Pseudo-anonimato basado en el algoritmo de Firma Ciega Justa

José Luis González y Pierre Plaza
Telefónica I+D
c/Emilio Vargas, 6 28047 Madrid

Vicente Benjumea y Javier López
Universidad de Málaga
Avda. Cervantes, 2 29071 Málaga

Telf: 913129965
E-mail: jluis@tid.es

Resumen

Telefónica I+D y la Universidad de Málaga presentan un trabajo conjunto en el cual se lleva a cabo la realización de un mecanismo de autenticación que permite ocultar la identidad de un usuario, ofreciendo la misma fiabilidad de una PKI tradicional.

1. Introducción

El creciente uso de la red para el comercio electrónico, y los medios de pago necesarios para ello, dejan tras de si un rastro de información que permite reconstruir las acciones emprendidas por las personas que la usan. Estas huellas pueden ser un medio inestimable para la investigación de fraudes y delitos, pero también pueden ser utilizadas, a costa de invadir nuestra privacidad, para obtener información con fines deshonestos.

Las innegables ventajas que nos proporciona el creciente uso de los certificados de identidad por parte de gobiernos y entidades privadas, conlleva también el hecho de que nuestra privacidad se vea cada vez más amenazada.

En ocasiones, la percepción de la utilidad del anonimato en nuestra sociedad, especialmente cuando existen servicios de pago, es de un medio para ocultar fines deshonestos, e incluso delictivos. En cambio, este desarrollo busca que el anonimato solamente sirva para ocultar información a la curiosidad, o las malas intenciones de aquellos que intervienen en los servicios mencionados, sin servir por ello como pantalla para otros fines.

Por ello, la necesidad de establecer relaciones anónimas, que protejan la privacidad de las personas en este ámbito, pero que además, permitan a las autoridades el acceso a la información en el caso de una investigación, ha llevado a Telefónica I+D, en colaboración con el departamento de Telemática de la Universidad de Málaga, a desarrollar un mecanismo de Pseudo-anonimato que cumpla con estas expectativas.

Basado en un esquema desarrollado y publicado en el contexto del proyecto IST-UBISEC, el Pseudo-anonimato utiliza la Firma Ciega Justa (*FBS*, por las siglas de *"Fair Blind Signature"*) para crear una serie de documentos certificados, que proporcionen el suficiente anonimato como para impedir el rastreo cuando solo se posee una parte de la información necesaria.

El diseño comprende un esquema, por el cual los usuarios pueden emplear los privilegios adquiridos de manera anónima. Este esquema, es complementario a las infraestructuras de gestión de privilegios (*PMI* por las siglas de *"Privilege Management Infrastructure"*) y de las infraestructuras de clave pública (*PKI* por las siglas de *"Public Key Infrastructure"*), por lo que se emplean los recursos existentes y estandarizados de ambas, sin que por ello sean necesarios cambios, o nuevos estándares que modifiquen los existentes.

Una infraestructura clásica de clave pública es un medio que asegura la identidad de los usuarios, las Autoridades de Atributos (*AA*) pueden emitir certificados que avalan privilegios para dichos usuarios. Estos certificados de atributos (*AC* por las siglas de *"Attribute Certificate"*) están descritos en [2]..

Es de suponer que las terceras partes que confíen en la solvencia de quienes componen este sistema, pueden ofrecer al usuario servicios basados en los privilegios que tiene. Se convierte por tanto, en clave para el éxito del servicio, tanto la exactitud con la que dichos atributos han sido emitidos, como en la seguridad de los mismos.

Sin embargo, la ventaja innegable que supone esta capacidad de asegurar la identidad de quien porta estos atributos, y los privilegios que representan, puede constituir un freno en su empleo, tanto en determinados entornos donde el anonimato es un bien a proteger, como en aquellos donde el anonimato ya esté establecido y sea de difícil erradicación.

Tomemos como ejemplo cualquier servicio cuyo pago en efectivo aporta un cierto grado de anonimato, mientras que el pago con cualquier otro medio rompe dicho anonimato. Este cambio puede frenar la expansión de dicho servicio.

El anonimato puede emplearse en numerosas relaciones en nuestra sociedad, especialmente en aquellas en las que impulsa la participación, sin circunscribirse exclusivamente a las económicas. De esta manera los foros de discusión, la fidelización de

clientes o el control de accesos también puede quedar cubierto por esta forma de anonimato.
Por último, es importante recalcar que tanto este documento, como el desarrollo realizado, se orientan únicamente al ámbito de los documentos electrónicos y a los rastros que los mismos dejan en diferentes registros; quedando completamente fuera de su alcance los aspectos relativos al anonimato real de las personas.

2. Los actores y el proceso

En el esquema de Pseudo-anonimato aparece la figura de un Tercero en Confianza (*TTP* por las siglas de "*Trusted Third Party*") cuyo cometido es tanto la salvaguarda de la identidad del usuario anónimo, como la revelación de la misma en caso necesario.
Esta tarea se realiza mediante la emisión de un documento llamado pseudónimo.
Asimismo, las Autoridades de Atributos que intervienen en el esquema deben tener la capacidad de emitir certificados anónimos de atributos. Por su parte, un nuevo complemento a estas autoridades, que es la Entidad de Cobro, o sub-Autoridad de Atributos (*AAi*), estará a cargo de la verificación de los requisitos que se exigen al usuario para obtener determinado atributo en su certificado anónimo.
El papel que juegan estas tres entidades en el proceso puede resumirse de la siguiente manera: El usuario solicitara anónimamente, tantos pseudónimos como le sean necesarios al Tercero en Confianza. Dichos pseudónimos tendrán un periodo de validez, tras el cual caducan y no pueden emplearse más. Cada pseudónimo consta de dos partes, una privada y otra pública; y nos referiremos a ellas como pseudónimo público y pseudónimo privado. A partir de este momento, la misión encomendada al Tercero en Confianza será la de salvaguardar la relación que existe entre ambos pseudónimos, hasta finalizar el periodo de validez.
A partir de este momento, el usuario deberá enviar a la sub-Autoridad de atributos una prueba y el pseudónimo público por cada atributo que precise en sus certificados anónimos. La prueba requerida en cada caso dependerá del atributo en cuestión, aunque en la mayoría de los casos, consistirá en una prueba de compra del privilegio que el atributo representa; de ahí la denominación alternativa de Entidad de Cobro de la sub-Autoridad de Atributos. La misión de la sub-Autoridad de Atributos consiste en la comprobación tanto de la verdadera identidad del usuario como de la veracidad de la prueba, y la emisión de un bono (o "*token*") como recibo de éxito de estas comprobaciones. Adicionalmente, la sub-Autoridad de Atributos también estará a cargo del registro y la salvaguarda de la relación existente entre la identidad real del usuario, el pseudónimo público y el bono emitido.
En este punto interviene por primera vez el algoritmo de firma ciega justa, mediante el cual se emplea el pseudónimo público para emitir el bono, como veremos mas adelante.
Este algoritmo, también permite al usuario modificar el bono sin que pierda ninguna validez, ocultar la relación existente con el pseudónimo público y crear una relación con el pseudónimo privado.
Con este bono, ahora relacionado con el pseudónimo privado, el usuario accede a la Autoridad de Atributos para la emisión de su certificado anónimo de atributos.
En este punto del esquema, la Autoridad de Atributos, puede asumir que el usuario cumple los requisitos para exigir los privilegios que le da el certificado anónimo de atributos, ya que porta un bono válido. No obstante, no puede saber a quien está emitiendo dicho certificado, ya que el usuario no se identifica y el bono está relacionado con un pseudónimo privado.
Un compromiso en la seguridad de la Autoridad de Atributos, o de la sub-Autoridad de Atributos, e incluso una confabulación de ambas, no dará como resultado la identificación del portador del certificado anónimo, mientras el Tercero en Confianza mantenga en secreto la relación entre pseudónimo público y privado.
Se ha de presuponer, por tanto, que el Tercero en Confianza es una entidad lo suficientemente solvente como para asegurar este secreto, entre tanto que no se den las circunstancias adecuadas para romperlo. Estas circunstancias pueden ser la rotura por una de las partes del acuerdo al que se somete el esquema, o la comisión de un delito, en cuyo caso las autoridades judiciales pueden exigir esta revelación.
Al concluir satisfactoriamente este proceso, el usuario puede exigir los privilegios que le atribuye el certificado de atributos, que, al ser anónimo no estará relacionado con ninguna *PKI*, aunque, al contener una clave pública, el usuario que conozca la correspondiente clave privada ha de ser forzosamente el dueño.

2.1. Escalabilidad del esquema

El pseudo-anonimato es un esquema basado en la fragmentación de la información para impedir la reconstrucción del conjunto completo, y es, precisamente esta, una de las vulnerabilidades del sistema; que se demostrará más seguro cuanto mas separadas en el tiempo estén las acciones unas de otras, y cuantas más acciones del mismo tipo se realicen simultáneamente.
Tomemos como ejemplo una única operación en la que se verifica, en muy poco tiempo, la solicitud de un pseudónimo, el pago de un servicio y la obtención del certificado anónimo. Una confabulación de las Entidades de Cobro y la Autoridad de Atributos puede, fácilmente, establecer la identidad del usuario al no ser necesario que el Tercero en Confianza desvele la relación entre los dos únicos pseudónimos que entran en juego.
Por este motivo, la seguridad del sistema estará en función del tiempo que pase entre la obtención del bono y el certificado, y del número de operaciones

que otros usuarios realicen entre tanto. Cuanto mayor sea ese tiempo, y mas bonos y certificados se soliciten, mas difícil será establecer las relaciones entre todos los pseudónimos públicos y privados que se han presentado.
Otra de las vulnerabilidades del esquema se presenta al reutilizar el pseudónimo para varias operaciones, ya que puede permitir establecer una pauta en el comportamiento del usuario para acotar la búsqueda. No obstante, la solución a esta vulnerabilidad consiste simplemente en utilizar un pseudónimo diferente cada vez.

3. El anonimato en la actual infraestructura de *PMI*

Si tomamos la estructura de un certificado de atributos estándar, observamos que el campo *"Holder"* puede contener un resumen o referencia a un objeto.
Es por este medio, y a través de un nuevo objeto que llamaremos Estructura de pseudónimo (*PS* por las siglas de *"Pseudonym Structure"*), por el que los certificados de atributos quedaran provistos del anonimato condicional de sus dueños.
La figura 1 muestra la composición de los diferentes campos de la Estructura de pseudónimo, cuya descripción es:

- **Etiqueta de Estructura de pseudónimo** (*"Pseudonym Structure Label"*):
  Es un campo estático que nos permite identificar un objeto como Estructura de pseudónimo.
- **Pseudónimo** (*"Pseudonym"*):
  Pseudónimo privado emitido por el Tercero en Confianza que se especifica en el siguiente campo.
- **Identificador del Tercero en Confianza** (*"TTP Identifier"*):
  Emisor y depositario de la relación entre los pseudónimos públicos y privados.
- **Condición**:
  Es la o las condiciones que permiten romper el anonimato y revelar la identidad del usuario, contemplado en un acuerdo alcanzado y aceptado por todas las partes.

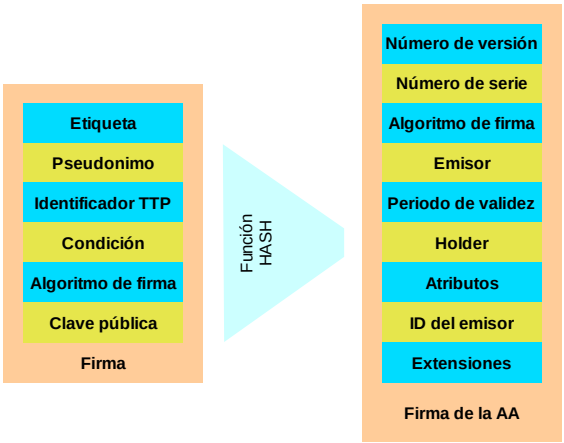

Figura 1. Estructura e un pseudónimo.

- **Algoritmo de firma** (*"Signature Algorithm"*):
  Identifica el algoritmo de firma y verificación de documentos a emplear con la clave pública almacenada en el siguiente campo.
- **Clave Pública** (*"Public Key"*):
  Clave empleada para autenticar al dueño del certificado de atributos. El proceso de autenticación se realiza retando al supuesto dueño del certificado anónimo de atributos, a firmar una prueba con su clave privada, que solamente puede verificarse con la clave pública contenida en el certificado.
- **Firma** "*Signature*"):
  El usuario anónimo firma la Estructura de pseudónimo para probar su autenticidad y que está en posesión de la clave privada de dicha firma. Esta misma firma hace implícita la aceptación por parte del usuario de las condiciones enumeradas en el cuarto campo.

Un certificado anónimo de atributos X.509 consiste, por tanto, en un certificado de atributos estándar, junto con una Estructura de pseudónimo. La relación entre ambos documentos se establece mediante el campo *"Holder"* del certificado.
El certificado de atributos estará respaldado por la firma de una Autoridad de Atributos, que a su vez acepta las condiciones enumeradas en la estructura de pseudónimo que utilizo para emitir el certificado; con lo que se asegura que tanto la autoridad como el usuario conocen y aceptan tanto la política de autorización como las condiciones que rigen el certificado.
Es de suponer, por tanto, que el Tercero en Confianza, no podrá revelar la relación entre pseudónimos públicos y privados, a menos que se cumplan y demuestren las condiciones enumeradas en el certificado y la Estructura de pseudónimo.
Por otra parte, también se da por supuesto que el usuario no ha de entregar el certificado anónimo de atributos, junto con su clave privada o pseudónimo público a nadie.

4. El demostrador

Telefónica I+D ha realizado un demostrador que implementa tanto las funciones matemáticas, como el proceso descrito, simulando la reserva y uso anónimo de los servicios de un hotel.
Este demostrador se ha realizado atendiendo a fines didácticos, por lo que cada proceso o actor es independiente con respecto al resto.
La instalación se ha realizado en las oficinas de Telefónica I+D en Madrid, donde la integración en el demostrador domótico que esta empresa mantiene, ha permitido la simulación de accesos a auténticos

servicios, como el control de accesos físicos, o el uso de recursos multimedia mediante el certificado anónimos de atributos.

4.1. El almacén seguro

Uno de los aspectos clave del esquema de Pseudo-anonimato es el almacén en el cual han de guardarse los documentos electrónicos.

Este almacén contendrá todos los elementos necesarios para que el usuario pueda acceder a cada uno de los actores que intervienen en el proceso, por lo que un fallo en su seguridad, equivale a la rotura del anonimato.

La solución escogida en este caso son las tarjetas inteligentes, que constituyen un medio extremadamente seguro para la salvaguarda de documentos, mediante el uso de funciones criptográficas propias de las mismas, y un control de accesos que evita que programas malintencionados puedan intentar extraer más información que la estrictamente necesaria en cada momento.

Aunque el uso de tarjetas inteligentes implica la disponibilidad tanto de zócalos de lectura, como de programas adecuados para acceder a ellas, se ha valorado positivamente el progresivo incremento que actualmente está experimentando el uso de estas tarjetas.

5. El protocolo de obtención y uso de los certificados anónimos de atributos

Este protocolo se basa fundamentalmente en el trabajo presentado en [1] bajo el nombre de firma ciega justa con registro; aunque no obstante, la nomenclatura ha sido adaptada para enmascarar los procesos matemáticos subyacentes al mismo.

5.1. Actores

Los actores que intervienen en el proceso son:

- *U* (usuario) es el usuario del esquema, y se le supone en posesión de una clave privada, cuya correspondiente clave pública está respaldada por una *PKI* solvente.
- *N* es la clave asimétrica del usuario anónimo. Esta clave no está respaldada por ninguna *PKI*.
- *P* es el pseudónimo del usuario, y consta de dos partes. Por un lado *Ppubl* es el pseudónimo público que el usuario presentara junto con su identidad real, y *Ppriv* es el pseudónimo privado.
- *TTP* es el Tercero en Confianza que emite los pseudónimos y salvaguarda su relación.
- *AA* es la Autoridad de Atributos que emite los certificados de atributos. Su clave pública *AApubl* está respaldada por una PKI solvente.
- *AAi* es la sub-Autoridad de Atributos que comprueba que el usuario cumple los requisitos para poseer determinado privilegio, y emite el correspondiente bono. Su clave pública *AAipubl* está respaldada por una *PKI* solvente.
- *ATTRi* es el atributo que el usuario reclama, y cuyos requisitos han de ser comprobados por la *AAi*. Este mismo atributo *ATTRi* es el que figurara en el certificado emitido por la Autoridad de Atributos.
- *ATTRiU* es la prueba de que el usuario *U* cumple con los requisitos del atributo.
- *SP* es el proveedor de los servicios a los que tienen derecho los dueños de un certificado con el atributo *ATTRi*.
- *fpubl* y *fpriv* son dos registros que especifican que partes del pseudónimo son público o privado.
- *val_period* es el periodo de validez del pseudónimo.
- *fblindX(m)* representa un mensaje m protegido por una firma ciega de *X*.
- *SxPpubl (fblindx (m))* es la firma ciega de *X* del mensaje *m* bajo el pseudónimo público *Ppubl*.
- *SxPpriv (m)* es la firma ciega de *X* del mensaje *m* con el pseudónimo privado *Ppriv*, después de ser transformado desde su forma pública.

5.2. Terminología y nomenclatura

Los siguientes ejemplos ilustran la nomenclatura del protocolo criptográfico:

- *A : act*
  La acción *act* de *A*.
- *A → B: m*
  Se envía *m* desde *A* a *B*.
- $m = (m_1, m_2)$
  m se compone de m_1 y m_2
- $c = E_z(m)$
  c es el resultado de cifrar *m* con la clave *z*
- $m = D_z(c)$
  m es el resultado de descifrar *c* con la clave *z*
- A_{publ}, A_{priv}
  Son la pareja de claves asimétricas pública y privada de *A*
- $c=E_A(m)$
  c es el resultado de cifrar *m* con la clave pública *A*
- $m=D_A(c)$
  m es el resultado de descifrar *c* con la clave privada *A*
- *h=H(m)*
  h es el resultado de aplicar a *m* el algoritmo *Hash*
- $S_m=S_A(m)$
  Firma del mensaje *m* con la clave privada *A*
- $m_s=S_A(m)$
  Mensaje firmado compuesto de *m* y la firma anterior
- $b = V_A^?(m_s)$

Resultado de la verificación del mensaje anterior con la clave pública *A*

- *z=NSK()*
  Creación de una nueva clave simétrica *z*
- *A=NAK()*
  Creación de un nuevo par de claves asimétricas *A*

5.3. Obtención de un pseudónimo

Este proceso consiste en el registro, y posterior obtención por el usuario de un una firma ciega justa con el protocolo de registro descrito en [1].
La figura 2 ilustra esquemáticamente el flujo de información desde la fuente hasta la tarjeta inteligente del usuario.
En este proceso se asume que el Tercero en Confianza, a quien el usuario solicitará el pseudónimo, es una entidad reconocida por el resto de las partes.
Durante este proceso, el usuario sin identificar solicitara la creación de un pseudónimo válido. El Tercero en confianza creará dicho pseudónimo, cuyas partes pública y privada firmará, identificando a cada una con su propósito (mediante *fpubl* y *fpriv*) y su periodo de validez.
A continuación el pseudónimo será enviado al usuario y una copia guardada en un almacén seguro.
Es importante recalcar que el Tercero en Confianza no conoce en absoluto la identidad del usuario, y que por tanto no podrá ni almacenar, ni revelar ningún dato relativo a esta identidad.
Este proceso se realizara en su totalidad cada vez que el usuario solicite un pseudónimo, que será diferente en cada caso.
El desarrollo matemático del proceso será por tanto:

1. $U : z = NSK()$
2. $U \rightarrow TTP : E_{TTP}(z, Pseudonym\_Request)$
3. $TTP : New\_Pseudonym (P_{publ}, P_{priv})$
4. $TTP : STORE (val\_period, P_{publ} \leftrightarrow P_{priv})$
5. $TTP \rightarrow U : E_z (S_{TTP} (f_{publ}, val\_period, P_{publ}), S_{TTP} (f_{priv}, val\_period, P_{priv}))$

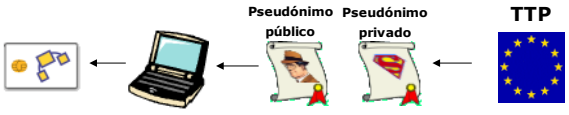

Figura 2. Obtención del pseudónimo

5.4. La maquina Pseud-o-matic

La implementación del algoritmo de obtención del pseudónimo se presenta en forma de sitio WEB de acceso libre, donde, mediante un applet de java, el usuario recorre el protocolo comunicándose con el Tercero en Confianza, y descargando la estructura del pseudónimo (con sus partes pública y privada) en la tarjeta inteligente. La figura 3 muestra el aspecto del sitio WEB.

Figura 3. La máquina Pseud-o-matic

5.5. Obtención del bono

En esta parte del protocolo se emplea el proceso de firma con protocolo de registro por firma ciega justa descrito en [1]. Por este medio, el usuario obtiene un mensaje firmado por la sub-Autoridad de Atributos encargada de verificar los requisitos necesarios para obtener un determinado privilegio.
Precisamente es el medio por el que se realiza la firma ciega justa, que se garantiza que el firmante desconoce lo que está firmando, que no es más que el pseudónimo público del usuario. No obstante, el usuario cambiara este pseudónimo por el privado, sin que pierda validez la firma.
Es importante recordar que el la firma ciega justa proporciona las herramientas matemáticas que permiten realizar este cambio una sola vez.
Por lo tanto, la clave de este paso está en obtener una prueba que asevere el cumplimiento de los requisitos por el usuario, sin que nadie pueda relacionar esta prueba con dicho usuario, sino con el poseedor de una determinada clave privada.
La prueba consiste en una clave pública firmada por la sub-Autoridad de Atributos. El poseedor de esta prueba permanece anónimo, es decir, que nadie puede deducir quien es a partir de la prueba en sí. Sin embargo, la prueba que presentara el usuario mas adelante tiene una firma que está enlazada con un pseudónimo privado, pero nadie puede saber quien es el dueño de ese pseudónimo, ya que en el momento de la firma, la sub-Autoridad lo hizo sobre el pseudónimo público, que si está relacionado con la identidad del usuario.
Como conclusión y resumen del proceso de obtención del bono, podemos decir que el usuario crea un nuevo par de claves asimétricas, de las que entrega a la sub-Autoridad de Atributos solamente la clave pública, junto con el identificador del Tercero en Confianza, el pseudónimo público y la prueba de cumplimiento de los requisitos.
La autoridad comprobará la validez del pseudónimo, tanto por su periodo como por su emisión, y la validez de la prueba aportada.
En el caso de que todas las comprobaciones sean positivas, todos estos elementos se almacenan y la clave pública aportada será firmada con firma ciega justa para el pseudónimo público. Una vez que el usuario recibe el resultado de este proceso, ha de

transformar la firma, en una firma en claro de la clave pública para el pseudónimo privado:

1. $U : N = NAK()$
2. $U \rightarrow AA^i : S_U (TTP, S_{TTP} (f_{publ}, val\_period, P_{publ}), ATT^i_U, fblind_{AA}i (N_{publ})$
3. AA^i : IF $(\neg V^?_{TTP} (S_{TTP} (f_{publ}, val\_period, P_{publ})) \vee \neg fulfil\_req (U, TTP, P_{publ}, ATTR^i_U))$ THEN Abort
4. $AA^i : STORE (U \leftrightarrow ATTR^i_U \leftrightarrow TTP \leftrightarrow S_{TTP}(f_{publ}, val\_period, P_{publ})$
5. $AA^i \rightarrow U : S^{Ppubl}_{AA}i (fblind_{AA}i (N_{publ}))$
6. $U : S^{Ppriv}_{AA}i(N_{publ})$

El resultado de este proceso será el bono que prueba el cumplimiento de los requisitos. La siguiente figura ilustra gráficamente la obtención del bono.

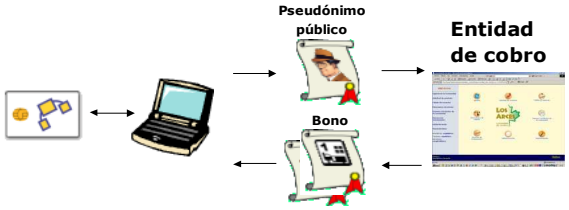

Figura 4. Obtención del bono

5.6. Primer acceso al hotel

El demostrador presenta al usuario el sitio WEB del hotel *"iCubes"*. En este sitio, que contiene tanto el acceso a la Entidad de Cobro, la Autoridad de Atributos como de los servicios que ofrece el hotel, es posible acceder a la Solicitud de una reserva.
Este acceso abre un canal seguro en el que ambas partes se autentican, demostrando con ello quienes son mientras que la validez y veracidad de sus credenciales son comprobadas.
Una vez que el acceso le ha sido concedido al usuario, este puede escoger la modalidad de servicio que desea obtener. Esta selección implicara que la Entidad de Cobro emplea una firma diferente para cada modalidad, como prueba de que el usuario la ha pagado.

Figura 5. El sitio WEB del Hotel iCubes

El proceso de cobro se ha obviado en este demostrador, ya que no aporta ningún elemento activo al proceso. Sin embargo, en un caso real, el proceso de cobro debería realizarse después de la selección del usuario, y la emisión del bono debe quedar supeditada al éxito del mismo.
Al igual que en la máquina Pseud-o-matic, un applet de java se encarga de realizar la comunicación entre el usuario y la Entidad de Cobro, para finalmente guardar el bono obtenido en la tarjeta inteligente.

5.7. Obtención del certificado

En esta parte del protocolo, el usuario utilizará el bono obtenido en el paso anterior para solicitar un certificado de atributos estándar.
Para ello, el usuario crea una estructura para albergar la información del pseudónimo. Esta estructura ha de ser firmada para demostrar la autenticidad de la información que contiene, y que, como poseedor de la clave privada asociada a la clave pública contenida, está de acuerdo con los términos expresados en la estructura.
Junto con la estructura firmada, el usuario envía el bono obtenido en el paso anterior, es decir, la firma ciega justa de la clave pública que, recordemos, está relacionada con el pseudónimo privado.
La Autoridad de Atributos verificará cada una de las firmas como primera medida para emitir el certificado, para después registrar las condiciones expresadas en la estructura, especialmente aquellas que hacen referencia a la revelación de la identidad real del usuario.
De esta manera, quedan claros los términos que el usuario y el Tercero en Confianza han aceptado. Esto implica que el Tercero en Confianza estará obligado a revelar la relación entre los pseudónimos públicos y privados cuando se le presente el Certificado anónimo de Atributos y la condición se demuestre cumplida. La Entidad de Cobro estará obligada, por su parte a revelar la relación entre el pseudónimo público y la identidad real del usuario.
Terminadas satisfactoriamente las verificaciones, la Autoridad de Atributos crea el certificado por un periodo de validez que establece que el propietario de la estructura descrita anteriormente posee un determinado atributo. El propietario de la estructura, no es más que aquel que pueda demostrar que conoce la clave privada relativa a la clave pública, contenido en dicha estructura.
El desarrollo matemático del proceso será por tanto:

1. $U : Pseud\_Inf = S_N (Label_{PI}, P_{priv}, TTP, Cond, Sig\_Alg, N_{publ})$
2. $U \rightarrow AA : (S_{TTP} (f_{priv}, val\_period, P_{priv}), S^{Ppriv}_{AA}i (N_{publ}), Pseud\_Inf)$
3. AA : IF $(\neg V^?_{TTP} (S_{TTP} (f_{priv}, val\_period, P_{priv})) \vee \neg V^?_{AA}i (S^{Ppriv}_{AA}i (N_{publ})) \vee \neg V^?_N(Pseud\_inf) \vee (\neg Agree\_on (Cond)))$ THEN Abort

4. *AA : Attr_Cert = S_{AA} (Vers, Serial, Sig_Alg, AA, Va_ Period, H (Pseud_Inf), $ATTR^i$*

5. *AA → U : Attr_Cert*

La siguiente figura ilustra la obtención del certificado.

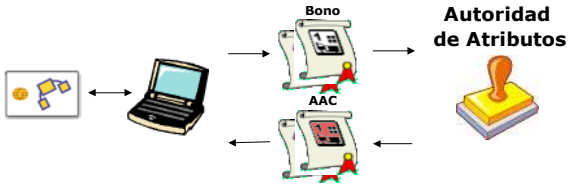

Figura 6. Obteniendo el certificado

5.8. El registro en la recepción

La figura que corresponde a la obtención del certificado en el demostrador es el registro de entrada en la recepción del Hotel *"iCubes"*. En este momento, el usuario recibe el certificado que le permitirá hacer uso del privilegio adquirido, que no es mas que una habitación en concreto, y los servicios asociados a la modalidad elegida.
Como en los casos anteriores, un applet se encarga de gestionar la comunicación entre el usuario y la Autoridad de Atributos para descargar el certificado anónimo de atributos resultante en la tarjeta.

5.9. Verificación del Certificado anónimo de Atributos

Esta es la última parte de esta descripción técnica, y corresponde a la validación de los certificados emitidos en el anterior paso. Para ello, el usuario envía el certificado junto con la información del pseudónimo. El proveedor de servicio verificará que el atributo que contiene el certificado es adecuado para el servicio solicitado; posteriormente se envía un reto al usuario para que sea firmado, y de esta manera pruebe que es el dueño del certificado que aporta. Si el resultado es satisfactorio, el proveedor puede dar el acceso solicitado.
El desarrollo matemático del proceso será por tanto:

1. *U → SP : (Attr_Cert, Pseud_Inf)*
2. *SP :* IF *($\neg V^{?}_{AA}$(Attr_Cert) ∨ (H (Pseud_inf) $\neq^{?}$ Holder_Field(Attr_Cert)) ∨ ¬fulfill_req (Service. Attr_Cert, Pseud_inf))* THEN Abort
3. *SP → U : challenge*
4. *U → SP : S_N (challenge)*
5. *SP :* IF *($\neg V^{?}_{N}$ (S_N (challenge)))* THEN Abort
6. *SP → U : Service_granted*

No obstante, si el usuario hace mal uso del privilegio de un certificado, el proveedor del servicio deberá reunir las pruebas de demuestren ese mal uso.

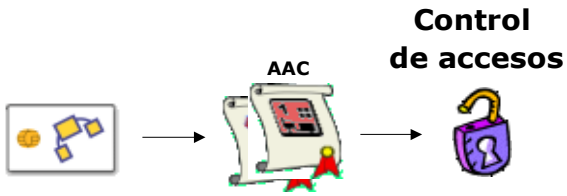

Figura 7. Verificación del certificado

En el caso de que el mal uso vulnere directamente las condiciones expresadas en la estructura del pseudónimo, pueden ser presentadas a la Autoridad de Atributos y el Tercero en Confianza para la revocación del certificado y el revelado de la identidad real de usuario. En caso de que el mal uso incurra en delito o falta, serán las autoridades pertinentes las que recaben esta información.

5.10. Los servicios del hotel iCubes

Como punto final y objetivo de todos los pasos anteriores, el usuario puede presentar como credencial el certificado obtenido en el registro de entrada, introduciendo la tarjeta inteligente en el lector habilitado para tal fin, a la entrada de cada uno de los servicios del hotel (gimnasio, sauna, etc.). El conocimiento del PIN de acceso a la tarjeta será la prueba de que es el propietario de la misma, mientras que el atributo contenido en el certificado demostrara que tiene acceso al servicio en cuestión.
En otros casos, como el del acceso a la habitación, será necesario comprobar no solamente el atributo, sino el pseudónimo privado al que fue emitido, para permitirle acceder únicamente a él.
El demostrador también muestra servicios como el acceso a contenido multimedia, que permite al usuario seleccionar y reproducir aquellos contenidos a los que tiene derecho; o la solicitud y compra de nuevos privilegios y certificados.
Por último, el usuario puede comprobar el uso realizado con su certificado, y los servicios contratados adicionalmente.
La última parte del demostrador consiste en la simulación de la rotura del anonimato. Para ello, se recaba toda la información relativa al pseudónimo privado que ha hecho mal uso de los privilegios que tenía, como por ejemplo, dejando impagada la factura de los servicios adicionales. Esta información, no basta para obtener la identidad real del usuario, aunque se acceda a los registros de la Entidad de Cobro, al no conocer el pseudónimo público relacionado con el privado.
Es el Tercero en Confianza, quien nos revelara esta relación.

6. Conclusiones

El trabajo realizado en conjunto por el Universidad de Málaga y Telefónica I+D, ha permitido el desarrollo de una serie procedimientos mediante los cuales se otorgan certificados en tarjetas inteligentes para la concesión de derechos sobre bienes, protegiendo la privacidad del usuario, utilizando un pseudónimo con el cual el usuario se identifica.

Dicho anonimato, se puede romper en casos en los cuales se utilice el pseudónimo de manera fraudulenta y sea necesaria la identificación del usuario. Los procedimientos se basan en el uso de algoritmos para la implementación de la firma ciega justa.
Se ha desarrollado un demostrador que emplea esta tecnología simulando los procedimientos existentes para la contratación de servicios relacionados con un Hotel.

Referencias

[1] M. A. Stadler, J. M. Piveteau, and J. L. Camenisch. Fair blind signatures. In L. C. Guillou and J. J. Quisquater, editors, Advances in Cryptology – EUROCRYPT'95, volumen 921 de Lecture Notes in Computer Science, paginas 209–219. Springer-Verlag, 1995.

[2] C. Adams and S. Farrell, `` Internet X.509 Public Key Infrastructure Certificate Management Protocols," 1999. RFC 2510.