la TV y el Contador, que sólo este último puede abrir[13]. Tras esto, en la Tarjeta del Votante se genera una «información adicional» (cuyo significado no veremos por ahora) que se junta con el *Sobre Seguro C* y se «guarda» en un nuevo *Sobre Seguro U* que sólo la Urna puede abrir. A continuación la Tarjeta le entrega al Punto de Votación este *Sobre Seguro U* para su posterior envío a la Urna. (Véase Figura 11.19).

B) Con el *Sobre Seguro U* referido en el paso anterior, el Punto de Votación genera una APDU y la envía a la Urna (solamente la Urna sabe leer esa APDU).

C) La Urna, tras eliminar el *Sobre Seguro U* que protege lo recibido (y que sólo la Urna es capaz de «abrir»), obtiene la «información adicional» (cuyo significado no veremos por ahora) y la pieza de información que constituye el *Sobre Seguro C* (que sólo el Contador puede «abrir» y que contiene, repetimos, el voto cifrado, la clave k_{dV} y la clave k_{dV} firmada por el Administrador). La Urna almacena estos *Sobres Seguros C* hasta el final del periodo de votación. El Punto de Votación informa al Votante de que ha terminado el proceso de entrega de su voto.

---

* Este *Sobre Seguro* sirve para que el destinatario obtenga el *mensaje* con total garantía de confidencialidad e integridad y sin información alguna que permita asociarlo a su origen. Si únicamente se cifrara el voto con la clave pública del destinatario sería muy sencillo el que un atacante externo *adivinase* el voto entregado por un votante simplemente cifrando todas las posibles opciones de voto con la clave pública correspondiente y comparando los resultados obtenidos con la pieza de información entregada por el Votante.

Una Tarjeta de Votante que haya completado el proceso anterior y haya emitido el voto almacenará un indicador y rechazará realizar de nuevo el proceso de entrega de voto, aunque su Votante propietario lo intente (la tarjeta es resistente ante manipulaciones), lo que garantiza que cada Votante vota sólo una vez. No obstante, aunque consiguiera romper la protección de la tarjeta no conseguiría que se le contabilizase más de un voto (como más adelante veremos).

A tenor de las explicaciones anteriores, parece bastante claro que el *anonimato* está bastante bien garantizado porque aunque el votante se autentica **ante su tarjeta**, no se autentica ante el Punto de Votación. Además, aunque posteriormente el Administrador vea la relación que hay entre la k_{dV} y el voto, no podrá saber nada de la identidad del Votante propietario de esa clave que el Administrador firmó a ciegas.

En principio, podemos pensar que tal y como está diseñado el proceso podríamos juntar el Punto de Autenticación y el Punto de Votación en una sola cabina. Eso simplificaría las cosas y no parece que tenga mayor problema si pensamos que los terminales son *tamper-resistant* y no van a hacer nada que no esté especificado en su funcionamiento. Pero el tema del anonimato es muy serio y no podemos permitir que sea una misma máquina la que maneje primero la identidad y luego el voto.

Por eso es mejor poner pared por medio y separar ambas máquinas. Así, aunque alguien consiguiese manipularlos o sustituyese un terminal manipulado haciéndolo pasar por bueno, ese Punto de Autenticación puede llegar a conocer la identidad pero no puede relacionarla con la k_{dV}, mientras el Punto de Votación conoce el voto pero no puede conocer la identidad. Además, las dos actuaciones pueden estar distanciadas en el tiempo a voluntad del Votante (puede quedarse deshojando la margarita antes de votar) y en el espacio (puede depositar el voto en otro lugar donde también exista un Punto de Votación). Esta posibilidad de distancia en el tiempo y en el espacio es una de las posibilidades que ofrecen los sistemas de votación telemática (requisito número 10, *movilidad de los votantes*) que no existe en los sistemas de votación mediante papeleta ni en otros de los que hemos denominado de *voto electrónico convencional*. Además, conviene que no exista una relación uno a uno entre las dos máquinas.

Cuanta menos relación, mejor. Así evitaremos que la fila de votantes ante el PV se produzca en el mismo orden que la fila de votantes ante el PA, y evitaremos la tentación de que alguien pueda establecer registros que luego puedan cotejarse. Es sencillo idear varios procedimientos organizativos para romper la relación entre ambas máquinas. Puede pensarse que es una exageración ponerse tan puntillosos y andar con tantas sospechas y conjeturas. Pero en lo tocante al anonimato, todas las prevenciones están justificadas (piénsese que los sistemas de voto telemático deben ser no sólo **tan seguros** como los sistemas de votación mediante papeleta, sino **más seguros** aún).

En cuanto al requisito de *imposibilidad de coacción*, parece claro que el Votante no puede conocer **su** k_{dV} porque su tarjeta inteligente no se la deja ver. Así, no podrá posteriormente demostrar ante nadie qué es lo que ha votado y podrá evitar votar bajo coacción o vender su voto al mejor postor.

En cuanto al tercer y último requisito que estamos analizando, del análisis del procedimiento empleado y de la robustez de los mecanismos criptográficos utilizados, se deduce que la fiabilidad del sistema ante ataques externos (según se analizó en el punto A y en las notas aclaratorias) es suficientemente aceptable, así como la garantía de la *integridad de los datos* que se manejan.

En resumen, podemos afirmar que el SistemaA descrito cumple bastante bien con la exigencia de anonimato, no coacción y fiabilidad que remarcábamos al principio.

¿La cumple también el SistemaB? Analicemos brevemente su comportamiento. Los tres pasos A, B y C que antes hemos señalado para el SistemaA se llevan a cabo

de forma muy similar para el SistemaB. Nuevamente hay que recordar que las tareas de transformación criptográfica de los datos y la conformación de las APDUs se llevan a cabo cooperativamente entre la tarjeta y la applet. Debido a ello, la applet sí «ve» en algún momento el valor de la k_{dV} en claro. Por esa razón, generando una applet falsa podría llegar a conocerse k_{dV}. Este riesgo lo tendremos en cuenta a la hora de decidir qué es lo que publicará el Contador después del recuento.

Si la votación se realiza desde casa, o desde sitios dispersos y desconocidos, el anonimato está aceptablemente garantizado porque es evidente que el Votante disperso no es fácilmente espiable. Pero, en cambio, la coacción está servida. Al calor del hogar (o de la residencia de ancianos) todo se reblandece. Lo mismo cabe decir de la compra de votos a domicilio. Este es un riesgo excesivamente grande.

Hay que decir que el uso para el que están pensados sistemas con una estructura similar al SistemaB están relacionados con la sustitución del voto por correo, que lleva consigo los mismos riesgos de coacción, pero aumentados. Si además el voto por correo está pensado para electores que viven fuera del país en el que se realiza la votación, con el añadido de las embajadas y de la privatización de los servicios postales a nivel internacional, la cosa es todavía más imperfecta. Es decir, que un sistema de las características del SistemaB es mucho más fiable que lo que existe actualmente para el voto de esos electores ausentes. Si se concentrasen los puntos de votación en locales especializados (por ejemplo embajadas o casas regionales) este riesgo disminuiría notablemente, porque la solución se aproximaría a la de los PA y PV diseñados para el SistemaA.

La concentración de los computadores que hacen las veces de puntos de votación en el SistemaB acarrearía, no obstante, posibles riesgos de manipulación del computador desde el que se vota (según hemos discutido al analizar el SistemaA). Pero con todo, al tratarse de una applet firmada, los riesgos de manipulación son menores que los riesgos de coacción que antes hemos comentado.

En resumen, un sistema de las características del SistemaB no soportaría la comparación con un sistema convencional de urnas y papeletas y sólo se justificaría su implantación si el modelo al que trata de sustituir, como es el voto por correo, conlleva todavía mayores riesgos.

APERTURA DE LA URNA Y RECUENTO

En los sistemas convencionales de votación mediante papeleta, los votos permanecen guardados en la urna hasta que finaliza el periodo de votación, instante en el cual se abre la urna. Si las urnas son transparentes, como es el caso del Estado español, las papeletas de votación deberán estar guardadas en sobres para mantener oculto su contenido ante miradas indiscretas. En el momento de la apertura, se sacan las papeletas de los sobres y las personas autorizadas proceden al recuento de los votos obtenidos por las distintas opciones. Algo similar (y si es posible, más seguro aún) debe ocurrir con los sistemas de votación telemática.

c) El recuento debe hacerse de forma fiable y auditable

En primer lugar, la Urna debe guardar los votos de forma fiable de manera que no sea factible alterarlos durante el tiempo que dura el proceso de votación (requisito número 7: *fiabilidad en los procedimientos* e *integridad* de los votos guardados). Además,

hasta que no se llegue al final de la votación nadie puede conocer resultados parciales (requisito 9: *neutralidad*) para que no se puedan establecer influencias en el electorado.

Por otra parte, en los sistemas de votación mediante papeletas, la presencia de representantes (interventores) de las candidaturas o de los electores representa una garantía tanto para el proceso de entrega de voto como para el proceso de recuento. En lo que a este último se refiere, en los sistemas de votación telemática deberán existir mecanismos robustos y procedimientos organizacionales que garanticen la corrección de los resultados finales (requisito 8: *certificabilidad* o *auditabilidad*).

Analicemos el comportamiento del SistemaA para evaluar si cumple adecuadamente estas exigencias. Todos los votos permanecen en la Urna hasta el final del periodo de recepción de votos. Además, la Urna los guarda pero ni ella ni nadie (excepto el Contador) puede leerlos por estar protegidos en *Sobres Seguros C*. La apertura se realizará de la manera siguiente:

1. Para proceder a la apertura de la Urna se necesitará la presencia física y simultánea del Gestor del Sistema Administrador y de la Autoridad de Elección que aportarán una información secreta introduciendo sus respectivas tarjetas inteligentes en los lectores habilitados para ello en la Urna y autenticándose biométricamente ante sus respectivas tarjetas.
2. La Urna aleatoriza todo lo que ha ido recibiendo (modifica el orden de aparición de los registros) y lo envía al Contador, publicando a su vez una lista con lo enviado (aquí están los votos cifrados dentro de *Sobres Seguros C*).
3. En ese momento, la Urna borra toda la información que ha ido adquiriendo durante su funcionamiento. El proceso mediante el cual se produce el borrado será auditable por parte de aquellas personas o entidades que políticamente se determine que tengan autorización para ello.

A continuación se procederá al recuento de los votos, que se llevará a cabo de la forma siguiente:

1. Antes de iniciar la lectura de los resultados, nuevamente el Gestor del Sistema Administrador y la Autoridad de Elección, con sus tarjetas inteligentes (mediante un procedimiento de secreto compartido) proporcionarán de forma conjunta al Contador su clave privada (que ha permanecido guardada y oculta hasta este momento) necesaria para que el Contador entre en funcionamiento.
2. El Contador, después de recibir toda la información procedente de la Urna «abre» los *Sobres Seguros C* que contienen la información sobre el voto antes descrita: voto cifrado con k_{cV}, la clave k_{dV} y la clave k_{dV} firmada por el Administrador. Para cada uno de los votos, el Contador verifica que la k_{dV} (que sirve para abrir el voto cifrado) esté correctamente firmada y, a continuación, lo descifra.
3. La clave k_{dV} firmada por el Administrador sirve de garantía para el Contador de que nadie excepto un Votante autorizado puede entregarle un voto válido. Aunque la Tarjeta de Votante impide que el Votante pueda votar más de una vez, si esta protección fuese violada, el Contador lo detectaría (y subsanaría esa incidencia) porque aparecería más de un voto con la misma k_{dV}.
4. Por último, una vez realizado el recuento, el Contador hace públicos los resultados de la votación y genera una lista en la que para cada una de las entradas aparecen: a) el voto en claro, b) la clave k_{dV}, c) la clave k_{dV} firmada por el Administrador.

Los resultados globales de la votación serán, obviamente, públicos. La información generada por la Urna y la lista generada por el Contador deberán permanecer bajo custodia de la Autoridad de Elección (que pertenecerá, presumiblemente, al ámbito judicial) para atender a posibles reclamaciones o verificaciones por parte de personas autorizadas. Transcurrido un tiempo previamente regulado, toda esa información se destruirá de forma auditada. De esta manera, se suprime el peligro que representa el hecho de que las protecciones criptográficas, mediante las cuales se mantiene el anonimato de forma robusta, puedan ser superadas cuando, transcurridos unos años, evolucionen las técnicas criptográficas.

En cuanto al SistemaB, soslayaremos, por el momento, hacer un comentario detenido. Baste decir por ahora que el proceso de apertura de Urna y recuento puede ser exactamente igual al descrito para el SistemaA, pero que en la lista que genera el Contador no puede aparecer la k_{dV} en claro porque, como hemos dicho, es factible que el Votante la averigüe, con lo cual podría demostrarle al Gestor del Sistema Administrador o a la Autoridad de Elección cuál ha sido exactamente su voto. Ese peligro no existe en el SistemaA porque la k_{dV} permanece en la tarjeta inteligente del Votante sin que nadie, ni siquiera éste, pueda leerla.

De lo que acabamos de describir puede deducirse que los requisitos de fiabilidad y neutralidad se cumplen de manera bastante satisfactoria en este SistemaA, pero que la auditabilidad está sólo al alcance del Gestor del Sistema Administrador y de la Autoridad de Elección. No aparece de forma efectiva la presencia de la ciudadanía o de representantes de las candidaturas o de los electores.

En los procesos de votación mediante papeletas el Votante puede ver cómo su voto se guarda en la urna y asistir al proceso de recuento. Además, la presencia de **interventores** en representación de las candidaturas (o de los simples electores) introduce unas garantías que no aparecen en lo que hasta ahora hemos descrito del SistemaA y del SistemaB. Dicho de otra forma, el esquema reducido que hemos presentado en las Figuras 11.17 y 11.18 no satisface adecuadamente los requisitos relacionados con la *verificación individual* ni los que exigen la *verificación global* ni permite una *auditabilidad* satisfactoria del proceso (requisitos 5, 6 y 8 de la relación que antes presentamos). Habrá que mejorar su arquitectura y los procedimientos empleados para conseguirlo. De eso es de lo que hablaremos en los siguientes apartados.

VERIFICACIÓN INDIVIDUAL DEL PROCESO

El Votante pertenece a un tipo de mamíferos cuyos antepasados se irguieron sobre las patas traseras hace ya muchos miles de años (aproximadamente los mismos que lleva complicándole la existencia a toda especie de animal, vegetal o mineral que se ponga a su alcance), debido a lo cual, cuando el Votante se acerca a la urna pisando sobre el suelo y mirando la papeleta que introduce en ella, se encuentra «en su medio» y adquiere bastante confianza en que luego, cuando se abra, su papeleta será una de las que se tengan en cuenta (debido también a la presencia de interventores que vigilan que no se saque nada de la urna hasta que el proceso termine).

En el voto telemático, en cambio, todo es remoto, todo es virtual, nada está al alcance de la mirada que el Votante puede lanzar desde la ancestral posición erguida con la que participa en los procesos convencionales de voto mediante papeleta. Por todo ello, será necesario diseñar mecanismos robustos e ingeniosos para que el Votante (de por sí, o fiándose de la opinión de gente experta de su confianza) acepte

convencidamente su implantación. Estos mecanismos serán los que sirvan para dar satisfacción al requisito de *verificabilidad individual* recogido con el número 5 en la relación que estamos usando de referencia. Para que haya democracia es necesario que exista convencimiento, no resignación.

d) El Votante debe convencerse de que su voto ha sido tenido en cuenta correctamente

La dificultad que conlleva el generar una prueba palpable para que el Votante se convenza de que su voto ha sido tenido en cuenta es que tiene que llegar a ese convencimiento (como ocurre en la votación con papeletas) sin que se le entregue una prueba material legible porque en ese caso podría demostrar su voto ante terceros para aceptar una coacción o venderlo (se incumpliría el requisito número 4).

Dejando para más adelante el SistemaB, cabe decir que en el SistemaA se puede introducir una comprobación de voto tal que la representada en la Figura 11.20. Para ello se incorporan nuevos agentes telemáticos:

- *Puntos de Verificación.* Se trata de cabinas, sin capacidades criptográficas, dotadas de lector de tarjetas inteligentes que permiten al Votante comprobar que su voto ha sido tenido en cuenta y ha sido correctamente contabilizado.

Una vez haya finalizado la votación, y durante un periodo de tiempo prefijado, cada Votante puede comprobar de forma independiente que su voto ha sido correctamente tenido en cuenta. Para ello basta con que el Votante se dirija a un Punto de Verificación y, siempre de forma individual, utilice su tarjeta y pida que se le muestre el voto asociado. El sistema ubicado en el Punto de Verificación está habilitado para leer la k_{dV} almacenada en la tarjeta del Votante, de manera que, una vez obtenida dicha clave de la tarjeta, accede vía telemática a la lista de parejas k_{dV} *en claro-voto* generada por el Contador y le muestra el voto asociado, de forma que el Votante y sólo éste pueda leerlo. Pero no se le entrega ninguna prueba fehaciente.

En realidad se trata más de una comprobación que de una verificación robusta. Este procedimiento sirve para comprobar que no han existido errores técnicos, pero no protege contra la falta de honradez del sistema global. Por ejemplo, si el Contador ha obtenido unos resultados correctos y ha publicado unos resultados falsos, cuando un Punto de Verificación le pregunte, le informará del resultado correcto, con lo cual el Votante quedará contento y defraudado.

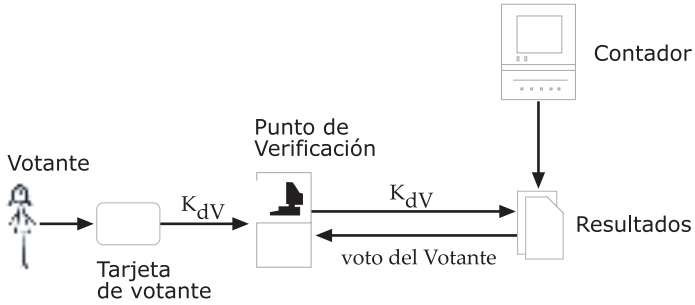

Figura 11.20. Comprobación por parte del Votante de la presencia de su voto en el resultado.

Este problema se puede eliminar o disminuir mejorando los procesos colectivos de auditoría y control que más adelante comentaremos. No obstante hay que prever que el Votante, de forma individual, quiera tener pruebas criptográficamente robustas que le sirvan en caso de duda o sospecha. En ese caso, o en el caso de que el Votante no esté conforme con la opción visualizada, es necesario buscar un procedimiento más seguro, tal y como se discute a continuación.

e) En caso de reclamación, el Votante debe recibir pruebas del sentido de su voto

De lo que se trata es de cumplir de forma más rigurosa el requisito número 5 relativo a la *verificabilidad individual*, sin vulnerar otros requisitos que pueden aparecer como contradictorios. El mecanismo criptográfico que puede resolver este compromiso será un *comprobante de votación* que reciba el Votante con el contenido de su voto pero que esté suficientemente protegido como para que no se pueda «negociar» con él ni usarlo fuera de circunstancias muy especiales y en presencia de testigos relevantes.

En la Figura 11.21 se muestra la forma de obtener el *comprobante* tanto en el SistemaA como en el SistemaB, aunque para explicar su utilización nos centraremos en el primero de ellos debido a que aún no hemos dicho cómo publica los resultados el SistemaB. La incorporación del comprobante se consigue modificando el proceso que describimos en el apartado (de este mismo epígrafe) *Entrega del voto a la Urna*. Así:

- En el punto A) decíamos que en la Tarjeta del Votante se genera una «información adicional» que se junta con el *Sobre Seguro C* y se «guarda» en un nuevo *Sobre Seguro U* que sólo la Urna puede abrir (Figura 11.19). Esa es en realidad una *clave simétrica* que la TV manda a la Urna.
- En el punto C) la Urna, tras abrir el *Sobre Seguro U* a ella destinado, obtiene, como ya se dijo, además del *Sobre Seguro C*, esa «información adicional» (la *clave simétrica*). A partir de esos datos, devuelve al Punto de Votación un *comprobante* de la votación realizada. Para generar el comprobante realiza las siguientes operaciones: a) la Urna cifra el Sobre Seguro C con la clave pública de la Autoridad de Elección, y b) la Urna firma lo anterior con su clave privada. A continuación la Urna cifra el comprobante con la *clave simétrica* que recibió del Punto de Votación. Una vez hechas las tres operaciones envía lo resultante al Punto de Votación.
- Es necesario añadir a la descripción un nuevo punto, el D), que consiste en que el Punto de Votación entrega lo recibido a la Tarjeta de Votación, la cual elimina el cifrado con la clave simétrica, obteniendo *el comprobante*. Después verifica la corrección de la firma por parte de la Urna (si bien no puede conocer

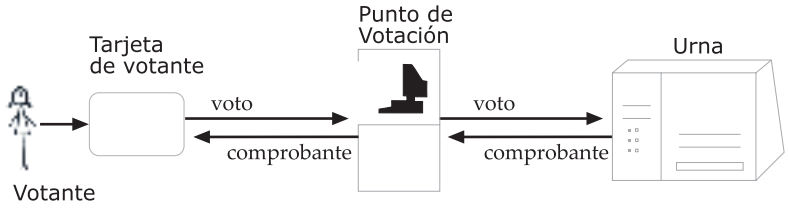

Figura 11.21. Incorporación de un comprobante de votación.

el contenido del comprobante por estar cifrado con la clave pública de la Autoridad de Elección). El comprobante de voto es guardado en la Tarjeta del Votante y sólo la Autoridad de Elección podrá acceder a los datos de ese comprobante en caso de reclamación (según estipulen las reglas que se dicten), una vez haya finalizado el proceso de votación.

Este comprobante así generado es una prueba que el Votante no puede verificar en el momento de la votación (sólo sabe que ha sido firmada por la Urna), pero que sabe que podrá usar en caso de reclamación. El procedimiento podría modificarse para que la TV sí pudiese verificar que el comprobante es exactamente el *sobre Seguro C* que ella envió, pero firmado por la Urna. Eso dejaría la protección de la no posible lectura del comprobante «sólo» en brazos de la cualidad *tamper-resistant* de la tarjeta. Por ello, para dejar más cubierto el requisito número 4, lo mejor es optar por la solución antes descrita.

Una vez finalizado el proceso de votación y publicados los resultados, con el *comprobante* almacenado en su tarjeta, cifrado con la clave pública de la Autoridad de Elección, el Votante puede decidir iniciar un *Proceso de Reclamación* (o verificación robusta) ante esa misma Autoridad de Elección. Para ello deberá solicitar esa comprobación y acudir en compañía de algún representante legal que, además, tenga conocimientos criptográficos para poder dar fe de la corrección o no de las pruebas que se le presenten. En esa comparecencia se le entregará la tarjeta inteligente del Votante a la Autoridad de Elección (que, como hemos dicho, lo razonable es que pertenezca al ámbito judicial).

En ese mismo acto la Autoridad de Elección, tras recibir la tarjeta del Votante, puede demostrar sin ninguna ambigüedad un tratamiento correcto o incorrecto del voto, pues tiene acceso a:

- La k_{dV} del Votante almacenada en su tarjeta.
- El comprobante enviado por la Urna al Votante (firmado por la Urna y garantizada su inviolabilidad por la clave pública de la Autoridad de Elección) donde se contiene el voto emitido.
- Los registros del Contador que relacionan la k_{dV} firmada por el Administrador, la k_{dV} en claro y el voto cifrado con k_{cV}.

Con todo ello la Autoridad de Elección, apoyándose en pruebas criptográficas robustas, que puede exhibir ante el Votante o ante su representante-perito, dictaminará si el Votante no tiene razón o si ha existido una falsificación por parte del sistema.

La limitación de que en esta prueba el Votante tenga que desvelar su voto hace que esta verificación sólo pueda ser llevada a cabo por ciudadanos comprometidos (de los que tantos existen en un proceso de votación) que, incluso, hayan hecho pública previamente su decisión acerca de qué es lo que van a votar. Pero la robustez de la prueba es tal que con **un solo caso** comprobado en el que la autoridad judicial dictamine que *el Sistema*, **o sus gestores**, han cometido fraude, podría declarar NULO todo el proceso electoral. Lo cual representa una espada de Damocles tan cierta, que el Sistema se ve impelido a **ser honrado** y no cometer fraude alguno (todo esto además de que, como hemos visto, ni los agentes telemáticos ni los gestores tienen resquicios razonables para poder «meter mano» en el proceso).

AUDITABILIDAD Y VERIFICACIÓN GLOBAL

Por lo general, el Votante no se fía en exceso de lo que sus conciudadanos oponentes puedan hacer con su voto, quizás porque piense que sus adversarios políticos no deberían fiarse de lo que pudiese hacer él con los suyos. Por eso, para que el proceso electoral pueda considerarse aceptable es necesario que se permita la existencia de **interventores**, que serán determinados ciudadanos que representan a las candidaturas que compiten en la elección, o bien simplemente pertenecerán a agrupaciones de electores interesados en el proceso.

Algo semejante habrá que pensar en el diseño de sistemas de voto telemático. Como se pone de manifiesto en los requisitos detectados (número 6, *verificabilidad global*, y número 8, *auditabilidad*), esta supervisión deberá hacerse tanto durante el transcurso del proceso de votación (mediante el registro de pruebas que permitan a posteriori comprobar la corrección del sistema) como al final del proceso, cuando se proceda a la apertura de la Urna y al recuento de los votos. De la búsqueda de protocolos y mecanismos que generen pruebas criptográficas robustas para garantizar esta supervisión es de lo que nos ocuparemos en los párrafos que siguen.

f) Debe permitirse que ciudadanos autorizados supervisen todo el proceso

Pensemos por un momento cómo se desarrollan las cosas en un sistema convencional de votación mediante papeletas, por ejemplo el que está establecido en el Estado español (que será similar, con algunas variaciones, al que se sigue en otros países de nuestra misma zona cultural). La persona que va a votar selecciona primeramente su voto y lo introduce en un sobre opaco. Posteriormente se aproxima al lugar en el que está ubicada la urna, custodiada por un pequeño ejército de ciudadanos constituido por el presidente de la Mesa y dos vocales designados por sorteo entre todos los electores, además de un número indeterminado de *interventores* que actúan en representación de distintas candidaturas contendientes (pueden ser también simples ciudadanos que manifiesten, conforme a unas normas existentes, su deseo de participar en el proceso en calidad de observadores). Todos ellos constituyen la Mesa electoral y aguantan allí más de doce horas, unidos por el destino y sentados en sillas habitualmente diseñadas para escolares con una base de sustentación bastante menos generosa que la que han alcanzado los adultos constituyentes de la Mesa.

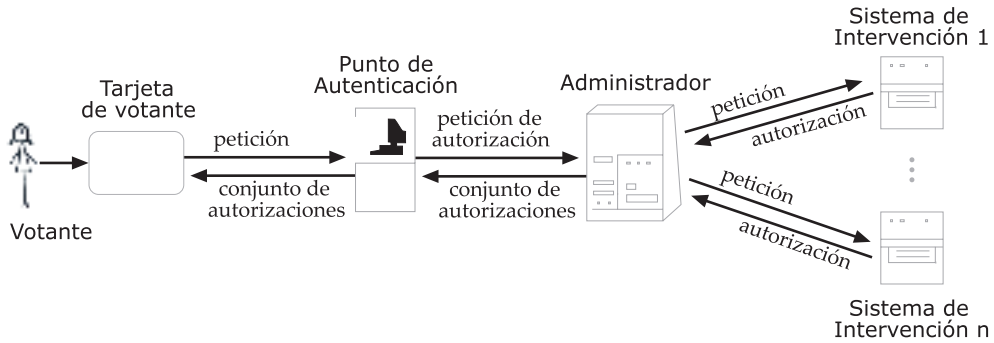

Figura 11.22. Incorporación de Sistemas de Intervención.

Los representantes «oficiales», el presidente y los dos vocales, disponen de un listado en el que aparecen todas y cada una de las personas con derecho a depositar su voto en esa urna. Una copia idéntica de dicho listado está en posesión de todos y cada uno de los interventores.

Cuando la persona que va a depositar su voto se acerca a la urna, se identifica documentalmente ante el presidente, el cual pronuncia en voz alta su nombre. Tanto el vocal que maneja el listado como las personas que actúan como interventoras localizan al votante en la lista, dicen en voz alta el número de orden que ocupa en ella, y lo tachan, indicando con ello que ya ha ejercido su derecho al voto. En ese momento se introduce su voto en la urna.

Estudiemos a continuación cómo puede trasladarse un escenario similar a un esquema de voto telemático. Para ello veamos una mejora que puede añadirse a los dos sistemas, SistemaA y SistemaB, que estamos utilizando como ejemplo a efectos didácticos. Con esta mejora aparecen nuevos agentes telemáticos y nuevos actores humanos. Éstos son:

- Varios Sistemas de Intervención (SIs) que complementan la labor del Administrador. En la Figura 11.22 se representa ese añadido.
- Interventores responsables de cada uno de los Sistemas de Intervención. Cada uno de estos sistemas está controlado por un Interventor nombrado por cada una de las agrupaciones de electores o candidaturas autorizadas para supervisar la votación.

La incorporación de estos nuevos Sistemas de Intervención sirve para que comprueben, en paralelo con el Administrador, que la solicitud realizada por el Votante es correcta y también para que esos sistemas firmen la autorización de votación que recibe el Votante. Ello permitirá que, en caso de producirse una incidencia, todos tengan constancia de ella (al igual que ocurre en la votación convencional por papeleta que acabamos de referir). Cabe señalar que la función fundamental de los SI es supervisar la actuación del Administrador para evitar manipulaciones. Así, el proceso que describimos en el apartado (de este mismo epígrafe) *Autenticación y autorización del Votante* se vería modificado de la manera siguiente:

- En el punto 1 decíamos que la tarjeta genera una *clave de solicitud de autorización* (k_A, a la que luego denominamos k_{dV}) y que la opaca para el Administrador. Ahora es necesario añadir que la opaca también para todos y cada uno de los SIs. Posteriormente, en el punto 3, el Administrador, una vez recibida la APDU procedente del Punto de Autenticación, debe enviar todos los datos **a todos** los Sistemas de Intervención.
- Cada uno de los Sistemas de Intervención, al igual que el Administrador, deberá comprobar si el identificador de votante recibido es correcto y si el Votante no ha realizado previamente otra autenticación. Si esto es así, cada uno de ellos firmará a ciegas la clave opacada de solicitud de autorización.
- Al final del proceso de autenticación, una vez que la TV retira todos los factores de opacidad de la autorización recibida, se queda con la clave de autorización k_A (o k_{dV}) firmada por el Administrador, la k_A (o k_{dV}) firmada por el Sistema de Intervención 1, la k_A (o k_{dV}) firmada por el Sistema de Intervención 2 y así sucesivamente. Esta k_A (o k_{dV}) **firmada** por el Administrador y por todos los SIs constituye la verdadera *autorización* para votar.

Consecuentemente, este nuevo valor de la autorización para votar repercute en todos los restantes pasos del proceso. Así, cuando la TV entrega el voto a la Urna, el contenido del *Sobre Seguro C* no será exactamente el mismo que describimos al explicar el SistemaA reducido (Figura 11.19), sino que la firma de la clave de descifrado será $Ad_S(k_{dV})$, $SI1_S(k_{dV})$, ..., $SIn_S(k_{dV})$ (suponiendo que existan n Sistemas de Intervención). Asimismo, cuando el Contador hace públicos los resultados de la votación, junto al voto en claro y a la clave k_{dV} añadirá todas esas firmas de la clave de descifrado, que sirven para garantizar que esa fue la clave que supervisaron tanto el Administrador como todos los Sistemas de Intervención durante el proceso de autenticación y autorización.

g) Debe permitirse que ciudadanos autorizados puedan verificar la corrección del recuento

Como hemos visto, la presencia de Interventores y de los Sistemas de Intervención por ellos gestionados sirve para introducir registros y elementos de auditoría durante el transcurso del proceso de entrega de voto. Asimismo, podemos imponer mejoras en el procedimiento descrito en el apartado *Apertura de la Urna y recuento*, de manera que sea necesaria la presencia física y simultánea no sólo del Gestor del Sistema Administrador y de la Autoridad de Elección, sino también de los respectivos Interventores, los cuales (mediante un procedimiento de secreto compartido semejante al

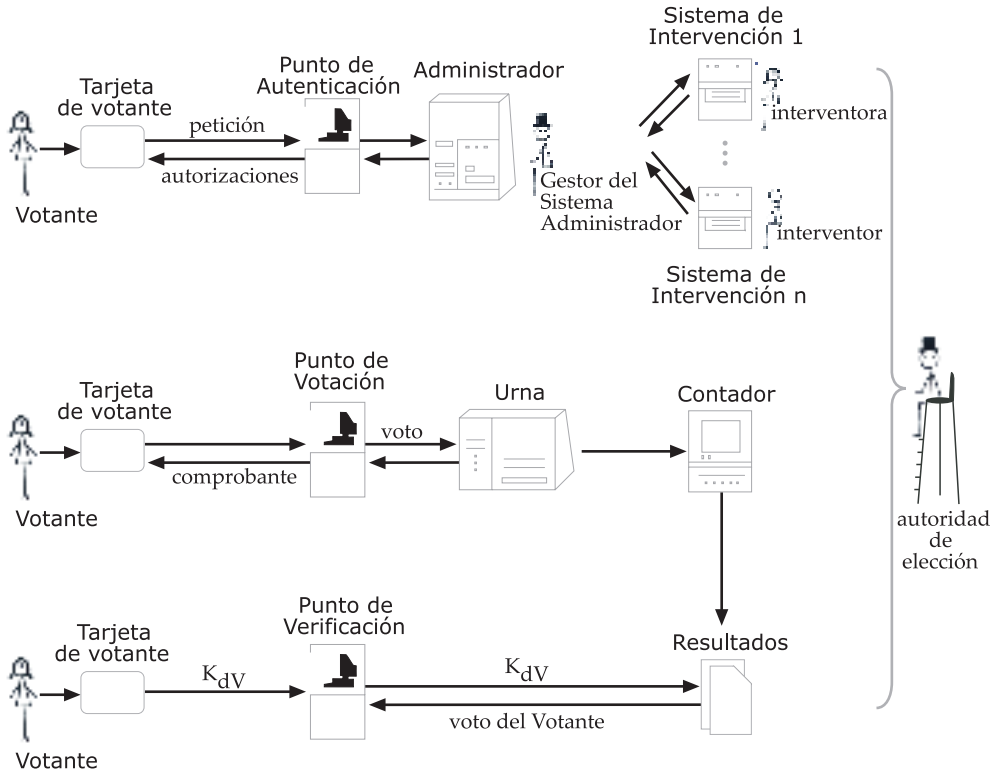

Figura 11.23. SistemaA completo.

que ejemplificamos en el epígrafe 11.1) sean protagonistas imprescindibles para que se pueda abrir la Urna y obtener la clave privada del Contador.

Esta presencia de los Interventores, que representan a las candidaturas o a agrupaciones de electores, puede servir, haciendo uso de toda la información complementaria que hemos ido comentando, para llevar a cabo una verdadera verificación global de los resultados. En efecto, con la intención de que los distintos Interventores obtengan una prueba del correcto funcionamiento del Contador, se le puede entregar a cada uno de ellos una copia de la lista generada por el Contador para que compruebe que son correctos los resultados finales publicados.

En realidad, se podría entregar a los Interventores la lista generada por la Urna para que la analizaran y evaluaran por sus propios medios. Ello no representaría ningún problema para garantizar el anonimato del voto debido a las protecciones criptográficas robustas de esos registros. Pero, como comentamos antes, lo que hoy se puede garantizar puede ser vulnerado años después cuando la evolución de la criptografía lo permita.

Para evitar ese riesgo, la *Verificación global* debe llevarse a cabo de forma que la copia de la lista que se entrega a los Interventores se cargue en las mismas máquinas en las que residen los Sistemas de Intervención (que forman parte del Sistema), que podrán ser previamente auditadas por peritos de confianza para comprobar que solamente sirvan para llevar a cabo las operaciones que tienen encomendadas y que no puedan almacenar información en discos u otros dispositivos periféricos.

Se deberá establecer un periodo de vigencia tanto para las listas de registros generados por el Contador como para las listas de información entregadas a cada candidatura, de manera que, una vez transcurrido el tiempo estipulado para permitir la verificación individual y la verificación global, toda esa información sea destruida de forma auditada (al igual que en las votaciones convencionales se destruyen las papeletas).

Con los añadidos analizados en los últimos apartados, puede deducirse que el SistemaA (u otro sistema que sea capaz de responder positivamente a los interrogantes que nos hemos ido planteando) cumple bastante satisfactoriamente los diez primeros requisitos enunciados en la relación que estamos usando de referencia. En la Figura 11.23 se muestra el escenario completo de este sistema simplificado al que, a efectos de su utilización didáctica, hemos dado en denominar SistemaA. Podríamos decir, incluso, que un sistema de votación telemática tal que este ofrece bastantes más garantías y seguridades que un sistema de votación mediante papeletas.

¿Y el otro sistema (el SistemaB) que estábamos usando como referencia didáctica para analizar las funcionalidades que debe cubrir un sistema de votación? Habíamos visto que cubre moderadamente bien los requisitos que condicionan la fase da autenticación y autorización, así como que cumplía deficitariamente los que condicionan la fase de entrega de voto. Una vez vista la información que, en el SistemaA, el Contador pone en conocimiento del Gestor del Sistema Administrador, de la Autoridad de Elección y de los Interventores, se deduce que el posible conocimiento que el Votante del SistemaB puede adquirir acerca del valor de la clave de descifrado de voto, k_{dV}, hace que una solución tal que esa posibilitaría la coacción y la venta de votos. Será necesario, por tanto, buscar soluciones que no exhiban la k_{dV} de forma tan manifiesta. Es posible encontrar soluciones que, aunque no de forma tan robusta como la descrita para el SistemaA, sirvan para cubrir esta exigencia. Por razones de espacio y de oportunidad, soslayaremos aquí analizar y evaluar estas posibles soluciones.

Bástenos aquí la descripción que de estos sistema hemos hecho. Nuestro objetivo inicial no era conocer cómo funcionan estos dos ejemplos simplificados sino apoyar-

nos en ellos para discutir acerca de los requisitos y exigencias que demandan los sistemas de votación telemática. El objetivo didáctico de estos análisis es, como antes decíamos, contribuir a que el lector esté en condiciones de aplicar esos criterios para evaluar los distintos sistemas de votación telemática que se le presentan en la actualidad y los que se le presentarán en un futuro.

En el siguiente y último apartado de este epígrafe comentaremos otros requisitos y exigencias que también es necesario tener en cuenta a la hora de proponer este tipo de sistemas de votación.

OTRAS CARACTERÍSTICAS Y REQUISITOS DEL VOTO TELEMÁTICO

En los apartados precedentes hemos estado discutiendo acerca de las características que deben tener los sistemas de votación telemática para dar satisfacción a algunos de los requisitos demandados. De hecho, nos hemos centrado sobre los nueve primeros requisitos (los que conllevan mayores retos desde un punto de vista tecnológico) y hemos tocado de pasada el requisito número 10 relativo a la movilidad de los votantes.

También hemos tenido muy en cuenta la salvaguarda que representa no guardar registros criptográficos que en el momento de la votación son computacionalmente muy seguros pero que pasados unos años pueden dejar de serlo.

Dos aspectos tecnológicos que no se han abordado adecuadamente en la descripción que antes se ha hecho son los relacionados con la imposibilidad de colusión entre los agentes del sistema y los fallos que pueden producirse en las comunicaciones (ambos incluidos en el requisito de *fiabilidad*). En cuanto al primero de ellos, antes de dar por bueno un sistema de votación telemática será necesario analizar detenidamente todas las condiciones de riesgo que pueden presentarse y analizar las protecciones que tiene implementadas el sistema para evitar que eso pueda producirse. En cuanto al segundo, será necesario especificar con precisión los protocolos telemáticos en los que se soporta el sistema y las medidas de recuperación ante posibles fallos que puedan producirse en las comunicaciones y que dejen «a medias» cualquiera de los procesos de intercambio de datos y claves que antes hemos comentado.

Pero quedan otros requisitos (once, según la relación en que nos estamos apoyando, si incluimos entre ellos el de *movilidad de los votantes*) que también deben ser satisfechos por los sistemas telemáticos que pretendan ser candidatos a sustituir a los actuales sistemas convencionales de votación mediante papeletas. ¿Podemos calificar como «menores» a estos requisitos porque no se traduzcan en mecanismos de seguridad avanzados e ingeniosos? Responder afirmativamente a esta pregunta sería caer en el error «tecnocéntrico», tan común, de considerar poco importante todo lo relacionado con los condicionantes sociopolíticos que marcan la implantación de los sistemas presentes en la Sociedad de la Información. La realidad es bien distinta: serán precisamente esos condicionantes los que determinen en mayor medida la viabilidad o improcedencia de los sistemas propuestos.

Este es un texto dedicado a la ingeniería de seguridad en redes telemáticas y, por cuestión de oportunidad, debe prestar mayor atención a los temas más directamente relacionados con esa temática, pero es necesario avisar al lector de la importancia que tienen todos esos otros temas. Consecuentemente, recomendamos a quienes pretendan abordar la implantación de sistemas de votación telemática el análisis detenido de estos requisitos y de las fuentes documentales en que se apoyan. Bástenos, no obstante, aquí, hacer una breve referencia a algunos de los aspectos que consideramos más llamativos.

El requisito de movilidad de los votantes presenta facetas muy interesantes. Tanto en el SistemaA como en el SistemaB que hemos estado utilizando como ejemplo hemos supuesto la existencia de **una sola** Urna, pero en un sistema de votación a gran escala parece razonable que existan distintos distritos electorales y distintas *mesas* electorales. En el caso de España, el actual sistema electoral divide a los electores en *mesas* atendiendo a cuestiones de distribución geográfica, de tal forma que el número de electores que depositan su voto en una urna concreta no sea excesivo (el tope suele imponerse en torno a los 1.000 electores) para posibilitar las posteriores tareas de recuento. Pero en una votación telemática una sola Urna puede atender a bastantes más electores, dependiendo de cómo se dimensione. No obstante, habrá que tener en cuenta problemas de congestión para asegurar el *voto rápido*. Además, en la actualidad se conocen los resultados parciales por mesa y por distritos, y en un futuro la reglamentación de la votación telemática deberá determinar en qué medida ese conocimiento parcial es conveniente o perjudicial, determinando en base a ello la agrupación de los electores en colegios electorales y en urnas. Y esa es una decisión política muy importante.

En la actualidad, los votantes, para depositar su voto, tienen la obligación de acudir al espacio físico en el que se ubica su colegio electoral. Por contra, en un sistema de votación telemática, aunque el Votante tenga que acudir a votar a las distintas cabinas en las que se concentran los puntos de votación, y aunque el voto se deposite en la Urna lógica que corresponda a la «mesa» en la que esté inscrito, el Votante podrá acudir a cualquier cabina de las existentes, independientemente del lugar geográfico en el que se encuentre.

Otro aspecto directamente relacionado con el anterior es el relativo al periodo de tiempo que puede durar el proceso electoral hasta que se dé por cerrada la votación y se proceda al recuento de los votos. En la actualidad esa duración está condicionada por el aguante que cabe esperar de todas la personas que actúan simultáneamente en el proceso, pero en un sistema de votación telemática ese tiempo puede ser mucho mayor, aunque exista la figura del Interventor, ya que la supervisión del sistema puede organizarse a través de equipos de supervisores coordinados entre sí. También es este un tema políticamente muy sensible (con repercusiones técnicas y organizativas) que deberá ser abordado en la reglamentación que en su día se apruebe.

Conviene remarcar que para que se pueda hablar con propiedad de sufragio universal dentro de la Sociedad de la Información será necesario tomar medidas de alfabetización digital que den como resultado la *igualdad de oportunidades en la votación,* de tal manera que se minimicen las diferencias que en tal sentido puedan existir entre ciudadanos procedentes de distintos estratos sociales.

Para cerrar estos comentarios, seleccionemos el condicionante reflejado en el requisito reseñado con el número 14. Se trata del que preconiza que el código fuente de todos los programas debería ser conocido y verificable por todos los auditores y supervisores presentes en el sistema. Podría añadirse algo más: debería estar publicado en el Boletín Oficial del Estado (o en un documento allí referido). Es razonable que todas las personas y todas las empresas que participan en los procesos de votación convencionales (fabricando urnas, montando instalaciones y trayendo y llevando papeletas y resultados) sean compensadas económicamente de forma adecuada. Pero lo que no parecería de recibo es que los procedimientos reglamentados fuesen propiedad de nadie que no sea el propio Estado.

Paralelamente, en la plasmación telemática de las votaciones oficiales, la definición de los sistemas, los procedimientos organizativos y el comportamiento definido en los programas informáticos deben ser conocibles y evaluables por la ciu-

dadanía en general y estar bajo titularidad pública. Todo ello sin menoscabo de que, como ocurre en los procesos convencionales, cada cual reciba una compensación proporcional a su esfuerzo y dedicación, pero nada más. Otra cosa bien distinta serán los sistemas de votación desarrollados e implementados para dar satisfacción a la demanda que existe en diversos sectores privados (empresariales, deportivos, culturales, etc.), en los cuales las cosas se regirán según las consabidas y difícilmente evitables reglas del mercado.

11.7. LA TARJETA COMO ELEMENTO CONSTITUTIVO DE LOS SISTEMAS QUE PROPORCIONAN SERVICIOS DE ANONIMATO

De lo que hemos visto en epígrafes anteriores acerca de los escenarios que se presentan en aplicaciones como las de voto telemático o comercio electrónico se deduce que, en los sistemas que hemos tomado como modelo, la tarjeta inteligente aparece, en todos ellos, como un elemento constitutivo del sistema global.

No es que esto tenga que ser necesariamente así, pero dado lo rigurosos que son los requisitos que deben cumplir estos sistemas, la experiencia dicta que las soluciones que incluyen tarjetas inteligentes ofrecen muchísimas posibilidades para conjugar el doble requisito de autenticación de la persona que accede al sistema y la garantía de anonimato en algunas de las operaciones que allí se llevan a cabo.

En los dos apartados que siguen vamos a prestar atención a dos aspectos muy importantes de esa presencia de la tarjeta inteligente en la arquitectura global del sistema:

a) La autenticación del usuario ante **su** tarjeta. Esta deberá ser siempre una fase preliminar. Con posterioridad, el usuario tendrá o no que autenticarse ante el Sistema global, pero inicialmente es insoslayable que se garantice que solamente la persona legítimamente propietaria puede usar una tarjeta inteligente concreta.
b) Contribución de la tarjeta inteligente en el soporte de la Aplicación Cliente. Para utilizar una nomenclatura que nos permita hablar con soltura de las distintas partes de un sistema (complejo o no), denominaremos Aplicación Cliente a aquella que utiliza la Persona Usuaria para acceder a los servicios del Sistema global. Como veremos más adelante, son posibles varias alternativas a la hora de definir esa participación.

AUTENTICACIÓN ANTE LA TARJETA

De todo lo visto se deduce el gran interés que tienen las tarjetas inteligentes como elementos constitutivos de los sistemas que estamos analizando. Pero tienen un talón de Aquiles: la posibilidad de que alguien malicioso consiga la tarjeta de la que es titular otra persona y consiga autenticarse como legítimo titular de ésta.

Por remota que sea esta posibilidad, caso de producirse, echaría abajo todo el edificio que hemos venido montando en torno a considerar a la tarjeta inteligente como el testigo de seguridad más idóneo para almacenar la clave privada del titular. Si un usuario malicioso consigue este propósito (por descuido o por fuerza) puede realizar firmas y operaciones en la red de las que sería responsable administrativa y

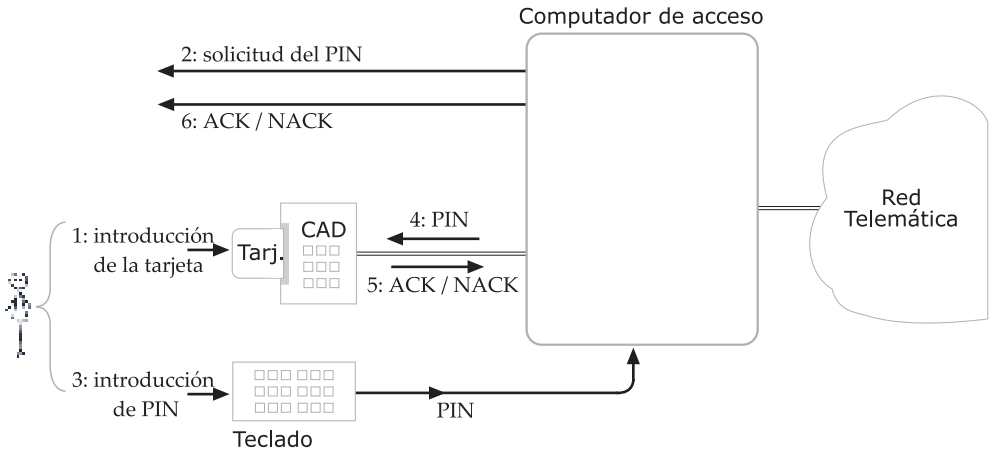

Figura 11.24. Autenticación del titular mediante PIN a través del computador.

judicialmente la entidad propietaria de la tarjeta. Y esto es así porque, en la Red, la clave privada actúa como un *alter ego* de su titular.

Por ello, los mecanismos de autenticación del usuario ante su tarjeta merecen toda nuestra atención. Como ya comentamos en el Capítulo 2, los más plausibles (en la doble acepción de la palabra) son el uso de un PIN o contraseña y el uso de mecanismos biométricos (principalmente los basados en huella digital).

Una cosa que hay que dejar clara es que en el proceso de autenticación del titular de una tarjeta ante su propia tarjeta, cuantos menos elementos intermediarios intervengan, tanto mejor. Es imprescindible que intervengan algunos porque la tarjeta inteligente no dispone de periféricos propios, así que «alguien» se los tendrá que proporcionar (aunque, según comentaremos más adelante, dentro de los procesos de mejora y evolución de las tarjetas inteligentes, una de las tendencias que existen es la de ir dotando de periféricos elementales a las tarjetas, convirtiéndolas, así, en dispositivos semiautónomos).

Un esquema clásico para este tipo de autenticación es, con algunas variaciones, el representado en la Figura 11.24. El computador, tras detectar que el titular ha introducido la tarjeta en el dispositivo de lectura-escritura (CAD), solicita que sea introducido el PIN a través del teclado. El computador envía el PIN recibido a la tarjeta y la aceptación o no (ACK o NACK) de la tarjeta se la comunica a la persona propietaria de ésta. En este esquema quien tiene el número secreto y quien realiza la comprobación es la tarjeta, pero el computador hace de intermediario y puede adquirir información muy sensible para la seguridad de la persona propietaria de la tarjeta. En efecto, un atacante malicioso puede alterar el normal funcionamiento del computador y capturar así el número secreto que le permitirá, consiguiendo la tarjeta, suplantar la personalidad de su legítimo titular.

Este esquema mejoraría notablemente si el teclado se comunicase directamente con la tarjeta a través del CAD (sin pasar a través del computador). De esta forma se acorta el camino y las posibilidades de ataque, ya que es más difícil y menos fiable proteger el programa del ordenador que gobierna el proceso representado en la Figura 11.24 que proteger el teclado y el CAD. Y si el CAD está integrado con el teclado en un subsistema autónomo, tanto mejor.

La autenticación mediante PIN se podría sustituir o reforzar mediante una autenticación biométrica, que es algo mucho más fiable. Según los entendidos, el análisis del

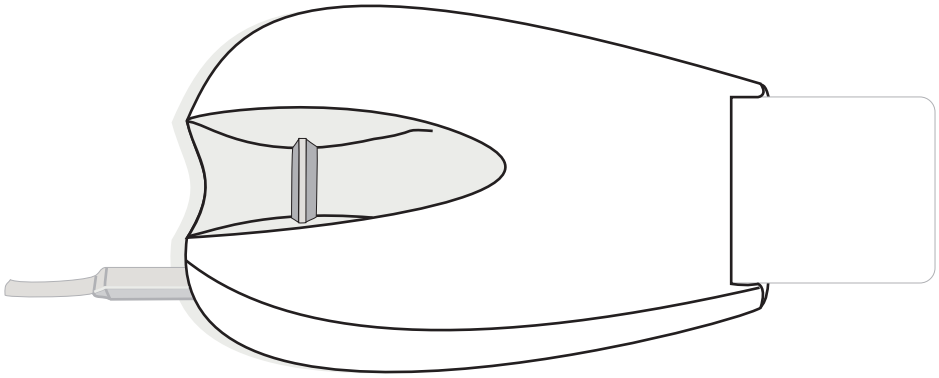

Figura 11.25. Lector de tarjeta con lector de huella incorporado.

iris del ojo es de las pruebas que mayor garantía ofrecen, debido a lo preciso de la información que aporta y al hecho de que se puede comprobar que no se trata de una muestra estática sino que la observación se está realizando sobre una persona «viva». No obstante, dentro del campo de la autenticación biométrica en tarjetas inteligentes, el análisis de la huella dactilar es la técnica que tiene mayor predicamento.

Esto es así porque al ser la tarjeta un componente manejable con la mano (valga la redundancia semántica) la autenticación mediante la huella de los dedos propicia un escenario bastante ergonómico y fácil de plantear. Aunque es relativamente sencillo capturar maliciosamente huellas dactilares de personas a las que se quiere suplantar la personalidad, la configuración de los lectores y de los escenarios donde se realice la comprobación puede ayudar a minimizar este riesgo. Así, algunos lectores de huella obligan a que el dedo sobre el que se tome la muestra se deslice sobre una especie de banda estrecha y en relieve (Figura 11.25), lo cual requiere que exista algo de movimiento y «vida» en el sujeto evaluado. (A buen seguro que a medida que avance el tiempo se irán introduciendo de forma creciente procedimientos ingeniosos que sirvan de salvaguarda contra los también ingeniosos métodos que puedan ocurrírseles a los atacantes para falsificar la prueba.)

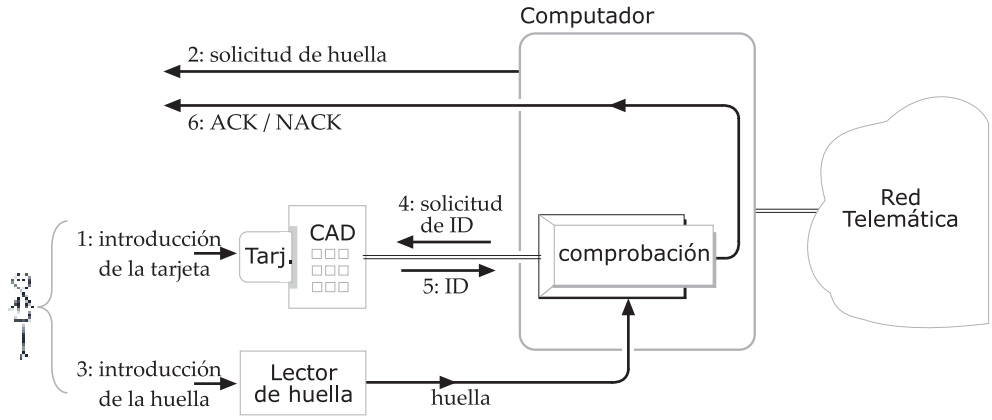

Figura 11.26. Autenticación mediante huella y verificación en el computador.

En la Figura 11.26 se representa un posible esquema para realizar la autenticación del titular de una tarjeta inteligente mediante análisis de la huella dactilar. En este caso, la huella está almacenada en el computador, el cual, al mismo tiempo que le solicita a la persona propietaria de la tarjeta que introduzca su huella dactilar, le solicita a la tarjeta un identificador que pueda permitirle verificar la validez de la huella.

Por las razones antes dichas, este esquema es muy poco atractivo de cara a las aplicaciones a las que antes hemos hecho referencia. En estos casos, en los que frecuentemente se requiere en alguna medida un servicio de anonimato, lo que debe plantearse es aprovechar las ventajas que proporcionan las técnicas biométricas, pero teniendo muy presente que hay que preservar los derechos de los ciudadanos que participan en esas comunicaciones. Por ello, será necesario minimizar lo más posible los problemas que puede acarrear la introducción masiva de muestras biométricas que vulneren la intimidad de los ciudadanos y la privacidad de sus actuaciones en la Red [14].

Así pues, para garantizar esta privacidad resulta necesario que se realice dentro de la tarjeta la comparación entre la huella suministrada por la persona que se dice propietaria de la tarjeta y el patrón almacenado. Con esta funcionalidad, que se conoce en inglés como *match-on-card*, lo que se consigue es que sea la propia tarjeta la que compruebe que la huella de quien accede coincide con la que en su momento se tomó a la persona legítimamente propietaria de la tarjeta. Ello implica que en el momento de personalización de la tarjeta, antes de entregársela a su titular, será necesario almacenar la huella dentro de ella.

Un escenario para plasmar esta comprobación de la huella podría configurarse de forma semejante al representado en la Figura 11.24 (en ese caso la comprobación del PIN también se hace en la tarjeta, aunque ya comentábamos allí que sería más conveniente independizar la comunicación entre el lector del PIN y el CAD). Para materializar esa independencia, en el caso de la huella, casi siempre que se utiliza una verificación *match-on-card* lo que se hace es emplear un solo dispositivo (de aspecto similar a un ratón) en el que se integran el lector de huella y el CAD. En la Figura 11.27 se representa esquemáticamente una situación de este tipo en la que se ha

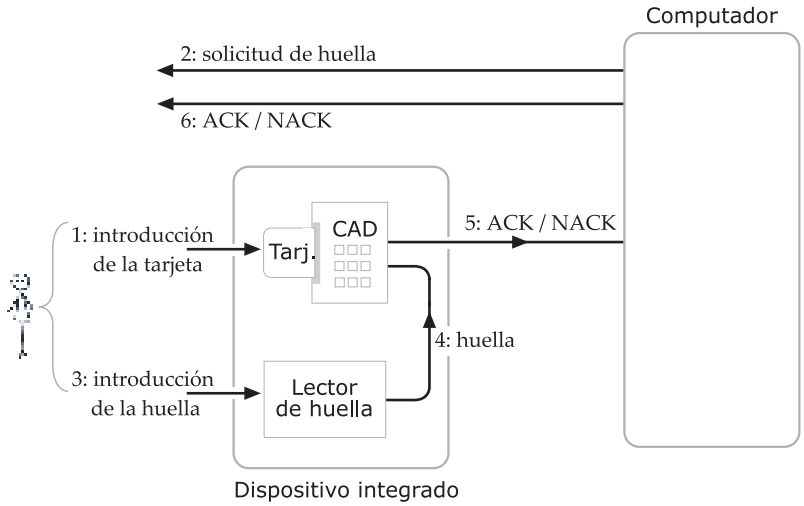

Figura 11.27. Autenticación mediante huella y comprobación de coincidencia en la tarjeta (match-on-card).

supuesto que el computador solicita la introducción de la huella e informa del resultado, pero este paso también se puede eliminar, porque el lector puede informar directamente (mediante una señal luminosa) del éxito o fracaso de la autenticación.

Para rizar más el rizo, se puede plantear incluso incrustar el lector de huella **en** (más bien **sobre**) la propia tarjeta de plástico. En este caso, la comunicación entre el lector y el microcomputador que constituye realmente la tarjeta inteligente se realiza por dentro de la tarjeta de plástico a través de un bus interno. Algunos de los fabricantes que ofrecen estos componentes emergentes los denominan *system-on-card*. Esta opción tiene la ventaja evidente de reducir al mínimo el riesgo de captura fraudulenta de la huella del titular, pero tiene dos inconvenientes: uno es el precio de la tarjeta (que se vería incrementado con el precio del lector de huella incorporado) y el otro inconveniente es que el grosor de la tarjeta en la zona donde está el lector es bastante mayor que el normalizado para todas las tarjetas conformes con la norma ISO 7816.

Algunos van más lejos y proponen incorporar también a la tarjeta una pequeña pantalla visualizadora en la que podrían aparecer, por ejemplo, el grupo sanguíneo y los medicamentos a los que es alérgica la persona portadora. Pero esto es en realidad un pequeño microcomputador portátil configurado en forma de tarjeta inteligente. Por el tipo de ejemplo que hemos puesto para justificar la posible utilidad de estos emergentes dispositivos, podemos deducir que su campo de aplicación está alejado de las necesidades que es necesario cubrir en las aplicaciones telemáticas seguras.

Para centrarnos en el campo que nos interesa, adoptando una posición práctica y realista, podemos concluir que nos sería suficiente disponer de tarjetas inteligentes que permitiesen, además de ejecutar cierto tipo de programas, garantizar la autenticación de su titular por medio de un PIN o una prueba biométrica y que, en ambos casos, la comprobación de coincidencia la realice, dentro de la tarjeta, el microcomputador incorporado en ella.

Como ya hemos dicho, en el caso del PIN, este tipo de comprobación es posible llevarla a cabo en tarjetas inteligentes tradicionales, es decir, totalmente conformes con la norma ISO 7816 (en sus siete partes). Teóricamente, no hay problemas insalvables para conseguir que la autenticación de huella *match-on-card* se pueda realizar también en este tipo de tarjetas, pero en la práctica la mayoría de las tarjetas que son capaces de llevarla a cabo son del tipo Java Card.

En este caso, la Tarjeta Java deberá disponer de un API biométrico añadido al conjunto de elementos que componen el entorno de ejecución Java Card (JCRE).

LA APLICACIÓN CLIENTE

Como antes decíamos, denominaremos Aplicación Cliente a aquella que utiliza la Persona Usuaria para acceder a los servicios del Sistema global. La Aplicación Cliente será, por tanto, una parte de la aplicación completa. El Sistema podrá proporcionar diversos servicios, a cada uno de los cuales se accederá con una Aplicación Cliente específica.

En la Figura 11.28 se representa el segmento de un escenario en el que la Aplicación Cliente está repartida entre el computador terminal del Sistema y la tarjeta inteligente. Es evidente que habrá muchos casos en los que la Persona Usuaria acceda directamente al Sistema sin necesidad de apoyarse en una tarjeta inteligente, pero, como ya hemos dicho, las situaciones que nos interesa analizar ahora son aquellas en las que sí es necesario el concurso de estos testigos de seguridad. En cualquier caso, la situación en la que no existiese una tarjeta inteligente para cooperar en la plasma-

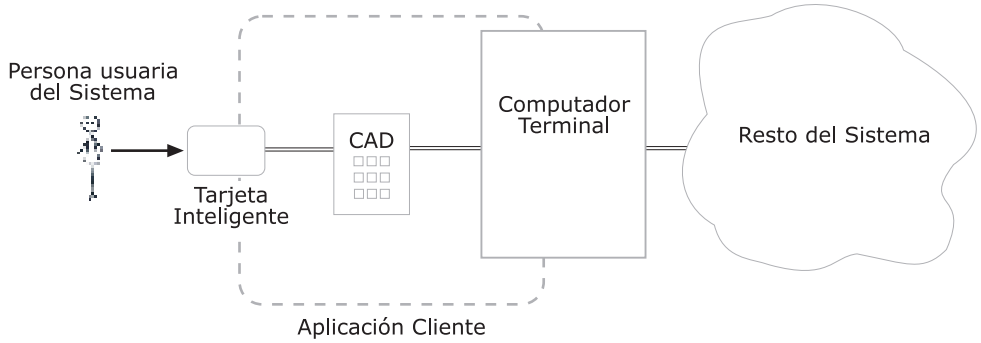

Figura 11.28. Acceso al Sistema mediante la Aplicación Cliente.

ción de la Aplicación Cliente sería un caso particular de la más general representada en la figura.

Como hemos visto anteriormente, en los distintos sistemas que hemos analizado para la provisión de servicios de voto telemático o comercio electrónico, la Persona Usuaria no accede siempre al mismo punto del Sistema global. Es decir, el computador terminal que se representa en la Figura 11.28 puede representar agentes telemáticos y puntos de acceso diversos, en los que residan entidades diversas. Por tanto, la que hemos llamado Aplicación Cliente es un caso genérico de las múltiples que pueden presentarse.

Dentro de una situación como esta podríamos a su vez distinguir tres casos:

a) La Aplicación Cliente se ejecuta casi en su totalidad en el computador terminal del Sistema. La tarjeta inteligente le sirve a la aplicación: a1) como un testigo de seguridad que guarda informaciones particulares y privadas de la Persona Usuaria; y a2) como simple auxiliar para la realización de pocas y específicas operaciones criptográficas. Más concretamente, la clave privada de la Persona Usuaria está almacenada en la tarjeta y **no viaja nunca** fuera de ella, de forma que cualquier operación de cifrado o firma que deba realizarse utilizando dicha clave deberá ser llevada a cabo, mediante los necesarios algoritmos criptográficos, **dentro** de la tarjeta.
b) La Aplicación Cliente se ejecuta mayoritariamente en el computador terminal pero también la tarjeta inteligente está involucrada directamente en la aplicación. Además de las tareas señaladas en el caso anterior, la tarjeta contiene datos propios de la aplicación, realiza autenticaciones de la entidad residente en el computador terminal, procesa o modifica los datos contenidos en su memoria en función de las APDUs que reciba y realiza internamente una parte importante de las operaciones criptográficas requeridas.
c) La Aplicación Cliente se ejecuta mayoritariamente en la tarjeta inteligente de forma que el computador terminal se comporta como un simple auxiliar de la tarjeta, sirviendo para: c1) prestar sus terminales de entrada-salida para posibilitar el diálogo y la interacción con la Persona Usuaria; y c2) albergar la entidad comunicante que gobierne el protocolo telemático seguro mediante el cual se relaciona con los restantes agentes del sistema.

En esta clasificación no se ha querido tener en cuenta el caso en el que la tarjeta inteligente actúa como un simple testigo de seguridad que guarda datos particulares de

la Persona Usuaria pero que no realiza operación criptográfica alguna. Además, esta división que acabamos de exponer no es absolutamente rigurosa ni conlleva que ante cualquier escenario que pudiera presentarse fuese inmediato averiguar a cuál de estos tres grupos pertenece. Posiblemente no sea este el caso y puede que el escenario en cuestión sea un híbrido entre algunos de los tres aquí señalados.

Para lo que sí nos va a servir esta clasificación es para permitirnos hacer una discusión acerca de los métodos necesarios para desarrollar la Aplicación Cliente en el acceso a los servicios telemáticos que sirven de soporte a la Sociedad de la Información.

a) La tarjeta como simple auxiliar

En este caso, la Aplicación Cliente reside en el computador terminal y la mayor parte de las tareas que lleva a cabo las realiza con recursos propios de esa máquina. Como tiene que ser capaz de soportar un protocolo seguro para comunicarse con el resto de los agentes telemáticos del Sistema, tendrá necesidad de realizar diversas operaciones criptográficas, para lo cual contará con una placa que contenga un módulo criptográfico, o bien con una librería contenida en un fichero lógico.

Una opción es desarrollar el programa que gobierna la aplicación en un lenguaje de alto nivel (también existe, en teoría, la posibilidad de codificarlo en lenguaje de ensamble, pero esto resulta mucho más tedioso) y, posteriormente, compilarlo y cargar el ejecutable en el computador terminal. Otra alternativa puede ser diseñar la aplicación para que resida en un determinado servidor y recuperarla en el momento oportuno mediante un proceso de telecarga usando, por ejemplo, tecnología Java. En este último caso sólo sería necesario que en el computador terminal residiese de forma fija un pequeño programa que fuese capaz de conectar con el servidor y descargar la Aplicación Cliente [15].

La tarjeta inteligente que se requeriría para un escenario de este tipo podría ser una tarjeta convencional (de las que hemos estado denominando tradicionales) en la que el proceso de personalización consistiese básicamente en introducir en ella unos cuantos datos y parámetros particulares de la persona titular de la tarjeta. También podría ser una Tarjeta Java, pero sería más cara y necesitaría trabajos de desarrollo adicionales.

Entre los datos guardados en la tarjeta cabría incluir, al menos, un par de claves (pública y privada) que le permitan actuar como entidad comunicante dentro del Sistema. (Como ya hemos apuntado en otras ocasiones, si la tarjeta lo permite, sería conveniente que la Persona Usuaria generase por su cuenta un nuevo par de claves y enviase la nueva clave pública a la Autoridad de Certificación adecuada para que generase el correspondiente certificado.)

En este caso, los datos almacenados en el proceso de personalización no cambiarán dinámicamente de forma significativa durante la ejecución de la Aplicación Cliente, por lo que la utilización que ésta haga de la tarjeta se limitará a lo que posibilite un sencillo API (*Application Programming Interface*) que proporcione el fabricante. En cuanto a las operaciones criptográficas se refiere, una buena solución es que este API sea compatible con la PKCS#11 de RSA (*Cryptographic Token Interface Standard*) que especifica un API normalizado para acceso a dispositivos (tarjetas inteligentes, por ejemplo) que guardan información criptográfica y llevan a cabo operaciones criptográficas.

b) Una tarjeta especialmente diseñada (e involucrada en la aplicación)

Un paso adelante en este asignar atribuciones a la tarjeta inteligente se presenta cuando, al diseñar el Sistema completo en el que se lleva a cabo la aplicación de que se trate, se llega a la conclusión de que la seguridad del Sistema global y la garantía del anonimato en algunas de las operaciones en las que participa la Persona Usuaria del Sistema mejorarían notablemente si algunas de las tareas que tiene que realizar la Aplicación Cliente se llevasen a cabo dentro de la tarjeta.

De esta forma, se puede conseguir que algunos de los datos resultantes de esas operaciones que se realizan en la tarjeta no viajen fuera de ésta, evitando así que pueda adquirir información sobre ellos el propio computador que actúa como terminal del Sistema ante el usuario final. En principio, cabe suponer que todos los agentes telemáticos que intervengan en el proceso sean honrados y que se diseñarán mecanismos técnicos y procedimentales para garantizarlo. Pero una idea útil en seguridad es que la mejor manera de fiarse de todo el mundo es no fiarse de nadie (o fiarse del menor número posible de cosas).

Piénsese además que, con frecuencia, las aplicaciones en las que se van a ver inmersos los ciudadanos, dentro de las comunicaciones presentes en la Sociedad de la Información, serán tales que la máquina ante la que tiene que autenticarse y operar la persona propietaria de la tarjeta pertenecerá a una organización sobre la que ella no tiene ningún tipo de control y, las más de las veces, ante la que tiene que establecer salvaguardas.

Sea como fuere, llegado el caso que estamos suponiendo, los diseñadores de la aplicación pueden contemplar la posibilidad de utilizar una tarjeta inteligente tradicional procurando sacarle el mayor partido posible a las funcionalidades que ofrece (por ejemplo, aprovechando inteligentemente la gestión del sistema de ficheros) y especificando algunas pocas funcionalidades complementarias [Dieg00] que deben ser programadas e incluidas en la memoria interna.

Habida cuenta que el microcomputador insertado en la tarjeta es una máquina de propósito general, esta tarea de programación es perfectamente posible. Pero, ¿quién tiene acceso a llevar a cabo esa programación? Por regla general, las tarjetas convencionales (conformes con la totalidad de la ISO 7816) que pueden adquirirse vienen ya con los programas grabados, y solamente podrán abordar esa tarea quienes tengan acceso a la estructura interna de su sistema operativo y al tipo de instrucciones soportadas por el microprocesador. Y eso es algo que, también por lo general, está fuera del alcance del equipo de diseñadores responsables de la aplicación global.

Así pues, tendrán que pedir a un fabricante de tarjetas (de primera o de segunda fuente) que programe en código nativo (Figura 11.29) esas nuevas tareas e instale esos pequeños añadidos en el programa previamente grabado en la memoria EEPROM de la tarjeta. Por eso decimos que en este caso se trataría de *una tarjeta especialmente diseñada para la aplicación* (aunque esta tarjeta también podría seguirse usando de forma convencional). Obviamente, cuanto más ligeros sean los cambios, más sencillo será realizar esa especialización.

Otra alternativa será usar una Java Card y diseñar las applets necesarias. De eso es de lo que hablaremos a continuación.

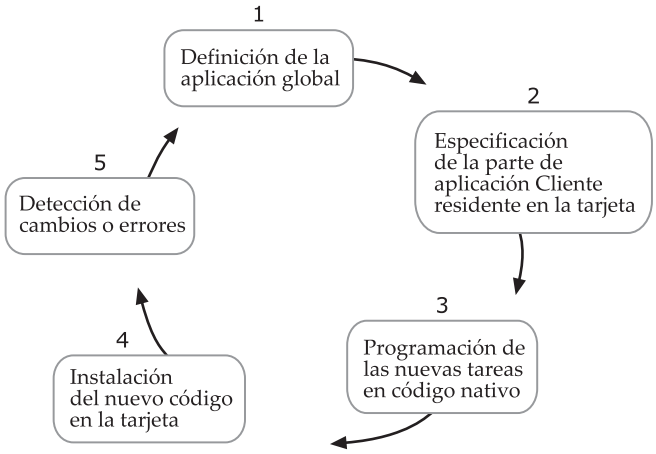

Figura 11.29. Proceso de instalación de nuevas funcionalidades en la tarjeta tradicional.

c) La Aplicación Cliente reside mayoritariamente en la tarjeta

Continuando con el razonamiento expuesto en los últimos párrafos, si lo que se desea es que, por las razones antes aducidas, la tarjeta se haga cargo de la mayoría de las tareas, la opción de implementarla directamente sobre una tarjeta tradicional sólo puede ser llevada a cabo por quienes tengan acceso a la configuración bajo la que está fabricada dicha tarjeta.

A veces, quienes diseñan una aplicación global medianamente evolucionada (por ejemplo, los sistemas que en epígrafes precedentes hemos denominado Sistema1, Sistema2 y SistemaA) deciden que la parte de la Aplicación Cliente que resida en la tarjeta inteligente se comunique con el computador terminal conforme a un protocolo condicionado por resultados intermedios, que use internamente determinadas funciones criptográficas y que sea capaz de manejar estructuras de datos sencillas.

Como hemos dicho, podría optarse por un proceso similar al representado en la Figura 11.29. Suponiendo que se encontrase alguna empresa fabricante dispuesta a hacerlo, esta opción sólo sería viable económicamente si el número de tarjetas modificadas es muy elevado. Además, el programa de la Aplicación Cliente deberá ser suficientemente estable y deberá estar exhaustivamente probado, porque cualquier detección de errores o necesidades de cambio conllevaría (Figura 11.29) iniciar de nuevo el proceso.

Por todo ello, en ese caso, lo razonable es pensar en Tarjetas Java y en programar una o varias applets residentes en la tarjeta.

Según hemos comentado en el apartado *Estructura y funcionamiento de las Tarjetas Java* (epígrafe 11.2), este tipo de dispositivos permite que la aplicación sea programada y compilada en un sistema de desarrollo convencional y posteriormente instalada dentro de la tarjeta para realizar las tareas previstas en cooperación con la máquina virtual y con todos los componentes que constituyen el entorno de ejecución Java Card (JCRE).

En la Figura 11.30 se representa el proceso mediante el cual una applet es generada e introducida en la tarjeta. Como resultado de la compilación del código fuente,

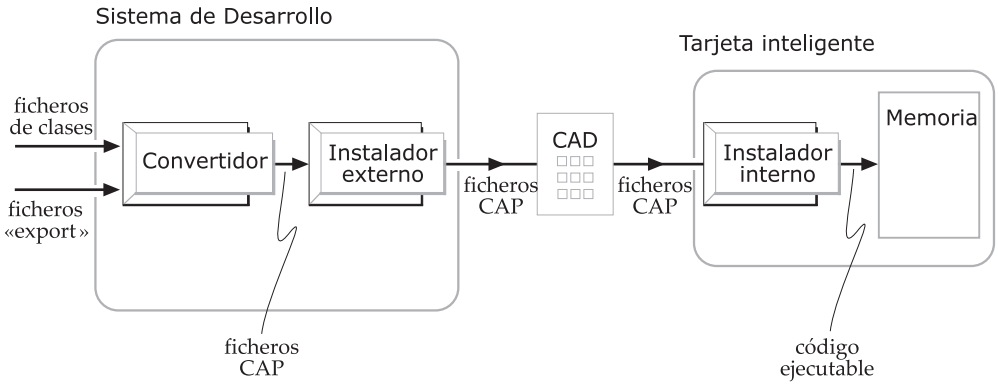

Figura 11.30. Proceso de introducción de una applet en la tarjeta Java.

se habrán generado los ficheros que contienen las distintas clases o módulos en que está descompuesta la aplicación. Para introducirlos en la tarjeta (debido a las particularidades de Java Card con respecto a los entornos de ejecución Java residentes en sistemas informáticos convencionales) es necesario transformarlos a través de un programa Convertidor (*Converter*) que genera unos ficheros denominados *CAP* (*converted applet*) que son los que se transfieren al programa instalador para que los almacene en la memoria de la tarjeta.

Para realizar esa transformación, el Convertidor no sólo parte de la información contenida en los ficheros de clases, sino también en unos ficheros, denominados ficheros *export*, que contienen la información de otras clases que la aplicación necesita incorporar para su correcta ejecución. Como se refleja en la Figura 11.30, la tarea de instalación se lleva a cabo mediante la cooperación de dos programas instaladores (uno residente en el sistema de desarrollo y el otro en la tarjeta) que se comunican a través del dispositivo de lectura-escritura en la tarjeta (CAD).

Aunque lo que antecede es una explicación muy resumida y algo imprecisa de todo el proceso que es necesario llevar a cabo para la generación de las applets necesarias (una descripción más pormenorizada puede encontrarse en las referencias indicadas en el epígrafe 11.2), sí nos sirve para hacernos una idea de las posibilidades y limitaciones que se nos presentan a la hora de abordar el diseño de la Aplicación Cliente y la posibilidad de que, en mayor o menor parte, resida en la tarjeta inteligente.

La gran diferencia entre el computador y otros automatismos consiste en que posibilita que el usuario determine su funcionamiento mediante el diseño y posterior almacenamiento en memoria de un programa. Las tarjetas tradicionales, aunque en realidad están constituidas por un microcomputador programable, en la práctica se presentan ante el diseñador de aplicaciones como un dispositivo bastante «cerrado» y difícil de programar. La Tarjeta Java, en cambio, se nos ofrece como una máquina «casi vacía» que nos permite inventar comportamientos y plasmarlos a través de programas.

11.8. PLATAFORMAS PARA LA DEMOCRACIA DIGITAL

La penetración de las nuevas tecnologías y del uso de los ordenadores se hace cada vez más patente en todos los ámbitos de la vida de los ciudadanos. Sin duda, la

creciente aparición de la Sociedad de la Información debe conllevar la utilización de estas nuevas tecnologías como herramientas que sirvan para impulsar el progreso de los derechos civiles, de la economía y de la sociedad.

La expansión del uso de Internet, tanto en su implantación como en las funcionalidades y servicios utilizados, ha dado lugar al surgimiento en todo el planeta de gran número de iniciativas y nuevas propuestas de infraestructructuras telemáticas para ser utilizadas en la administración de nuestros sistemas políticos. No pocas veces estas nuevas propuestas no son sino adaptaciones de antiguas propuestas teóricas, impracticables en el pasado, pero que, apoyándose en las nuevas tecnologías, es posible considerarlas actualmente como viables.

Todas estas iniciativas y propuestas se consideran como elementos que contribuyen a la implantación de lo que se denomina *Democracia Electrónica* o *Democracia Digital* (aquí, por razones similares a las que nos han llevado a aceptar el término *voto telemático*, preferiremos utilizar la segunda de estas dos denominaciones). No obstante, cuando se hace referencia a Democracia Digital, nos encontramos con que bajo esta acepción conviven diversas concepciones e interpretaciones. Veamos algunas de ellas.

DIFERENTES TIPOS DE PLATAFORMAS

De forma general, podríamos clasificar los sistemas de Democracia Digital en distintas categorías dependiendo de las funcionalidades que sean capaces de soportar las plataformas que pretendan dar servicios de democracia. De menor a mayor rango de funcionalidades, esta clasificación de plataformas podría establecerse de la siguiente manera:

a) Aquellas que utilizan el término Democracia Digital simplemente para referirse a procesos de «ventanilla electrónica», es decir, la sustitución del trámite de papeleo burocrático presencial por un formato telemático (en su concepción mínima, a veces se trata simplemente de páginas web de consulta). Aunque su incorporación representa una mejora indudable en la gestión pública y en la relación de los ciudadanos con la Administración, es evidente que este tipo de plataformas resultan, hoy en día, bastante insuficientes (aunque estadísticamente sean las que mayor presencia tengan).
b) Otro tipo de plataformas son aquellas en las que se tiende a identificar Democracia Digital con la traslación al ciberespacio de los procesos de votación tradicionales. En ellos, los ciudadanos eligen representantes, o bien eligen entre opciones previamente especificadas, bajo el modelo de referéndum. La mayoría de las propuestas en torno a lo que hemos denominado *voto telemático* caen bajo esta acepción, identificando miméticamente *voto* con *democracia*. Aunque en la discusión que se presenta en los epígrafes 11.5 y 11.6 se repite varias veces que el voto telemático debe ofrecer mayores posibilidades que el voto convencional mediante papeletas, lo cierto es que en la descripción de sistemas que allí se realiza predomina esta concepción tradicional del voto.
c) Una tercera categoría podría estar constituida por aquellas plataformas que, aprovechando las facilidades que dan los protocolos telemáticos, posibilitan el uso de procedimientos de votación que resultarían impracticables usando métodos convencionales. Por ejemplo:

c1) *Opciones de condicionalidad*. La ciudadanía debería estar en disposición de responder condicionalmente a la consulta que se realiza. Por ejemplo, en preguntas múltiples, debería poderse responder: si ocurre (o gana) *x*, entonces voto por *y*; pero en ausencia de *x*, no apoyo *y* sino que propongo *z*. El uso de sistemas informáticos en el escrutinio podría permitir el cómputo de preguntas condicionadas tan complejas como se quisiese. En los sistemas convencionales, la ausencia de condicionalidad en la respuesta ha permitido a ciertos políticos plantear algunos referendos de forma tramposa.

c2) *Opciones de elección múltiple o reiterada.* Los sistemas telemáticos podrían permitir un sistema de consultas reiteradas escalonadas en el tiempo, en árbol, en las que, tras una primera votación y el consiguiente debate público, se fuesen planteando otras nuevas consultas en las que la ciudadanía fuera capaz de ir perfilando los detalles y eligiendo sucesivamente. Esto podría permitir dilucidar los elementos de consenso y centrarse en buscar soluciones a los problemas que susciten diferencias. Es evidente que un planteamiento de este tipo es inviable con un sistema convencional mediante papeletas por el coste y el trastorno que representa la movilización de tantas personas y de tantos recursos y locales, pero sería perfectamente realizable si existiese una infraestructura telemática para las votaciones (que podría utilizarse también para otras actividades de «ventanilla electrónica»).

c3) *Mezcla de listas cerradas y abiertas*. La lista cerrada tiene la ventaja de respetar la proporcionalidad en cuanto a opciones políticas genéricas, y la desventaja de que limita la capacidad de distinción entre sus miembros. La abierta permite, en cambio, elegir a los candidatos preferidos, si bien no se garantiza la proporcionalidad. El uso de sistemas informáticos para el recuento de los votos permitiría hacer practicable de forma sencilla la combinación de las ventajas de ambos procedimientos.

c4) *Opciones de interactividad.* La votación de los ciudadanos debiera basarse en una interactividad simétrica. Es decir, la ciudadanía debería estar en disposición de preguntar sobre las preguntas planteadas e incorporar modificaciones.

d) Un cuarto grupo de plataformas son aquellas en las que las funcionalidades desempeñadas se sitúan bastante alejadas de los procesos de votación propiamente dichos. En estos casos se entiende la acepción Democracia Digital vinculada a las prácticas que permiten al ciudadano participar en los debates y expresar su opinión a través de plataformas telemáticas. Bajo este planteamiento, el énfasis se pone en los procesos de deliberación, discusión y contraste de la información objeto de debate.

Como compendio de todas ellas, la plataforma que soporte todas las funcionalidades descritas en los cuatro grupos anteriores será la que constituya la categoría más avanzada y completa de aquellas que pretendan proporcionar servicios de Democracia Digital. En este caso, se posibilitaría la comunicación interactiva no sólo entre los ciudadanos y las autoridades que gobiernan, sino entre los ciudadanos mismos, los cuales, tras poder discutir la información, pueden emitir su opinión y, llegado el caso, participar en el proceso de decisión mediante voto u otro tipo de mecanismos de consenso. Es por ello que todas las demás categorías pueden considerarse como subconjuntos de esta última.

IMPLANTACIÓN DE SISTEMAS PARA LA DEMOCRACIA DIGITAL

De lo dicho anteriormente cabe deducir que la implantación de la Democracia Digital no será algo que se resuelva de hoy para mañana ni como consecuencia de decisiones tajantes, sino que será el fruto de un proceso en el que de forma paulatina vayan asumiéndose iniciativas que, analizando los límites y oportunidades que los sistemas de información y las redes telemáticas ofrecen para el desarrollo de la democracia, sirvan para implantar sistemas que favorezcan la interacción, el debate y la más amplia participación de los ciudadanos en todos los aspectos de la vida pública.

En este sentido, es probable que la implantación de alguno de estos sistemas, como puede ser el caso de los sistemas de votación telemática, no se lleve a cabo de forma global y obligatoria en un instante dado, sino que lo esperable es que se vayan creando islas de participación ciudadana en las que la práctica regular del voto telemático evolucionado vaya facilitando la aceptación por parte de los ciudadanos de las ventajas que representa y reduciendo los temores en cuanto a su implantación. En cualquier caso, la implantación de sistemas de Democracia Digital deberá llevarse a cabo dejando la posibilidad de que los ciudadanos que lo prefieran puedan seguir usando métodos convencionales.

La introducción de estos sistemas dependerá de las condiciones políticas y sociales en las que se encuentre la colectividad de que se trate, evaluando en cada caso el balance entre los riesgos y los beneficios que tal implantación conlleve. Por ejemplo, la implantación de un sistema de urnas electrónicas tal como el llevado a cabo en Brasil, en el que se ha visto favorecida la participación de colectividades alejadas de los centros urbanos y con un deficiente nivel de alfabetización, posiblemente resultase inadecuado para ser implantado en otros países en los que los sistemas convencionales mediante papeletas ofrecen mayores garantías de supervisión y auditoría.

En la concepción que aquí estamos asumiendo de considerar la Democracia Digital como un componente más de las actividades que se lleven a cabo dentro de una Sociedad de la Información, las plataformas y los sistemas que diseñen deberán ser lo suficientemente flexibles como para permitir una configuración particularizada conforme a las necesidades de cada situación.

Las herramientas que posibiliten los procesos de participación ciudadana deberán proporcionar frecuentemente servicios de anonimato, lo que conlleva la utilización de mecanismos criptográficos robustos. En el caso de sistemas de votación telemática para la elección de representantes o para la celebración de referendos vinculantes, que pretendan sustituir a los actuales sistemas convencionales de votación, los requisitos de anonimato exigidos serán muy rigurosos (según hemos visto en epígrafes anteriores), pero en otras plataformas de participación la privacidad podrá garantizarse suficientemente con soluciones menos estrictas.

Al igual que en otros escenarios que hemos descrito en anteriores epígrafes, también para la participación de los ciudadanos en procesos de debate y decisión el uso de tarjetas inteligentes puede resultar muy beneficioso a la hora de diseñar protocolos y procedimientos que garanticen la privacidad y, en algunos casos, el anonimato. Aparte de las constatables ventajas de seguridad que proporciona, la tarjeta inteligente conlleva muchos matices simbólicos, ya que es un dispositivo personal y privado que aporta a su titular la sensación subjetiva de tranquilidad que supone que, cuando la retira del CAD en que está alojada, se lleva consigo todos los datos de seguridad personal que le pertenecen.

11.9. SEGURIDAD CÍVICA PARA LA SOCIEDAD DE LA INFORMACIÓN

Con el estudio de las características y posibilidades de aplicación de los servicios de anonimato que hemos estado abordando en el presente capítulo hemos cubierto el arco de los seis principales servicios de seguridad cuya existencia detectamos en el Capítulo 1. En relación con los servicios de anonimato hemos estado analizando lo imprescindible de su uso de cara a la implantación de las aplicaciones telemáticas avanzadas que constituirán una parte importante de los sistemas que soporten las funcionalidades presentes en la Sociedad de la Información.

LOS CRIMINALES ATACAN DE NUEVO

Todo nuestro enfoque ha estado dirigido, conforme a lo que hemos denominado *Seguridad Cívica*, al estudio de los protocolos y mecanismos de seguridad que sirven para protegerse de los riesgos que aparecen en las comunicaciones telemáticas *teniendo en cuenta las necesidades de la vida diaria de los ciudadanos*.

Conviene recordar esto de nuevo porque en torno a la implantación de los servicios de anonimato y de los mecanismos criptográficos en los que se apoyan (por ejemplo, las firmas opacas) existe también un runrún de alarmas y temores catastrofistas acerca del uso perverso que de estos servicios puedan hacer los criminales. Así, se habla del pago anónimo de rescates, del blanqueo de dinero y de otras zarandajas.

Ya se justificó al final del Capítulo 1 el poco interés que para las necesidades de la Seguridad Cívica representan los planteamientos que tienen en cuenta los comportamientos criminales al por mayor, así como la convicción de que para hacer frente a esos comportamientos criminales se puede recurrir a diseñar adecuadamente los esquemas organizativos bajo los que operan los protocolos de seguridad que protegen las comunicaciones.

El problema no está en las redes sino en los planteamientos sociales y políticos que consienten o dan pie a que esos comportamientos existan. No es de recibo poner en duda la aplicación de mecanismos que den soporte a servicios de anonimato que fortalezcan los derechos civiles aduciendo su posible utilización para fines ilícitos. Para que exista dinero negro no es necesario recurrir ni esperar a que se instalen servicios de pago anónimo que preserven la privacidad de las pequeñas compras de los ciudadanos normales. Si existe es porque se consiente o no se ataja adecuadamente.

No obstante, conviene recordar que existen propuestas intelectuales de configuraciones para la provisión de servicios de anonimato que incluyen protocolos específicos con el objetivo de establecer salvaguardas para solucionar, llegado el caso, el posible uso inadecuado de las facilidades ofrecidas.

LA FORTALEZA DE LOS SISTEMAS

Un asunto que también apuntamos en el Capítulo 1 y que ahora, con más conocimiento de causa, conviene resaltar es el relacionado con el nivel de seguridad que deben tener las comunicaciones seguras para conseguir la confianza de los ciudadanos. En la Figura 11.31 se representa de nuevo la figura 1.9 en la que se refleja cómo la confianza surge cuando las medidas de protección introducidas superan «el peso» que tienen los riesgos de vulneración.

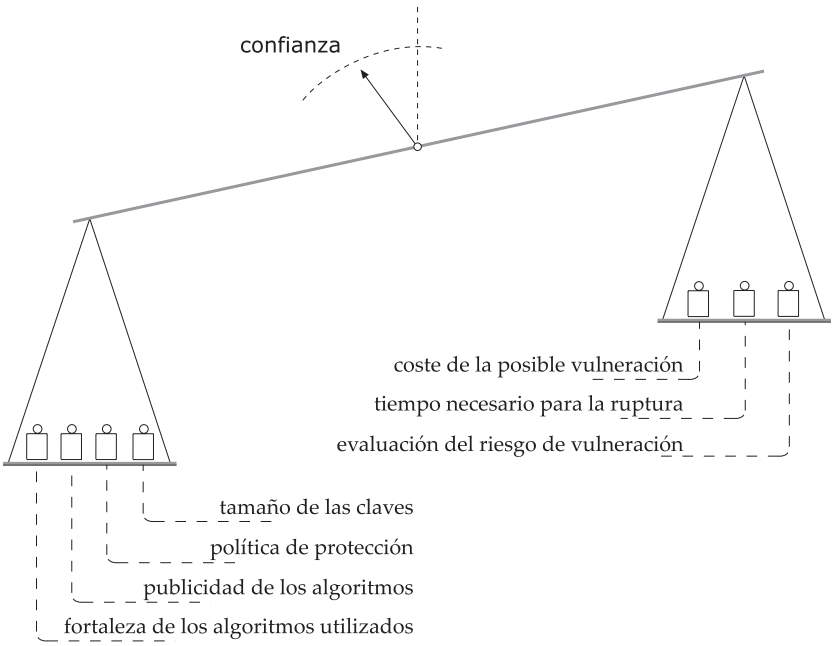

Figura 11.31. Confianza en los sistemas que interesan a los ciudadanos.

Así, por ejemplo, en un sistema de votación telemática que trate de sustituir a los sistemas actuales de votación mediante papeletas para la elección de representantes políticos, las garantías para asegurar que el voto es secreto deben ser elevadísimas, ya que trata de emular, e incluso superar, las garantías ofrecidas por los sistemas convencionales. Pero si de lo que se trata es de una plataforma cívica en la que se intercambian opiniones, y en algunos casos, además de la búsqueda de opciones consensuadas, se recurre a votar propuestas manteniendo el anonimato, las protecciones necesarias pueden ser más ligeras porque es bastante bajo el riesgo de que exista un atacante externo, armado con herramientas y procedimientos de ruptura robustos, interesado en vulnerar la seguridad de ese sistema. El escudo protector debe ser de tal grado que el coste y el esfuerzo necesario para romperlo sea superior al beneficio que pueda obtener el atacante.

De las descripciones que antes hemos hecho acerca de los mecanismos necesarios para conseguir servicios de seguridad robustos se deduce que la fortaleza de los protocolos y de los sistemas puede conseguirse con el concurso balanceado de tres formas de proceder:

a) Con medidas organizativas y procedimentales que garanticen la protección de la información. Por ejemplo, en el caso del voto telemático, para la apertura de la Urna se podría implementar un «secreto compartido» procedimental consistente en que la tarjeta inteligente que sirve para provocar que la Urna entregue los votos esté guardada en una caja cerrada y lacrada que solamente pueda desprecintarse en presencia de un determinado número de vocales y de interventores. De forma más genérica, en el Capítulo 10, entre las regulaciones de una CPS, se recogen multitud de referencias a medidas de seguridad que se apoyan en procedimientos organizativos.

b) Con protección mediante dispositivos resistentes contra manipulaciones (*tamper-resistant* o *tamper-proof*). Los programas que residan en los distintos agentes telemáticos que constituyen el sistema (por ejemplo, de voto telemático o de medios de pago) estarán almacenados en unidades de memoria cuyo contenido no se pueda alterar. Si previamente se ha auditado el contenido de esas memorias, se consigue una confianza bastante significativa en que el comportamiento de esos programas será el correcto y en que el sistema no puede actuar fraudulentamente. La tarjeta inteligente es, como tantas veces hemos insistido, un dispositivo cuya seguridad se apoya en gran medida en la característica de resistencia ante manipulaciones.
c) Con la generación, por parte de los actores del sistema, de piezas de información criptográficamente robustas y seguras que se puedan presentar como prueba demostrable ante terceros (que pueden, en algunos casos, actuar como jueces o árbitros) en caso de litigio o disconformidad con los resultados deducidos.

Este último tipo de protecciones son las más contundentes y las que, en último extremo, proporcionan un nivel de seguridad más elevado, pero deben utilizarse de forma conjunta y coordinada con las referidas en los dos párrafos anteriores. En cada caso concreto, teniendo siempre en cuenta las necesidades de los ciudadanos y los riesgos que se corren, se elegirán, de entre los tres grupos mencionados, las medidas que inclinen la balanza, de forma proporcionada, para que el sistema pueda ser considerado como digno de confianza.

NECESIDAD DE UNA COOPERACIÓN MULTIDISCIPLINAR

Según anunciábamos al final del Capítulo 1, el objetivo principal de este libro es servir de ayuda a los estudiantes de ingeniería (y a los profesionales) interesados en el diseño, implementación y puesta a punto de sistemas que garanticen, para usos civiles, la seguridad en las redes telemáticas. En este y en anteriores capítulos se ha procurado dejar sentadas las bases para que se puedan adquirir los conocimientos y las habilidades necesarias para ello, aunque quede aún mucho camino por recorrer.

Dentro de la Sociedad de la Información es necesario proporcionar servicios de seguridad que sirvan para garantizar la privacidad y el respeto de los derechos civiles en las comunicaciones que se establezcan, ya sean éstas de carácter social (relacionadas con prácticas de Democracia Digital), comercial (dentro de las distintas facetas de lo que se denomina Comercio Electrónico) o estrictamente personal.

Ante la complejidad de estas demandas, un ingeniero no puede, con la sola ayuda de sus conocimientos tecnológicos, abordar en solitario la solución de los problemas planteados. Antes bien, como ya hemos dicho, será más que conveniente la colaboración de equipos multidisciplinares que, de forma conjunta, averigüen las necesidades reales de los usuarios [Carr01] y sean capaces de determinar los requisitos que han de cumplir los sistemas que pretendan dar respuesta a ellas.

Será necesario, por tanto, que en el desarrollo de las aplicaciones telemáticas que den respuesta a la necesidades de la Sociedad de la Información, al mismo tiempo que se realicen los trabajos de ingeniería correspondientes, se hagan análisis sociológicos, políticos y jurídicos para determinar la viabilidad de los sistemas. La incorporación de servicios de seguridad en las redes telemáticas ha de servir para garantizar que los derechos y salvaguardas actualmente reconocidos en las comunicaciones con-

vencionales sean respetados también en la proyección y plasmación que éstos tienen en la Sociedad de la Información. Pero, siendo esto necesario, no es suficiente: los nuevos sistemas deberán proporcionar mejores protecciones y mayores cotas de seguridad y de privacidad en las comunicaciones.

No merece la pena desarrollar un sistema telemático técnicamente perfecto que incluya innovaciones notables y use las más avanzadas técnicas si el entorno social al que va dirigido, es decir, los ciudadanos para los cuales ha sido concebido, no confían en él o no responde a sus necesidades reales.

NOTAS AL CAPÍTULO 11

[1] Una propuesta interesante sobre esquemas que utilizan una TTP como ayuda en la generación y verificación de firmas opacas es la formulada en [FrYu94] acerca del opacado de «firmas débiles» (*weak signatures*). En este esquema, dado un mensaje *m*, la operación de generación de firma *y* es tan sencilla como realizar la operación $y = (a\ m + b) \bmod n$, donde a, b y n son parámetros predefinidos. Aunque, como decimos, los algoritmos son fáciles de entender, por cuestiones de espacio y de oportunidad no se han descrito en el texto, ni siquiera a título de ejemplo, porque sería necesario dedicar demasiado espacio para explicar las condiciones de existencia y la corrección de las operaciones que se realizan, tanto para la generación como para la verificación de las firmas. No obstante, el lector interesado puede, sin mucho esfuerzo, entender cumplidamente los planteamientos allí formulados.

[2] Los autores titulan este artículo como *Fair Blind Signatures*, que es tanto como decir firmas justas o firmas ecuánimes, en contraposición con las firmas opacas sin tercera parte, que serían, por tanto, según ellos, injustas o inadecuadas («en algunas circunstancias», cabe añadir). Más adelante, en el epígrafe 11.3, cuando se aborde el tema de los medios de pago, se comentará de nuevo el problema de los riesgos de las firmas no auditadas. Las realizaciones que se proponen en este artículo se apoyan en procedimientos criptográficos como «*Cut-and-Choose*» y «*Oblivious Transfer*» que, aunque no son especialmente complejos, no han sido explicados en el apartado correspondiente de este texto. Por ello, el lector interesado en analizar esos protocolos pormenorizadamente deberá pertrecharse previamente del correspondiente bagaje criptográfico, que puede adquirir en un texto especializado en esa materia (por ejemplo, [Schn96]).

[3] Las tarjetas de contactos tienen que insertarse en un dispositivo lectura-escritura, CAD, en una posición concreta para conseguir que los contactos coincidan exactamente con los equivalentes del lector. La tarjeta sin contactos no tiene esta restricción porque se comunica mediante una antena alojada en su interior, lo que evita el desgaste que se puede producir en éstos por el excesivo uso o a causa de operar en ambientes hostiles en los que pueda acumularse suciedad en los terminales. La tarjeta dispone de una pequeña pila y/o puede tomar energía rectificando la onda portadora que se modula para conseguir transmitir la información entre el dispositivo de lectura-escritura y la tarjeta. En realidad, la norma por la que se rige esta comunicación es la ISO 10536 (partes 1 a 3), aunque el funcionamiento global es en todo idéntico al que estamos comentando de las tarjetas de contactos conformes con la norma ISO 7816 (partes 1 a 7).

[4] Para el adecuado entendimiento de las descripciones y comentarios contenidos en este apartado y el siguiente, damos por supuesto que el lector conoce con cierto detalle las características del lenguaje de programación Java y el esquema de ejecución de los programas en una Máquina Virtual Java. En lo que fijaremos nuestra atención en estos apartados es en la particularización de esas características generales al reducido entorno del sistema microcomputador existente en una tarjeta inteligente, con el objetivo último de resaltar las ventajas que ofrecen las Tarjetas Java (en comparación con las que hemos convenido en denominar «clásicas» o tradicionales) en lo que se refiere al desarrollo de aplicaciones telemáticas seguras.

[5] Una descripción detallada de la estructura, funcionamiento y procedimientos de programación de las Java Cards puede encontrarse en [Chen00]. También puede encontrase información actualizada en la sección dedicada a *Java Card* dentro del sitio web *http://java.sun.com* de la empresa Sun (que fueron los inventores de este tipo de tarjetas), y en otros foros de Internet dedicados a este asunto.

[6] En [Carr02] se analiza con más detenimiento este problema y se hace referencia a algunos de estos estudios de investigadores sociales, entre los que cabe destacar las aportaciones de Manuel Castell (*The information Age. Economic, Society and Culture.* Vol I. Oxford. Blackwell Publishers, 1996-1997), Oscar Gandy (*Coming to terms with the panopticon sort.* In *Surveillance, Computers and Privacy*. University of Minnesota Press, 1996) y David Lyon (*Surveillance Society. Monitoring everyday life*. Open University Press. 2001).

[7] Conviene citar, no obstante, que casi todas las propuestas se apoyan en los trabajos teóricos iniciales de D. Chaum que pusieron las bases para todos los desarrollos posteriores. Dos referencias interesantes para conocer estos planteamientos son [Cha85] y [ChPe93]. Para obtener una idea panorámica de las distintas posibilidades y alternativas que se pueden presentar en la provisión de este servicio, puede consultarse [BuPi89]. Muchas de las aplicaciones existentes, como es el caso de Mondex, no han hecho públicas la estructura y funcionamiento de los protocolos en que se basan y se limitan a declarar las calificaciones de seguridad que han obtenido de distintos organismos de evaluación. Otras, aunque se conoce con más detalle su comportamiento, están sujetas a restricciones de publicación debido a los derechos de patentes (como ya se comentó, Chaum posee varias de ellas).

[8] Los que aquí hemos denominado *Sistema1* y *Sistema2* se corresponden con dos propuestas experimentales, en las que participó directamente el autor de este texto. El *Sistema1* se corresponde con [Dieg00] y con una versión simplificada y retocada que está recogida en [Carr02]. El *Sistema2* aquí descrito es una simplificación del descrito en [Gome00] modificado para adaptarlo al esquema *on-line* del *Sistema1*, y tiene partes comunes con alguno de los ejemplos descritos en [Schn96].

[9] Realmente, las compras para las que interesa mantener el anonimato son las que conllevan cantidades de dinero pequeñas o medianas, que son las que sirven para trazar los hábitos y modos de vida de los ciudadanos (qué, dónde y cuándo). Precisamente, las compras importantes (un automóvil, una casa) no necesitan anonimato porque son transacciones de por sí bastante visibles. Es más, a los ciudadanos corrientes les interesa que esas transacciones **no sean anónimas**, sino, por contra, que exista la máxima transparencia en su adquisición y titularidad (y en el pago de los correspondientes impuestos).

[10] Una descripción resumida de las experiencias de voto electrónico más significativas que se han llevado a cabo hasta la fecha puede encontrarse en [GoCa03]. Asimismo, en este artículo se hace una clasificación de este tipo de sistemas y se analizan las propuestas más relevantes que se apoyan en criptografía avanzada y en redes telemáticas (lo que daremos en llamar *voto telemático*). (Puede consultarse en www.vototelematico.diatel.es.)

[11] Este método de trabajo que aquí se expone es una esquematización del seguido durante el desarrollo de un proyecto de investigación sobre voto telemático (el proyecto VOTESCRIPT [CGMP02] [CGC03]) cuyo desarrollo se llevó a cabo mediante un equipo multidisciplinar compuesto por investigadores pertenecientes tanto al campo de la ingeniería telemática como al campo sociopolítico y jurídico. La tesis de partida de este proyecto es que la votación telemática es imprescindible abordarla desde equipos multidisciplinares, necesarios no sólo en la fase de diseño y desarrollo sino también en la fase de implementación y puesta a punto. Dentro de este proyecto se han desarrollado el *Sistema Votescript* de votación mediante cabina y el denominado *Sistema VERA* (*Votación Electrónica para los Residentes Ausentes*) vinculado a un proyecto conjunto de la Subdirección General de Política Interior del Ministerio del Interior de España con la FNMT (Fábrica Nacional de Moneda y Timbre). En base a las especificaciones de VERA, la FNMT-RCM desarrolló un sistema propio de votación, de cuyo prototipo se realizaron pruebas de campo en El Hoyo de Pinares (Ávila) en marzo de 2003. Este prototipo no incluía el proceso de verificación individual ni la presencia de comprobantes de votación. En la web del proyecto (www.vototelematico.diatel.es) puede encontrarse información sobre los artículos reseñados y sobre los trabajos sociológicos

llevados a cabo. Una información más detallada sobre estos últimos puede encontrarse en www.ucm/info/demodigi.

[12] Los que aquí hemos denominado SistemaA y SistemaB son una simplificación de dos sistemas de votación telemática diseñados dentro del proyecto VOTESCRIPT citado en la nota anterior. El SistemaA es una simplificación del denominado *Sistema Votescript* de votación mediante cabina y el SistemaB lo es de una versión menos segura del anterior que utiliza un computador convencional como punto de votación y acceso al Sistema.

[13] Para implementar este *Sobre Seguro* puede utilizarse un mecanismo habitualmente denominado *canal seguro* que es una mejora del mecanismo denominado *sobre* o *envoltura digital* (*digital envelope*) que analizamos en el Capítulo 5. Consiste en: *a)* generar una cadena aleatoria, *b)* generar una clave de sesión, *c)* concatenar la cadena y el mensaje a ocultar, *d)* obtener el *hash* (MAC, conforme a la nomenclatura usada en el Capítulo 8) de la concatenación anterior, *e)* concatenar el MAC, la cadena aleatoria y el mensaje, *f)* cifrar lo anterior con un algoritmo simétrico haciendo uso de la clave de sesión generada, *g)* cifrar la clave de sesión con la clave pública del destinatario, y *h)* enviar al destinatario el resultado anterior junto con el criptograma resultante del cifrado simétrico.

Pueden utilizarse también otros mecanismos que eviten el cifrado simétrico procediendo de la siguiente forma: *a)* generar una cadena aleatoria, *b)* concatenar la cadena y el mensaje a ocultar, *c)* obtener el MAC de ese conjunto mediante una operación *hash*, *d)* concatenar el MAC, la cadena aleatoria y el mensaje, y *e)* cifrar todo lo anterior con la clave pública del destinatario. El objetivo de la cadena aleatoria es el de evitar los ataques denominados *de fuerza bruta* comentados en la nota a pie de página (se podría adivinar el voto por tanteo de todas las opciones posibles). Por otra parte, el MAC garantiza la integridad y evita que aparezca el siguiente ataque: Un atacante podría alterar los votos que se envían desde el Punto de Votación a la Urna (sin ningún provecho, sólo por fastidiar). La Urna no detectaría la falta de integridad en lo recibido, por lo que lo aceptaría. Al final de la votación, durante la fase de recuento, se detectaría que la pieza de información no corresponde a un voto válido y, por lo tanto, sería desechada, consiguiendo así el atacante invalidar votos.

[14] Un esquema como este de la Figura 11.26, o bien una manipulación del esquema representado en la Figura 11.24, que permitiese establecer bases de datos con relaciones pormenorizadas de personas y de sus huellas identificativas (o palabras de paso) haría las delicias de los defensores de no-sé-bien-qué, que tanto abundan, y que tratan de protegernos contra nuestra voluntad a costa de pulverizar nuestra privacidad. La evolución de las tecnologías que posibilitan la implantación de controles biométricos en lugares públicos o de acceso semipúblico, que condicionan los movimientos de la ciudadanía en su conjunto, es algo ajeno al uso de las técnicas biométricas que aquí proponemos, aunque tengan en común una misma base teórica. El debate sobre las ventajas e inconvenientes de esas prácticas cae fuera del alcance de este texto.

[15] Una solución de este tipo es la adoptada en el sistema VERA [CGC03] del cual el aquí denominado SistemaB es una simplificación didáctica, según se refiere en nota anterior. En [LCP99] se describe otro sistema en el que se utiliza una applet que se descarga de un servidor central y utiliza una tarjeta inteligente como testigo de seguridad y auxiliar en la realización de operaciones criptográficas sencillas. La ventaja de este tipo de soluciones es que el desarrollo de la aplicación, en cuanto a la utilización de la tarjeta inteligente se refiere, resulta bastante sencillo.

CONTENIDO