Como proteger la privacidad de los usuarios en Internet. Verificación anónima de la mayoría de edad.

Jose A. Onieva, Isaac Agudo, Javier López
Dpto. de Lenguajes y Ciencias de la Computación
Universidad de Málaga
Email:{onieva, isaac, jlm}@lcc.uma.es

Gerard Draper-Gil, M. Francisca Hinarejos
Dpto. de Matemáticas e Informática
Universitat de les Illes Balears
Email: {gerard.draper, xisca.hinarejos}@uib.es

***Resumen*—La identidad digital está tomando una dimensión que se escapa de los esquemas tradicionales. Ha pasado de ser un mero identificador a un conjunto de características que nos definen. Cada vez compartimos más información personal en la red, en gran medida porque los modelos de interacción online requieren que la compartamos.**

Las grandes empresas de Internet se están acostumbrando a tener a su disposición o a exigir más información de la estrictamente necesaria para ofrecer sus servicios. Ante esta tendencia surge el denominado principio de minimización de datos contenido en la Directiva 95/46/CE sobre protección de datos que nos anima a utilizar mecanismos de protección de nuestra privacidad.

En este artículo se presenta una solución para la verificación anónima de la mayoría de edad que hace uso de la tecnología de *Information cards* para acceder a los servicios y del DNIe en la fase de registro con el Proveedor de Identidad.

I. Introducción

Uno de los ejemplos más claros en los que se infringe el principio de minimización de datos es en el de la verificación de la mayoría de edad. El mero hecho de solicitar la fecha de nacimiento va en contra de dicho principio, ya que la única información necesaria es saber si se sobrepasa un umbral de edad determinad, p.e. 18 años. En la vida real para poder demostrar la edad es necesario presentar un documento de identidad donde, además de la foto y fecha de nacimiento, constan otros datos que no son imprescindibles para verificar dicha información.

Podemos pensar que en la vida real, la persona que revisa nuestro documento identificativo no va a memorizar todos los datos para luego poder utilizarlos en su beneficio, pero si trasladamos este escenario a Internet, cada aplicación que requiera verificar nuestra edad tendría acceso a todos los datos de nuestro DNIe, los podría almacenar y tratarlos posteriormente. De hecho, podría crear un perfil de usuario, correlacionando todos los accesos del mismo usuario a los distintos servicios bajo el control de la misma empresa.

Aparte de la información que conscientemente compartimos con los proveedores de servicios también está el problema de la información que de forma indirecta estamos proporcionando, ya sea mediante las *cookies* almacenadas en nuestro navegador o mediante el uso de mecanismos de federación de identidad que proporcionan más atributos de los estrictamente necesarios y sobre los que el usuario no tiene ningún control.

El escenario de verificación de mayoría de edad es también relevante debido a que en la mayoría de las ocasiones, lo único que separa a un menor de edad del consumo de contenidos (o productos) solo aptos para adultos es un click que indique que efectivamente se es mayor de edad. Este procedimiento difiere sustancialmente del anteriormente descrito. Es más, en el caso de los menores de edad, este tipo de procedimientos contradice el artículo 17.e de acceso a la información adecuada del menor de la Convención sobre los Derechos del Niño [**?**]. No es suficiente con campañas de sensibilización previniendo de los peligros de la red; hay que adoptar medidas o sistemas que garanticen que las personas que ofrecen servicios a través de la red puedan verificar la edad del usuario; de tal manera que podamos cumplir las leyes que protegen a los menores de edad.

En Internet, a pesar de los avances llevados a cabo en materia de comunicación y seguridad, es difícil que los usuarios tengan la opción de acceder a un servicio proporcionando solo los atributos o propiedades necesarios, accediendo por tanto de forma potencialmente anónima. En la mayoría de los servicios online se requieren más datos de los necesarios en la fase de registro. Intentando asimilar el procedimiento tradicional y aprovechando el escenario descrito para dar una mayor aplicabilidad al *DNIe* [**?**] desarrollado en nuestro país, se puede trasladar el proceso a nuestra vida digital. Pero entonces, ¿Cómo mantenemos nuestra privacidad?.

Se hace por tanto necesario el uso de tecnologías que den un control total al usuario sobre la información proporcionada a los proveedores de servicio. Para que este esquema funcione, los proveedores de identidad deben colaborar con el usuario proporcionando credenciales de grano fino en las que se certifiquen solo los atributos necesarios para una transacción dada. Uno de los esquemas que mejor se adaptan a este tipo de escenarios es Information card[1] [**?**]; motivo por el que elegimos esta tecnología.

[1]Ver la sección V para una discusión acerca de la discontinuidad de Information cards desde Febrero de 2011.

Para reflejar de forma fiel el proceso de verificación de edad que se aplica en el mundo real, hemos implementado en el Proveedor de Identidad un mecanismo que mediante el uso del DNIe, en la fase de registro, le permite corroborar la edad del usuario para luego poder proporcionar esa información a los proveedores de servicios a los que acceda el usuario.

Para poner a prueba nuestro modelo hemos establecido un escenario de comercio electrónico a través de Internet. En nuestro desarrollo, un supermercado online permite la venta de productos de la misma manera que en cualquier sitio de comercio electrónico actual, con la salvedad de que ante el intento de compra de un producto catalogado para adultos, la tienda solicitará al usuario una Information card que demuestre su edad de manera **verificada** (y si el cliente lo desea, **anónima**) para permitirle continuar con la compra.

El resto del artículo se organiza de la siguiente manera. En la Sección II se presentan las tecnologías utilizadas en el desarrollo; es decir, Information card y el DNIe. A continuación, en la sección III se discuten los requisitos de nuestro escenario particular, así como el diseño final de nuestra aplicación. En la sección IV encontraremos el trabajo relacionado anterior al nuestro y estableceremos las principales diferencias con nuestras aportaciones. Por último, en la sección V se presentan unas conclusiones y las líneas de trabajo futuro.

II. Tecnologías relacionadas

En nuestro modelo juega un papel muy importante la identidad. La identidad digital, desde el punto de vista de la tecnología, representa una categoría de soluciones interrelacionadas que se utilizan para administrar autenticación de usuarios, derechos y restricciones de acceso, perfiles de cuentas, contraseñas y otros atributos necesarios para la administración de perfiles de usuario en los distintos servicios a los que tiene acceso. Con la multiplicación de servicios online que necesitan autenticación estamos obligados a gestionar una cantidad cada vez más grande de nombres de usuario y de contraseñas. Además, tenemos que proporcionar a menudo datos personales como nuestra fecha de nacimiento, nuestra dirección postal, etc. Para tratar de unificar la administración de nuestras identidades existen múltiples soluciones de federación de identidad.

Una de estas tecnologías es OpenID. Uno de los problemas de esta tecnología, sobre todo para usuarios inexpertos, son los ataques de phishing [**?**]. Es el proveedor de servicios el que redirecciona al usuario hacia el Proveedor de Identidad (IdP); y podría redireccionarlo a un IdP falso. Si la credencial es del tipo usuario/contraseña, sería difícil de proteger; provocando el temido phishing.

Aunque usemos mecanismos avanzados de autenticación, p.e. el DNIe, se pondrían en riesgo los datos del usuario. Esto permitiría a los atacantes disfrazarse como un Proveedor de Identidad de confianza y obtener información valiosa del usuario. Este hecho debilita el uso de OpenID y soluciones similares de redirección en nuestro modelo, de cara a garantizar el anonimato al usuario.

Incluso si subsanáramos dicho inconveniente, un problema adicional es el uso en OpenID de identificadores no unidireccionales que se convierten en un dato identificativo, lo cual entraría en conflicto con la cuarta ley de "Identidad dirigida" propuesta por Kim Cameron [**?**]. Es decir, la edad no sería anónima verificada, sino más bien pseudoanónima verificada.

Por otro lado, tecnologías como Information card tienen la ventaja de garantizar la edad de manera anónima ya que es el usuario el que envía de forma directa al proveedor de servicio las credenciales, mediante el uso de *tokens de seguridad* emitidos por el Proveedor de Identidad a partir de nuestra tarjeta.

No obstante, para poder emitir estas tarjetas es necesario una fuente fiable y eficiente de datos de identificación que permita realizar todo el proceso online desde el principio; incluyendo la fase de registro. Es aquí donde entra en juego el DNIe, ya que los certificados que contiene incorporan datos personales oficiales del individuo (en concreto la fecha de nacimiento que utilizamos en nuestro desarrollo). La combinación de ambas tecnologías representa el eje de nuestro modelo.

Un ejemplo de este modelo es la tarjeta universitaria. En dicha tarjeta aparecen menos datos que en el DNI. Quizás aparezcan datos diferentes, atributos afirmados por la Universidad. La Universidad solicita el DNI para emitir la tarjeta Universitaria en la que se integran datos oficiales (como la fecha de nacimiento) y afirmaciones acerca de nuestra condición (de estudiantes, profesores, etc.), con la que podemos beneficiarnos de los servicios bibliotecarios, transporte público, etc. Todo ello porque los servicios bibliotecarios y el transporte público confían en la entidad Universitaria. Y éste es precisamente el modelo a imitar por las Information cards.

II-A. Information card

Microsoft, Google y PayPal son las entidades que se unieron para formar la Information Card Foundation (ICF) [**?**], una organización cuya pretensión fue generalizar el uso de un nuevo sistema de identidad, que consiste en usar una tarjeta digital para la identificación. Estas nuevas tarjetas digitales, conocidas como Information cards, son como las tarjetas de fidelización que proporcionan muchos comercios; pueden ser emitidas por un *Proveedor de Identidad* (IdP) y aceptadas por entidades proveedoras de servicios. El usuario dispone de herramientas para la administración de estas tarjetas conocidas como selectores de identidad. Disponemos así de cuatro piezas claves para el funcionamiento de nuestra Information card:

- *Selector de Identidad*. Aplicación online o de escritorio que almacena y selecciona las Information cards. Un ejemplo es CardSpace, selector incorporado en el sistema operativo Windows 7.
- *Proveedor de Identidad*. Es un proveedor de servicio especial encargado de emitir Information cards y administrar información de identidades en nombre de los usuarios.
- *Servicio de Tokens de Seguridad* (STS). Es un servicio especial que acepta peticiones de tokens y genera una respuesta que contendrá el token correspondiente. Este servicio puede formar parte de un IdP o ser externo a él,

de manera que cuando se solicite un token el IdP pueda tener disponible más de un STS para obtenerlo.

- *Relying Parties* (RP). Es la parte que proporciona los servicios. Solicita una identidad digital en forma de token. El Relying Party puede solicitar un token de un proveedor en concreto o bien aceptar varios emisores. Entre IdP y RP existe una relación de confianza que permite que el RP considere auténticos los atributos emitidos por sus IdPs de confianza.

Para demostrar la identidad digital de un usuario ante un tercero (RP), éste debe presentar un token de seguridad. Por lo tanto, aunque esta operación es transparente al usuario (el selector realiza esta funcionalidad), cada vez que éste se autentica en el proveedor de servicio (RP) lo hace con un token de seguridad basado en los requisitos del servicio solicitado de acuerdo a la información contenida en la Information card. Es decir, que aunque el usuario solo percibe una comunicación con el RP, en realidad, el selector de identidad se comunica con el STS para solicitar un token de seguridad.

En nuestro caso este token de seguridad no es más que una afirmación SAML[2] (*Security Assertion Markup Language*) firmada por el IdP. De la misma manera, la Information card no es más que un fichero XML con los datos necesarios para contactar con el IdP y solicitar un conjunto de afirmaciones (token de seguridad).

Una característica importante de las Information cards es que no contienen información del usuario. Si examináramos el fichero XML, comprobaríamos que no contiene ninguna información personal. Es decir, aunque el IdP haya emitido una tarjeta que referencia nuestra fecha de nacimiento no veremos en el XML un campo en el que aparezca el valor de ese atributo. Se dice pues que la Information card es un artefacto (*artifact*); es decir, un elemento que con la intervención del selector permitirá al IdP/STS generar un token de seguridad con los atributos solicitados. Se dice también que las Information cards son una "metáfora" de la identidad, ya que representan datos del usuario sin contenerlos realmente. De hecho, como hemos indicado en el párrafo anterior, la tarjeta no se transmite en ningún momento, sino que construye la petición apropiada a partir de la información contenida en la misma. En la figura 1 podemos observar los distintos campos que presenta una Information card.

De estos campos, hemos de destacar el campo *Lista de atributos* (cuya etiqueta XML es *SupportedClaimTypeList*) en el que se especifica sobre qué atributos se pueden solicitar tokens de seguridad al IdP/STS. En nuestro caso se tratará de la edad, que obedecerá a un esquema determinado[3].

Para las implementaciones del IdP y el RP se ha hecho uso de la libreria *InfoCardphplib*. Esta librería está basada en SimpleSamlPHP [**?**] que hace uso del proyecto Carrillon IdP/STS [**?**].

Figura 1. Formato de una Information card

II-B. El DNIe

En la actualidad, un elevado número en aumento de ciudadanos españoles poseen un DNIe[4]. Este documento garantiza la identidad de cada individuo (rasgos y propiedades que le diferencian de los demás) mediante mecanismos y procesos electrónicos y no sólo físicos. El microchip almacena: los datos de filiación del titular, imagen digitalizada de la fotografía, imagen digitalizada de la firma manuscrita, plantilla de la impresión dactilar de los dedos índice de cada mano, un certificado cualificado para autenticación y otro para firma, certificado electrónico de la autoridad emisora y el par de claves (pública y privada). El hecho de que haya dos certificados persigue que el ciudadano pueda distinguir entre las actividades de autenticación y firma electrónica cuando se produzcan, al margen de la similitud de los procesos criptográficos implicados en ambas.

En las extensiones de los certificados X509 [**?**] contenidos en el DNIe podemos encontrar la extensión *subjectDirectoryAttributes* (OID 2.5.29.9) en la que se encuentra la fecha de nacimiento, *dateOfBirth* (OID 1.3.6.5.5.7.9.1); la cual permitiría comprobar, de ser necesario, la mayoría de edad de la persona que se identifica o firma y (lo que es más interesante para nuestro trabajo) por tanto, verificar la edad del individuo (ver la figura 2).

[2]En cualquiera de sus versiones.

[3]http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirth

[4]Veinticinco millones de DNIe expedidos según fuentes de la Policía Nacional en Septiembre de 2011.

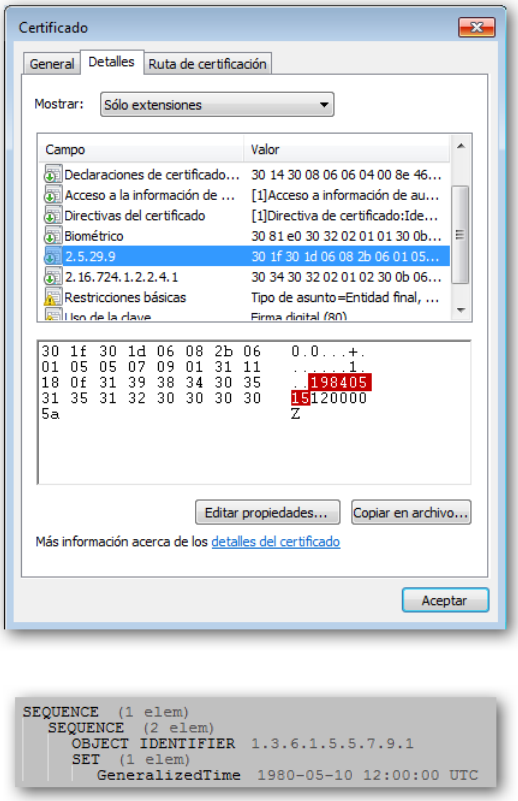

Figura 2. Extensiones necesarias del certificado del DNIe

III. Análisis de Requisitos y Diseño

Se hace necesario una toma de requisitos no solo generales (operacionales y funcionales) sino de seguridad. Nos centramos en este artículo en los requisitos de seguridad que se imponen en nuestro modelo. Aparte de los requisitos de seguridad cubiertos por las tecnologías anteriormente mencionadas, resulta imprescindible establecer una serie de requisitos adicionales, específicos de nuestra aplicación. Separamos estos requisitos según el actor al que afectan. Por un lado tenemos los requisitos del usuario.

- **RS-001**. El usuario debe preservar la confidencialidad e integridad en todas sus comunicaciones tanto con el RP como con el IdP.

A continuación, los requisitos del Proveedor de Identidad

- **RS-002**. El IdP ha de autenticarse en toda conexión entrante.
- **RS-003**. El usuario ha de autenticarse en toda comunicación con el IdP. Esta autenticación ha de llevarse a cabo con el DNIe en caso de petición de una Information card. En caso de solicitud de token al STS, ésta podrá ser débil (usuario/contraseña) o fuerte (DNIe).
- **RS-004**. El usuario debe tener la opción de elegir el método de autenticación en el STS.
- **RS-005**. Con el objeto de soportar una autenticación débil, las credenciales necesarias han de almacenarse en una base de datos segura haciendo uso de funciones hash.

Por último los requisitos del proveedor de servicios o Relying Party.

- **RS-006**. El RP ha de autenticarse en toda conexión entrante.
- **RS-007**. En el proceso de validación de un token recibido se debe validar el esquema.
- **RS-008**. Validación de la autenticidad, origen e integridad del token de seguridad (validación de la firma XML Signature [**?**]).
- **RS-009**. Validación de la caducidad del token de seguridad.

Teniendo en cuenta estos requisitos podemos diseñar los distintos casos de uso de nuestro modelo y establecer los diagramas de flujo que han de sucederse durante el funcionamiento del servicio.

La figura 3 muestra el diagrama de flujo para el acceso del usuario al proveedor de servicio. En ella observamos la petición de token al IdP/STS por parte del selector (RST, *Request Security Token*) y la respuesta de éste (RSTR, *Request Security Token Response*).

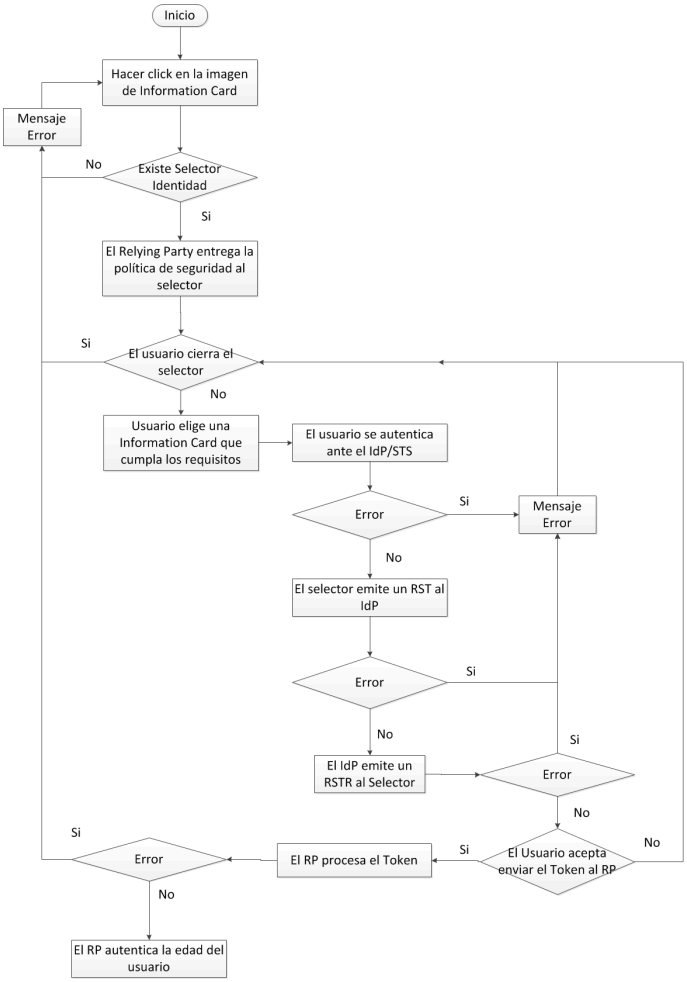

Figura 3. Acceso del usuario al proveedor de servicio

En la figura 4 se muestra el escenario de la solución propuesta para la obtención de una tarjeta de edad verificada,

donde el usuario utiliza su DNIe para autenticarse frente al Proveedor de Identidad a la hora de solicitar la tarjeta de edad verificada.

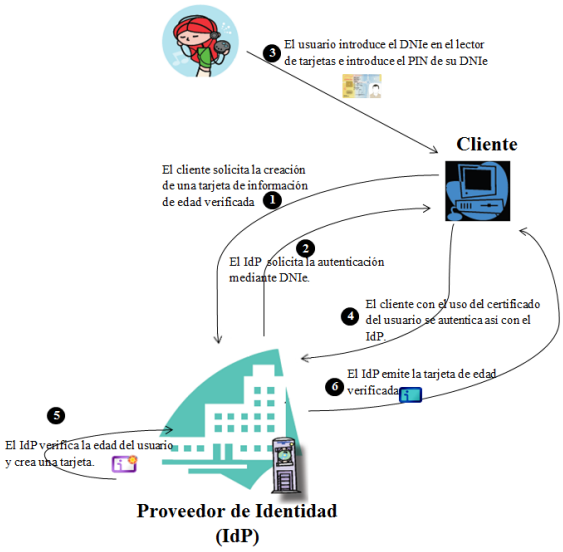

Figura 4. Obtención de una tarjeta de edad verificada

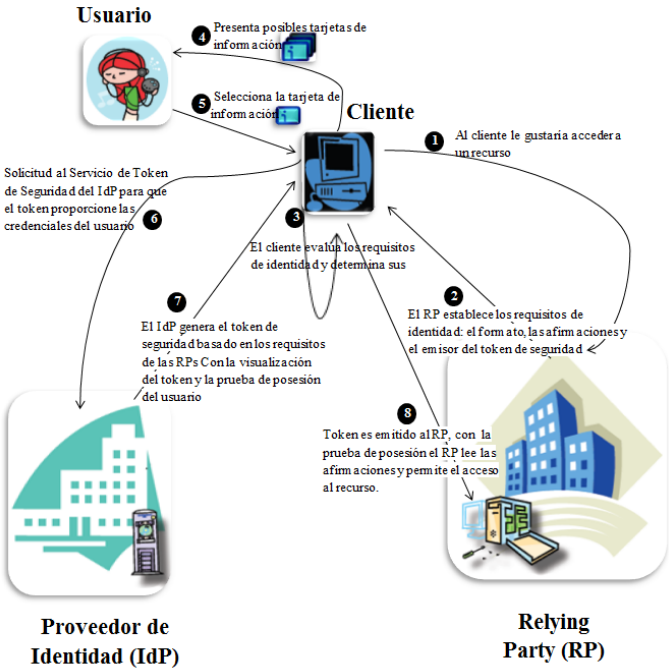

Figura 5. Uso de una tarjeta de edad verificada

Por otra parte, en la figura 5 podemos ver el escenario de la solución propuesta para el acceso a un servicio de la RP (en nuestro caso el supermercado online) haciendo uso de una tarjeta de edad verificada. Los pasos que se producen son los siguientes:

1. Al cliente le gustaría acceder a un recurso (ej. un artículo de un supermercado que sólo está a la venta a mayores de edad) que se encuentra en el RP.
2. El RP devuelve un mensaje donde se establecen los requisitos de identidad: el formato, las afirmaciones y el emisor del token de seguridad. El RP le envía al usuario la política de seguridad, en este caso necesita una Information card emitida por nuestro IdP y que contenga la afirmación de la fecha de nacimiento. De manera opcional se le puede mostrar la política de privacidad.
3. El navegador invoca al selector de identidad y el selector muestra las Information cards que cumplen esas políticas de seguridad.
4. El usuario acepta enviar la Information card seleccionada por él.
5. Solicitud al IdP/STS que proporcione las credenciales de usuario (en nuestro caso, un atributo indicando la mayoría de edad).
6. El IdP/STS genera el token de seguridad y es devuelto al cliente.
7. El cliente reenvía el token de seguridad al RP, que valida él mismo y permite/deniega el acceso al recurso (una vez comprobados los atributos; en nuestro caso, la mayoría de edad).

En cuanto a la implementación, aunque se omiten los detalles en este artículo, se hace uso de Web Services, con SOAP [?] como protocolo de transporte y WDSL [?] como lenguaje de descripción de servicios web. También se hace uso de Ajax para enriquecer la experiencia del usuario en el supermercado online y MySQL para el mantenimiento de la base de datos del lado del IdP. Puede encontrarse una demostración de la aplicación en [?].

IV. Trabajos Previos

Debido al hecho de que la proliferación de servicios en Internet ha sido meteórica, a la par que lo ha sido la integración de Internet en las vidas de los más jóvenes, no han sido pocos los autores que han abordado el problema de la autenticación de la edad a través de la red. Muchos son los estudios que intentan llamar la atención acerca de los problemas que acarrea la falta de verificación de edad por parte de los servicios web. A modo de ejemplo, en [?] se constata la cada vez mayor presencia de menores de edad en sitios de apuestas online.

En [?] se propone un solución similar a la nuestra pero que no hace uso de tecnologías existentes (utilizan una invención propia denominada Identificador de Edad Universal UAID) y que además precisa de la verificación inicial en la fase de registro de documentación no-electrónica (como el certificado de nacimiento). También la empresa Equifax diseñó un proyecto similar (y previo) al nuestro junto con la empresa Azigo que proporcionaba un selector de Information cards [?]. No obstante, hasta donde alcanza nuestro conocimiento, éste nunca se llevó a cabo, quizás porque aunque la fase de registro no requería la presencia del usuario, sí requería que el IdP contactara con diversas fuentes oficiales para poder verificar la edad del usuario.

En [?] los autores proponen un modelo de autenticación de usuarios con información mínima basado en proveedores

de redes sociales como Facebook. Para ello utilizan, imitando las distintas cuentas con distintos privilegios de UNIX, la utilización de dos cuentas de Facebook y el desarrollo de un *framework* que permite el *single sign-on* de forma automática con aquella que deseamos, haciendo uso de *Facebook Connect* [**?**]. Consideramos que aunque los objetivos son los mismos, la orientación dada en su solución carece de la verificabilidad de los datos proporcionados. Es decir, no puede considerarse que un proveedor de red social pueda ser un IdP fiable para todas las aplicaciones.

V. Discusión y Conclusiones

En este trabajo hemos visto cómo combinando un mecanismo fiable (y extendido entre todos los ciudadanos), pero sin propiedades avanzadas para proteger la privacidad de los usuarios, como puede ser el DNIe y un esquema de gestión de identidad suficientemente flexible como Information card, podemos conseguir un nivel alto de seguridad a la hora de verificar de forma anónima determinados atributos de los usuarios. La clave está en implementar un Proveedor de Identidad intermedio que filtre solamente los atributos necesarios para acceder a los servicios en cuestión y se los proporcione de forma confiable.

Además, en la actualidad, y aunque la legislación en muchos casos es autonómica, en nuestro país no existe una ley que regule de manera específica la venta de productos que requieren una mayoría de edad a través de Internet. Consideramos, pues, que damos con este trabajo un paso hacia delante en cuanto a verificación de edad anónima y fácilmente usable a través de Internet, haciendo uso de la tecnología de identificación y autenticación existente en el país.

La elección de Information cards en el momento de desarrollo del modelo parece acertada. Tal y como se indica en [**?**], Information cards es el *framework* de identidad centrado en el usuario de mayor difusión instalado (o instalable) en todos los sistemas operativos en el momento de la implementación de nuestra solución. Debido a la cancelación por parte de las empresas que la apoyaban, los siguientes pasos en esta línea de trabajo son: por un lado implementar este esquema usando otras tecnologías diferentes a Information card y añadir otras fuentes de información a nuestro Proveedor de Identidad intermedio, aparte del DNIe, que nos permitan trabajar con un rango mayor de atributos y por tanto ofrecer servicios más avanzados.

Agradecimientos

Queremos agradecer en especial a Enrique de la Hoz autor de la librería InfoCardphplib con la que se ha llevado a cabo el desarrollo de la aplicación y a Manuel Bordés Rodríguez por participar activamente en la parte de programación del modelo.

Este trabajo ha sido parcialmente financiado por el proyecto de investigación Consolider ARES (CSD2007-00004) del Ministerio de Ciencia e Innovación (MICINN) de España.

Referencias

[1] http://www2.ohchr.org/spanish/law/crc.htm
[2] DGPGC, *DNI electrónico. Guía de referencia básica*, 3rd ed., Comisión Técnica de Apoyo a la Implantación del DNI electrónico, octubre 2010.
[3] C. Burton, "The information card ecosystem: The fundamental leap from cookies & passwords to cards & selectors," White Paper, April 2009.
[4] B. van Delft and M. Oostdijk, "A security analysis of openid," in *Policies and Research in Identity Management*, ser. IFIP Advances in Information and Communication Technology, E. de Leeuw, S. Fischer-Hübner, and L. Fritsch, Eds. Springer Boston, 2010, vol. 343, pp. 73–84, 10.1007/978-3-642-17303-5_6. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-17303-5_6
[5] K. Cameron, "The laws of identity," Microsoft Corporation, Tech. Rep., 2006.
[6] http://informationcard.net/
[7] http://simplesamlphp.org/
[8] http://www.carillon.ca/tools/demo-sts.php
[9] *Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*, ITU-T X.509, March 2000.
[10] M. Bartel, J. Boyer, B. Fox, B. LaMacchia, and E. Simon, *XML Signature Syntax and Processing*, 2nd ed., W3C, June 2008.
[11] *SOAP Version 1.2 Part 0: Primer (Second Edition)*, W3C, abril 2007.
[12] *Web Services Description Language (WSDL) Version 2.0 Part 0: Primer*, W3C, junio 2007.
[13] http://www.lcc.uma.es/~onieva/demo.mov
[14] M. Griffiths and A. Barnes, "Internet gambling: An online empirical study among student gamblers," *International Journal of Mental Health and Addiction*, vol. 6, pp. 194–204, 2008, 10.1007/s11469-007-9083-7. [Online]. Available: http://dx.doi.org/10.1007/s11469-007-9083-7
[15] R. Cahn and T. Piliouras, "On-line anonymous age verification for controlling access to selected websites," US Patent US 2008/0033740 A1, 2008.
[16] http://informationcard.net/card-projects/equifax-over-18
[17] G. Kontaxis, M. Polychronakis, and E. P. Markatos, "Sudoweb: minimizing information disclosure to third parties in single sign-on platforms," in *Proceedings of the 14th international conference on Information security*, ser. ISC'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 197–212. [Online]. Available: http://dl.acm.org/citation.cfm?id=2051002.2051022
[18] Facebook for Websites [Online]. Available: https://developers.facebook.com/docs/guides/web/
[19] S. Poetzsch, M. Meints, R. L. Bart Priem, and R. Husseiki, "D3.12: Federated identity management – what's in it for the citizen/customer?" FIDIS - Future of Identity in the Information Society, Deliverable, 2009.