10054/03/ES
WP 68

Documento de trabajo sobre servicios de autenticación en línea

Adoptado el 29 de enero de 2003

EL GRUPO DE TRABAJO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

instaurado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995[1],

Vistos el artículo 29 y la letra a) del apartado 1 y el apartado 3 del artículo 30 de dicha Directiva,

Visto su reglamento interno, en particular sus artículos 12 y 14,

HA ADOPTADO EL PRESENTE DOCUMENTO DE TRABAJO:

1. INTRODUCCIÓN: LA EXPANSIÓN DE LOS SERVICIOS DE AUTENTICACIÓN EN LÍNEA

La creciente utilización de servicios de autenticación en línea ha transformado el panorama de Internet[2]. Cada vez es más frecuente que los sitios web propongan o exijan a sus usuarios que se registren, por ejemplo si facilitan información confidencial, ofrecen la posibilidad de registrar las preferencias del usuario, prestan un servicio de pago o si se trata de un servicio que se dedica al suministro de bienes. Todos estos tipos de sitios exigen al usuario que presente algún tipo de identificación, que suele constar de una dirección electrónica y algún tipo de verificación, normalmente una contraseña.

La utilización de la combinación «identificación de usuario/contraseña» plantea algunos problemas a los proveedores de servicios:

- Los usuarios suelen olvidar su contraseña. Los *help desks* cada vez reciben más llamadas o mensajes relativos al olvido de la contraseña. El coste que representa para los sitios web el restablecimiento de contraseñas también va en aumento.

- Cada vez es mayor el número de usuarios que utilizan métodos distintos de acceso a Internet, pero solicitan el mismo servicio a los proveedores de servicios. La tecnología de los métodos de acceso puede variar, desde el acceso a partir de un PC hasta el WAP, pero con mucha frecuencia se accede a Internet desde otros ordenadores, en cafés Internet o en bibliotecas publicas. Esto obliga a los usuarios a recordar múltiples contraseñas.

- Por último, a algunos usuarios les molesta tener que escribir su identificador de usuario y su contraseña, porque les supone una interrupción de la utilización. Los usuarios tienden a realizar el mínimo esfuerzo necesario, por lo que las contraseñas son breves y poco seguras y en muchos casos se repiten en otros muchos sitios web.

Cualquier solución a los tres problemas mencionados exige que el usuario delegue una parte de su autenticación. Actualmente se dispone de cuatro posibilidades:

---

[1] Diario Oficial L 281 de 23.11.1995, p. 31, disponible en: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

[2] Como ya señaló el Grupo de Trabajo en documentos anteriores, los principios de la Directiva son también aplicables a las actividades en línea. Véase, por ejemplo: *Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea*, adoptado el 21 de noviembre de 2002, WP 37.

- La administración de la contraseña se delega en el navegador del PC del usuario, como sucede, por ejemplo, en el gestor de contraseñas Mozilla.
- La administración de contraseñas se delega en un servidor *proxy* en Internet, en su caso facilitado por el proveedor de servicios de Internet.
- Un tercero facilita la autenticación mediante un protocolo de autenticación específico. Es lo que hace .NET Passport de Microsoft.
- La auténticación la realiza un contratista dentro de un «círculo de confianza». Se utilizaba un protocolo específico, como, por ejemplo, el del proyecto Liberty Alliance.

En los siguientes apartados se analizan estas posibilidades.

1. Un gestor de contraseñas en el PC
Contar con un gestor de contraseñas dentro del navegador de Internet únicamente resuelve una parte del problema. Ahorra al usuario el tener que escribir la contraseña, con lo que se reduce al mínimo el riesgo de pérdida de la misma. Pero no se resuelve el problema de los usuarios itinerantes que acceden a los servicios desde distintos ordenadores.

Desde el punto de vista de la protección de los datos, la situación es bastante sencilla. Todos los programas funcionan en el ordenador del usuario y bajo el control del mismo. No hay una empresa exterior que controle los datos. Se pregunta al usuario si se ha de incorporar la información en la base del gestor de contraseñas. El gestor de contraseñas registra la contraseña, pero no la envía sin el consentimiento del usuario. Desde el punto de vista de la seguridad es necesario tomar las medidas adecuadas para asegurarse de que el almacenamiento esté a salvo de ataques.

2. Utilización de un servidor proxy
En lugar de utilizar un gestor de contraseñas en el agente del usuario (es decir, el navegador), se puede instalar la misma funcionalidad en un servidor *proxy* en Internet. La funcionalidad es similar a la de los *proxies* que garantizan el anonimato, más conocidos. Un servidor *proxy* puede estar al servicio de muchos usuarios; por consiguiente, necesita registrar las contraseñas, una para cada usuario por cada sitio destinatario. Los usuarios deben confiar en el registro; esta confianza es muy explícita, porque el usuario debe tomar con conocimiento de causa la decisión de utilizar un *proxy* específico (no hay servicio por defecto). El usuario debe conectarse al *proxy* si desea utilizar sus contraseñas. Una vez conectado, el usuario extrae el mismo provecho del *proxy* que del gestor de contraseñas incorporado. La ventaja del *proxy* es que se puede acceder a él desde distintos ordenadores y desde otros tipos de aparato.

Estos *proxies* en ningún caso deben divulgar información sobre un usuario a un tercero sin el consentimiento del usuario. Si lo hacen, perderán la confianza de sus clientes y por consiguiente la razón de su existencia. Normalmente suele haber un contrato entre el proveedor de servicios *proxy* y el cliente. El servicio suele pagarse mediante otros recursos distintos de la publicidad, en su caso en combinación con el servicio prestado por un proveedor de servicios de Internet.

3. Servicios de autenticación en línea con protocolos especiales
Ninguna de las soluciones descritas anteriormente exige modificar el sitio web del proveedor. Otra posibilidad es realizar la autenticación utilizando un protocolo especial de autenticación. La arquitectura básica de estos protocolos es la misma; hay tres partes:

un usuario final, un proveedor de servicios y un proveedor de autenticación. Antes de que el proveedor de servicios preste el servicio, el proveedor de autenticación ha verificado la identidad del usuario. El proveedor de servicios confía en el proveedor de autenticación y acepta la introducción de usuario.

La arquitectura de .NET Passport utiliza un único servidor de autenticación, operado por Microsoft. El Passport contiene cierta información de identificación y autenticación, más otros datos de perfil. Se prevé que en el futuro se separen cada vez más estos dos conjuntos de información. El usuario que se ha conectado a Passport tiene un identificador único, un PUID. Si el usuario desea conectarse con un proveedor de servicios, ordena al servidor Passport que le facilite el PUID en una forma legible para el proveedor de servicios, actualmente codificado de manera simétrica.

El proyecto Liberty Alliance utiliza un modelo federado. El usuario puede federar su cuenta con dos proveedores de servicios. Una vez que una cuenta ha sido federada, un proveedor de servicios aceptará la introducción del otro proveedor, que a su vez actuará como servicio de autenticación.

El Grupo de Trabajo, consciente de la expansión de los servicios de autenticación en línea, decidió hace unos meses estudiar las repercusiones para la protección de datos del funcionamiento de estos sistemas[3]. El Grupo de Trabajo, aunque es consciente de la importancia de que existan mecanismos seguros de autenticación destinados a garantizar la seguridad y en particular la integridad de determinadas transacciones electrónicas, especialmente aquellas en las que se realizan pagos en línea, desea hacer hincapié en que el desarrollo de estos servicios debe respetar los principios de protección de datos que se establecen en la Directiva europea de protección de datos[4] y en las legislaciones nacionales que aplican esta Directiva.

2. CASO PRÁCTICO Nº 1: MICROSOFT .NET PASSPORT

.NET Passport es una iniciativa de notable importancia en este ámbito. Por ello, el Grupo de Trabajo realizó como primera prioridad un estudio inicial de este sistema en la primavera de 2002[5]. Tras un primer análisis, el Grupo de Trabajo llegó a la conclusión de que, aunque Microsoft había aplicado algunas medidas para resolver las cuestiones de protección de datos, una serie de elementos del sistema .NET Passport planteaba problemas jurídicos, por lo que era necesario seguir estudiándolos.

En los meses siguientes, el Grupo de Trabajo entabló un diálogo con Microsoft con el fin de comprender mejor el funcionamiento del sistema, debatir los distintos elementos en juego y especialmente evaluar si los principios europeos de protección de datos se aplican correctamente para, en su caso, determinar los elementos del sistema que han de modificarse. A raíz de este diálogo abierto y fructífero, Microsoft se ha comprometido a introducir cambios en el sistema que representarán mejoras desde el punto de vista de la protección de los datos.

---

[3] Consúltese el documento de trabajo WP 60, *Primeras orientaciones del Grupo de Trabajo del artículo 29 sobre los servicios de autenticación en línea*, adoptado el 2 de julio de 2002.

[4] Diario Oficial L 281 de 23.11.1995, p. 31, disponible en: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

[5] Consúltese el documento de trabajo WP 60, *Primeras orientaciones del Grupo de Trabajo del artículo 29 sobre los servicios de autenticación en línea*, adoptado el 2 de julio de 2002.

El compromiso de Microsoft de aplicar todas las medidas debatidas con el Grupo de Trabajo se recoge en varias cartas dirigidas al presidente del Grupo de Trabajo, el profesor Rodotà[6], y en un calendario en el que se fijan plazos para cada fase. La duración variable del período de aplicación se justifica por el distinto carácter de las fases. Algunas de las medidas acordadas, como la revisión del texto de la declaración de privacidad de .NET Passport y el suministro de información suplementaria sobre las páginas de registro, son sencillas y pueden aplicarse rápidamente. Otras, como el nuevo flujo de información que se describe más abajo, conllevan una nueva codificación del servicio .NET Passport, por lo que su aplicación requiere más tiempo.

El Grupo de Trabajo ha tomado nota del calendario presentado por Microsoft para satisfacer las preocupaciones del grupo. En el calendario se incluyen tres horizontes temporales: el primero abarca de 0 a 4 meses; el segundo, entre 4 y 8 meses; y el tercero, entre 8 y 18 meses. Después de cada medida se indicará el plazo entre paréntesis. Entretanto, algunas de las medidas debatidas se han aplicado y se indican posteriormente en el presente texto como prácticas actuales.

2.1. Breve descripción del sistema Microsoft .NET Passport

.NET Passport es un servicio de autenticación en Internet que ofrece un único inicio de sesión para numerosos sitios web colaboradores con el fin de ayudar a los usuarios a ahorrar tiempo y evitar la introducción repetida de sus datos cuando navegan por Internet. No se trata de un servicio de autorización o identificación, sino de autenticación, que tiene por objeto autenticar de una sola vez y de manera segura al usuario mediante la verificación de los datos que éste le presenta[7].

Se creó en 1999 y en el verano de 2000 se le asignó el nombre de .NET Passport. Actualmente hay más de 250 millones de cuentas en todo el mundo (un usuario puede tener varias cuentas, por ejemplo si tiene varias cuentas Hotmail). Más de 40 millones de cuentas pertenecen a residentes en la UE.

Hay varias maneras de obtener un Passport:
- en www.passport.net;
- en un sitio colaborador;
- abriendo una cuenta Hotmail.

Alrededor del 87 % de los usuarios se registran a través de un sitio colaborador o a través de Hotmail, en lugar de hacerlo directamente en el sitio de Microsoft. Alrededor de 120 millones de cuentas pertenecen a titulares de cuentas Hotmail y otra cantidad importante de usuarios se registra a través de Window Messenger. Hotmail es un servicio de correo electrónico utilizado en todo el mundo y completamente administrado por Microsoft Corporation u otras empresas controladas por Microsoft.

Actualmente se recogen tres tipos de datos personales:
1. Información mínima: nombre del usuario (dirección electrónica) y contraseña.
2. Datos personales: pregunta secreta y su respuesta, número de teléfono y número de identificación personal (PIN), clave de seguridad y otras tres preguntas y respuestas suplementarias, que son necesarias por si el usuario olvida su contraseña.

[6] Cartas de 19 de septiembre y 25 de noviembre de 2002.
[7] Debe tenerse en cuenta que, además de la Directiva sobre protección de datos, también podrían aplicarse otras directivas a estos servicios, como las que se refieren al comercio electrónico y a la firma electrónica.

Esta información no forma parte del perfil y no se transmite a otros sitios.
3. Información máxima relativa al perfil: la información mencionada, más nombre, apellido, zona horaria, sexo, fecha de nacimiento, ocupación y accesibilidad.
Los sitios participantes pueden optar por solicitar información suplementaria directamente al usuario y tratarla. Actualmente participan en .NET Passport 69 sitios exteriores (no relacionados con Microsoft), de los que 20 son sitios del EEE.

2.2. Problemas jurídicos planteados y resultado del diálogo con Microsoft

En su documento de julio de 2002, el Grupo de Trabajo señaló una serie de cuestiones que exigen un estudio más detallado. En los siguientes apartados se analizará cada una de estas cuestiones y el resultado del diálogo con Microsoft acerca de cada uno de los asuntos planteados.

Es importante señalar desde el punto de vista general que, además de las medidas específicas que se describen en los apartados siguientes, Microsoft ha decidido modificar el flujo de información de .NET Passport. Fundamentalmente, se volverá a codificar el servicio para separar claramente la creación de una cuenta .NET Passport del almacenamiento de datos personales en el perfil de Passport. Este nuevo flujo de información deberá tener, como se explicará con más detalle al tratar de las cuestiones de proporcionalidad, una repercusión positiva en la imparcialidad de la recogida y tratamiento de datos personales. El Grupo de Trabajo observa este hecho con satisfacción.

2.2.1. La información facilitada a los interesados en el momento de recoger los datos, tratarlos o transferirlos a terceros, situados en su caso en un tercer país

Cuando se comenzó a estudiar el funcionamiento del servicio de .NET Passport, el primer problema al que se enfrentó el Grupo de Trabajo fue la falta de información clara y transparente acerca de este sistema. Una parte de la información existente acerca del sistema era confusa, no ofrecía datos relativos a las principales cuestiones de la protección de datos (identidad del responsable del tratamiento, finalidad del mismo, derechos del interesado, destinatarios de los datos, elementos necesarios para garantizar un tratamiento imparcial) y en ocasiones contenía afirmaciones contradictorias.

Dos cuestiones que preocupaban especialmente al Grupo de Trabajo eran la falta de información adecuada acerca de la transmisión de datos personales a un tercer país y acerca de la relación entre Hotmail y Passport.

Entretanto, Microsoft se ha comprometido a aplicar las medidas siguientes con el fin de responder a las preocupaciones del Grupo de Trabajo sobre estas cuestiones:

- Microsoft facilitará, como recomendó el Grupo de Trabajo del artículo 29 en su recomendación 2/2001[8], un cuadro indicador que contendrá la información que se exige en el artículo 10 de la Directiva de modo muy accesible y fácil de utilizar. Se presentará un enlace con el cuadro indicador a los usuarios que se identifiquen como residentes en la Unión Europea justo en el punto de la página de registro en la que indiquen su país de residencia. Los usuarios que pulsen en el enlace podrán ver entonces el cuadro indicador

[8] Recomendación 2/2001 sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea, adoptada el 17 de mayo de 2001, WP 43.

en una ventana lateral. Esta característica estará disponible como máximo en abril de 2003.

- Los usuarios serán informados cuando se registren en un sitio colaborador del país en el que se encuentre el mismo (8-18 meses), y tendrán acceso a través del cuadro indicador a un enlace de la página de la Comisión Europea en la que figuran los países cuya legislación sobre protección de datos se considera adecuada con arreglo a las normas comunitarias (4-8 meses).

- Microsoft informará a los usuarios comunitarios a través del cuadro indicador sobre el período en el que mantiene los datos de registro (actualmente, no más de 90 días) (0-4 meses).

-Al principio del proceso se informará con claridad a los usuarios acerca del modo en que pueden abrir una cuenta .NET Passport sin utilizar su dirección electrónica verdadera, una funcionalidad que el Grupo de Trabajo ha recomendado en varias ocasiones que se incluya. Al mismo tiempo, se aconsejará a los usuarios acerca de las limitaciones de las cuentas seudónimas, de manera que puedan tomar una decisión con conocimiento de causa (8-18 meses).

- Microsoft se comprometió a actualizar todas las versiones lingüísticas de la declaración de privacidad de .NET Passport al mismo tiempo, salvo si por motivos locales es necesaria una modificación inmediata en una versión lingüística. En esos casos, que se prevé no sean muy frecuentes, Microsoft incluirá una indicación en las demás versiones lingüísticas de la declaración de privacidad en la que se señalará que se actualizarán en breve (0-4 meses).

-Microsoft se comprometió asimismo a emprender una serie de iniciativas relativas a la información que se proporciona a los usuarios de Hotmail con el fin de garantizar que cuando los usuarios se registren en Hotmail también se les informe de que deben obtener una cuenta Passport para acceder a Hotmail y que no pueden cerrar su cuenta Passport sin cerrar también su cuenta Hotmail (0-4 meses).

2.2.2. Valor y calidad del consentimiento dado por los interesados a estas operaciones.

Después de su análisis inicial del sistema, el Grupo de Trabajo se planteó algunas preguntas acerca de la validez y la calidad del consentimiento como fundamento del tratamiento, tal como se establece en la letra h) de la Directiva[9]. En otras palabras, no estaba convencido de quede el consentimiento dado por los usuarios fuera suficientemente informado, libre y específico, especialmente en el caso de los usuarios que se registren a través de Hotmail, o de la transmisión de datos personales a los sitios colaboradores.

Como se acaba de exponer, Microsoft ha decidido y está comprometido a aplicar un conjunto de medidas informativas destinadas a garantizar que se facilite a los usuarios información imparcial. Por otra parte, en relación con las posibilidades de que los usuarios decidan si facilitan información personal a Passport, el nuevo flujo de

[9] Se entenderá por «consentimiento del interesado» toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan.

información permitirá a los usuarios transmitir información personal a un sitio colaborador sin almacenarla en su perfil de Passport y obtener una cuenta Passport seudónima sin que se solicite información personal suplementaria (8-18 meses).

Por lo que respecta a los usuarios de Hotmail, además de la mejora del suministro de información, se están tomando medidas para que los usuarios tengan presente que cuando registran una cuenta Hotmail sus datos personales se utilizarán para enviarles publicidad (0-4 meses). Esto se hará señalando explícitamente en la página de registro de Hotmail que los usuarios aceptan recibir publicidad de Hotmail cuando suscriben las condiciones de Hotmail. Al igual que sucede con cualquier sitio colaborador, los usuarios que registren un .NET Passport en el sitio de Hotmail tendrán la opción de facilitar su información personal únicamente a Hotmail sin necesidad de almacenarla en su perfil de .NET Passport (8-18 meses).

El Grupo de Trabajo también debatió con Microsoft la posibilidad de que los usuarios de Hotmail puedan negarse a recibir publicidad personalizada. Microsoft explicó que una vez que los usuarios tienen una cuenta Hotmail, pueden negarse de manera gratuita a recibir publicidad personalizada, pero ello conlleva el cierre de su cuenta Hotmail. Los usuarios no pueden mantener una cuenta Hotmail gratuita sin recibir publicidad personalizada, ya que dicha publicidad genera los ingresos que permiten ofrecer gratuitamente una cuenta Hotmail.

El Grupo de Trabajo considera de todos modos que hay dudas acerca de la conformidad de esta práctica con la legislación europea, por lo que continuará reflexionando sobre esta materia en el futuro. No obstante, considera que está ligado a un problema específico, que es la práctica de algunas empresas consistente en ligar la prestación o servicio a la obligación de que el usuario acepte la utilización de sus datos con fines comerciales, sin la posibilidad de que aquél se niegue. Este problema, que es distinto de la cuestión de los servicios de autenticación en línea, objeto del presente documento de trabajo, se abordará en un contexto más amplio en el futuro.

Respecto al consentimiento que los usuarios dan a las sitios colaboradores, el nuevo flujo de registro proporcionará a los usuarios un Passport que contenga únicamente el nombre del usuario y su contraseña, separando la creación de una cuenta Passport de la decisión de transmitir datos personales a las sitios colaboradores o almacenarlos en el perfil (8-18 meses). Se informará a los usuarios de que pueden registrar un Passport en el sitio web Passport facilitando únicamente un nombre de usuario y una contraseña, y de que si se registran a través de un sitio colaborador podrán ser obligatorios otros datos para los fines de las actividades de dicho sitio (esta información se debe incluir en el cuadro indicador en el plazo de 4-8 meses). También se incluirá una nueva funcionalidad que permita a los usuarios decidir para cada sitio si desean transmitir sus datos de perfil. Se reconfigurará el perfil de usuario para que los usuarios puedan completar los campos que decidan y dejar otros en blanco (8-18 meses).

El nuevo flujo de información permitirá asimismo que los usuarios, cada vez que se registren en un sitio colaborador, puedan revisar la información de su perfil, modificarla, decidir si mantienen dichas modificaciones en su perfil de Passport y determinar qué información envían al sitio (8-18 meses).

2.2.3. La proporcionalidad y la calidad de los datos recogidos y almacenados por .NET Passport y transmitidos posteriormente a los sitios afiliados.

Al Grupo de Trabajo le preocupaba la cantidad de datos recogidos mediante Passport, especialmente los datos de perfil, y el hecho de que, una vez que el interesado crea un .NET Passport, los datos personales incluidos, si el interesado ha pulsado en las casillas de consignación los datos, se transmitan a todos los sitios colaboradores que visite y en los que inicie sesión, independientemente de si son necesarios para el sitio en cuestión. En el momento de emprender el primer estudio del sistema no era posible que el usuario autorizara la transmisión de una parte de los datos, ya que toda la información de perfil se consideraba un bloque.

El nuevo flujo de información que implantará Microsoft separará claramente la creación de una cuenta en .NET Passport de la decisión del usuario de transmitir información personal al sitio colaborador y, en su caso, a .NET Passport. Los usuarios podrán optar, mediante aceptación explícita, entre almacenar o no en su perfil de .NET Passport la información que decidan transmitir al sitio en el que se registren. Cuando un usuario que ha almacenado información en su perfil de .NET Passport visite otro sitios colaboradores, podrá modificar o eliminar la información de cualquiera de los campos antes de comunicársela al sitio colaborador. El usuario asimismo podrá decidir, mediante aceptación explícita, almacenar tales modificaciones y supresiones en su perfil de .NET Passport (8-18 meses).

Una vez introducidas, estas modificaciones, junto con la posibilidad de que el usuario decida no utilizar su dirección electrónica verdadera en determinados casos, resolverán las cuestiones planteadas por el Grupo de Trabajo, aunque a éste le gustaría continuar haciendo un seguimiento de esta cuestión, especialmente teniendo en cuenta el papel de Microsoft de responsable del tratamiento, así como de otros datos valiosos suministrados por los usuarios.

2.2.4. Las normas de protección de datos aplicadas a los sitios web *afiliados a .NET Passport.*

Otra preocupación del Grupo de Trabajo se refería a la falta de claridad respecto al nivel de protección que garantizan los sitios colaboradores.

En sus conversaciones con el Grupo de Trabajo, Microsoft explicó que no controla las prácticas de protección de datos de los sitios colaboradores, pero a través de sus contratos con dichos sitios impone una serie de salvaguardas, por ejemplo la obligación de que tengan una política de confidencialidad consistente y fácilmente accesible que se ajuste a las prácticas del sector, tomen medidas de seguridad adecuadas, cumplan la legislación aplicable y no utilicen los datos al margen de la prestación de servicios específicos sin el consentimiento del usuario.

Microsoft se ha comprometido a tomar una serie de iniciativas suplementarias:

- Revisará la declaración de privacidad para dejar sentado con claridad que Microsoft no controla las prácticas de protección de datos de los sitios colaboradores (0-4 meses).
- Microsoft animará a los sitios colaboradores a que se incorporen a TRUSTe, BBBOnLine o servicios análogos (0-4 meses).

- Se ofrecerá a los sitios colaboradores, tanto en la página en la que se recoge la información personal, como, de manera más detallada, mediante un enlace a partir de dicha página, la oportunidad de informar a los usuarios de los fines para los que el sitio utilizará los datos, sus destinatarios y el tiempo durante el que conservará los datos (8-18 meses).

El Grupo de Trabajo recomienda a Microsoft que informe a los sitios colaboradores en el plazo más breve posible de su recomendación sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea[10].

Deberá quedar claro en cualquier caso que, aparte del papel que desempeña Microsoft en el sistema .NET Passport, todos los sitios colaboradores deberán considerarse responsables del tratamiento de datos en relación con sus operaciones de tratamiento. Por consiguiente, son responsables de cumplir la legislación sobre confidencialidad.

2.2.5. La necesidad y condiciones de uso de un identificador único.

Desde el momento en que inició su análisis del sistema Passport, el Grupo de Trabajo reflexionó acerca de la utilización en .NET Passport de un identificador único (PUID) para cada usuario.

El identificador único Passport (PUID) se crea en el momento del registro y se mantiene mientras existe la cuenta. Tiene una longitud de 64 bits y se compone de dos partes: 16 bits para identificar el centro de datos desde el que se creó y 48 bits para identificar una cuenta específica. El requisito principal para crear el PUID es que sea único. El PUID no se basa en ninguna información facilitada por el titular de la cuenta y no se puede deducir del mismo información alguna acerca de los datos del titular de la cuenta.

El PUID se utiliza principalmente como índice de almacenes de datos de sitios específicos. El PUID por sí solo no permite el inicio de una sesión ni acceder a la información de perfil del usuario. Únicamente un tícket autenticación correctamente creado (que incluye el PUID), codificado en la clave asignada al sitio colaborador, puede utilizarse como bono de sesión. Cualquier usuario puede tener un PUID o más, dado que hay un PUID para cada cuenta Passport y los usuarios pueden tener más de una cuenta Passport.

Al Grupo de Trabajo le preocupaba principalmente que la utilización del PUID permitiera a los sitios colaboradores intercambiar información acerca de los usuarios de .NET Passport y crear perfiles de usuario. Los contratos entre Microsoft y los sitios afiliados prohíben la venta de registros PUID a terceros o el enlace entre sitios sin el consentimiento del usuario e imponen severas restricciones a la utilización del PUID, pero, pese a ello, siempre existe un riesgo cuando se dispone de la posibilidad técnica. Otra cuestión planteada por el Grupo de Trabajo fue la posibilidad de que los usuarios accedan a su propio PUID.

Respecto al segundo punto, Microsoft se comprometió a permitir que los usuarios que lo soliciten accedan a su PUID (8-18 meses). El Grupo de Trabajo desearía llamar la atención acerca del intervalo excesivamente largo para poder ejercer el derecho de acceso

[10] Recomendación 2/2001 sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea, adoptado el 17 de mayo de 2001, WP 43.

al PUID. Aunque no se proporcione el acceso en línea, deberían ofrecerse a los usuarios otros medios para ejercer su derecho a partir de ahora.

Se ha desarrollado un amplio debate entre Microsoft y los miembros del Grupo Operativo sobre Internet respecto a la utilización exclusiva de un identificador único. Microsoft comprende la inquietud del Grupo de Trabajo y ha decidido continuar estudiando otras arquitecturas de identificación para .NET Passport. Se ha acordado con Microsoft que se continuará el debate sobre esta cuestión en el futuro para tratar de encontrar una alternativa adecuada.

2.2.6. El ejercicio de los derechos de los interesados.

Al Grupo de Trabajo le preocupaban los actuales problemas relativos a los derechos de los interesados, en especial los que se plantean al tratar de cancelar la suscripción en Passport.

En sus contactos con el Grupo de Trabajo, Microsoft ha reconocido que anteriormente ha habido algunos problemas y ha acordado aplicar diversas medidas para facilitar el ejercicio de los derechos de los usuarios.

- Presentar en el cuadro indicador un resumen consistente y fácil de leer de la información exigida en el artículo 10 de la Directiva, incluida la relativa a los derechos del interesado (como máximo en abril de 2003).
- Informar a los usuarios en la declaración de privacidad y en el mensaje electrónico de presentación que deben dirigir sus preguntas y peticiones a passpriv@microsoft.com (práctica actual y 0-4 meses).
- Responder a las preguntas y peticiones de los usuarios de Passport en la lengua del cliente, siempre que Passport esté disponible en la misma (0-4 meses).

Desde septiembre de 2002, los usuarios pueden cerrar su cuenta .NET Passport fácilmente situándose en passport.net y pulsando en el enlace «servicios para usuarios». A continuación se irá guiando al usuario a través del procedimiento de cierre de su cuenta Passport particular. En el caso de las cuentas creadas en passport.net, el proceso está completamente automatizado. Se presenta al usuario una página en la que se exponen las consecuencias del cierre de la cuenta y se le ofrece un botón que puede pulsar para cerrarla. Para las cuentas creadas en Hotmail, el proceso es muy parecido: en primer lugar se dirige al usuario al sitio Hotmail, en el que aparece la página de cierre.

2.2.7. *Los riesgos para la seguridad que plantean estas operaciones*

El Grupo de Trabajo también examinó los posibles riesgos para la seguridad que puede conllevar el sistema, especialmente los relacionados con la concentración de datos en dos grandes bases de datos. Estas inquietudes se deben también a que Microsoft constituye un blanco muy destacado para los piratas informáticos.

El Grupo de Trabajo ha tomado nota de que Microsoft ha instaurado un programa de seguridad de la información en el marco del *Consent Order* («orden de consentimiento») emitido por la Comisión Federal de Comercio en 2002. Los requisitos principales son los siguientes:

- Inclusión de las salvaguardas administrativas, técnicas y físicas pertinentes, incluida la revisión de la política de seguridad sobre la base de la norma ISO 17799. Los

procedimientos normales de funcionamiento para cada grupo importante se modificarán en todo lo necesario para garantizar el cumplimiento del programa de seguridad de la información. Se realizará la actualización que sea pertinente de dichos procedimientos según la evolución tecnológica y económica.
- Designación de un asalariado o asalariados que coordinarán y serán responsables del programa de seguridad de la información. Algunos participantes destacados entre todos los cuerpos interesados prestarán ayuda para la creación y aplicación de los procedimientos normales de funcionamiento que se apliquen mediante el programa de seguridad de la información.

Se están formalizando y documentando varios programas al tiempo que se aplica el programa de seguridad de la información. En dichos programas se incluyen:

- Formación relativa a seguridad para operaciones y equipos de desarrollo de aplicaciones.
- Procedimientos de reacción ante las incidencias y de establecimiento de los pasos sucesivos.
- Creación de un grupo sectorial de supervisión de la seguridad.

2.3. Conclusión

El Grupo de Trabajo se congratula por las importantes medidas que Microsoft ha tomado y tomará en los próximos meses con el fin de garantizar que el sistema .NET Passport se ajuste a la Directiva europea de protección de datos. Naturalmente, el Grupo de Trabajo seguirá de cerca la evolución del sistema en los próximos meses, con el fin de observar el modo en que se aplican las medidas anunciadas por Microsoft.

El Grupo de Trabajo toma nota también de la preocupación expresada por algunas ONG acerca de la instauración de un sistema centralizado de almacenamiento de datos personales. El Grupo de Trabajo continuará haciendo un seguimiento sobre esta cuestión, asimismo en relación con las características de seguridad.

Por consiguiente, dado el carácter evolutivo del servicio .NET Passport, el posible desarrollo de su arquitectura futura y la necesidad de una reflexión permanente en torno a las cuestiones mencionadas, especialmente el PUID, el Grupo de Trabajo continuará supervisando la utilización del sistema y su desarrollo futuro, en caso necesario mediante el diálogo con Microsoft. Esta empresa ha aceptado ir informando al Grupo de Trabajo acerca de las medidas que tome en relación con el sistema .NET Passport.

3. CASO PRÁCTICO Nº 2: PROYECTO LIBERTY ALLIANCE

3.1. Breve descripción del sistema

El proyecto Liberty Alliance, establecido en diciembre de 2001, es una agrupación por contrato que actualmente abarca a más de 100 empresas, organizaciones sin fines de lucro y administraciones públicas de todo el mundo. Este proyecto no es una entidad jurídica, sino un proyecto específico en el que las distintas empresas participan según las condiciones de un acuerdo.

El cometido del proyecto Liberty Alliance es establecer normas abiertas de identidad de red federada mediante especificaciones técnicas abiertas. Los elementos clave del sistema son el inicio de sesión simplificado y la identidad de red federada (un sistema para

enlazar múltiples cuentas de un usuario determinado). El inicio de sesión único es la capacidad del consumidor de autenticarse una vez en una sesión con un proveedor de identidad, para navegar posteriormente a diversos proveedores de servicios dentro de ámbitos de confianza sin necesidad de una nueva autenticación.

El sistema funcionará dentro de ámbitos o círculos de confianza, que constituyen una federación de proveedores de servicios y de identidad relacionados empresarialmente sobre la base de la arquitectura de Liberty Alliance y acuerdos de funcionamiento, con la que los ordenantes pueden negociar en un entorno seguro y, según parece, sin problemas.

Las especificaciones del proyecto Liberty Alliance aún se encuentran en una fase muy temprana de desarrollo y por el momento no hay prácticamente ninguna aplicación[11]. Se prevé que en el futuro dichas especificaciones sean aplicadas por empresas tecnológicas con el fin de crear tecnologías que funcionen mediante Liberty.

3.2. Análisis de la situación actual

- El protocolo, en su estado actual, permite cumplir los requisitos de la Directiva. El Grupo de Trabajo desearía hacer hincapié en que Liberty Alliance es responsable en lo que respecta al desarrollo técnico del proyecto. Liberty Alliance debe aegurarse de que las especificaciones y el protocolo que elaboran permitan a los usuarios cumplir la Directiva. Además de esto, cada una de las empresas colaboradoras es responsable del tratamiento de los datos cuando administran un sitio que funciona con Liberty, por lo que también será resposable de cumplir la legislación vigente de protección de datos en el presente contexto.

- El protocolo de Liberty Alliance es neutral respecto a la protección de datos. Permite cumplir la Directiva, pero, indudablemente, no obliga a ello y no se toman medidas para garantizar su cumplimiento. El Grupo de Trabajo desea animar a Liberty Alliance a que elabore recomendaciones y directrices que impulsen a las empresas a utilizar las especificaciones de manera que se respete la confidencialidad o incluso se mejore la protección de la misma. El sistema también podría incluir características específicas relacionadas con la peculiaridad de la legislación europea sobre este ámbito. Esto podría tener especial importancia en relación con los proveedores de identidad que posean gran cantidad de información sobre los usuarios.

- El Grupo de Trabajo ha observado que numerosas empresas integradas en Liberty Alliance están establecidas en Estados Unidos, por lo que se prevé que, si se utilizan las especificaciones, de hecho se transferirán numerosos datos personales de Europa a dicho país. El Grupo de Trabajo pide a las empresas estadounidenses que participan en el proyecto Liberty Alliance que garanticen un grado adecuado de protección de los datos personales que les sean transmitidos.

- Actualmente, dado el desarrollo muy limitado de Liberty Alliance y puesto que aún no se utiliza de manera efectiva, es difícil prever con exactitud las consecuencias del uso de identidades binarias. No obstante, el Grupo de Trabajo desea hacer hincapié en que el sistema de identificadores binarios tiene la ventaja de que no establece un identificador único para el usuario, pero es necesario profundizar en esta cuestión desde la perspectiva de la protección de datos, especialmente en relación con la posibilidad técnica de que los sitios compartan los datos personales del usuario sin su consentimiento.

[11] Sun One funciona con Liberty.

Aun cuando la identidad binaria parezca ser un identificador más flexible que un identificador general, la posibilidad técnica de compartir las identidades binarias entre sitios colaboradores sigue suscitando inquietud.

3.3. Consideraciones acerca de las cuestiones en juego de cara al futuro

En este momento, las especificaciones de Liberty Alliance sólo son un prototipo que apenas se ha utilizado de manera efectiva y que indudablemente cambiará mucho en el futuro.

Por ello, el Grupo de Trabajo se propone seguir en el futuro su evolución para asegurarse de que se tengan en cuenta los requisitos de la Directiva. A este respecto, deberá estudiarse, por ejemplo, la utilización de *cookies*, la posibilidad de que los usuarios actualicen el descriptor[12], la federación automatizada[13], el cometido de los proveedores de identidad[14], el concepto y el funcionamiento de los «círculos de confianza» y los contratos que firmarán las empresas que utilicen una identidad federada.

El Grupo de Trabajo se propone pedir a Liberty Alliance que reflexione sobre las cuestiones planteadas en el caso práctico nº 1 y tener en cuenta las conclusiones de los debates con Microsoft cuando estudie las mismas cuestiones en relación con sus especificaciones. En concreto, deberán plantearse los mismos aspectos analizados respecto al PUID cuando se aborden los descriptores opacos y las identidades binarias en el ámbito de Liberty Alliance.

4. COMPARACIÓN ENTRE LOS ACTUALES SISTEMAS DE AUTENTICACIÓN EN LÍNEA

Gestor de contraseñas Mozilla	**Authenticación mediante *proxy***	**Passport de Microsoft**	**Liberty Alliance**
No hay un tercero que actúe como proveedor de identidad	El usuario elige a un tercero que actúa como proveedor de identidad	Microsoft actúa como tercero proveedor de identidad	El proveedor de servicios elige al tercero que actúa como proveedor de identidad (contratos recíprocos)
Únicamente acceso a través del PC propio	Acceso mediante los canales que ofrece el proveedor de autenticación	Posibilidad de acceder a través de distintos aparatos, actualmente sobre todo de tipo PC	Posibilidad de acceder a través de distintos aparatos, entre otros teléfonos móviles
Actualmente disponible y muy utilizado	Disponibilidad limitada	Actualmente disponible y utilizado por todos los servicios	Fases iniciales de aplicación

[12] El descriptor opaco es el medio utilizado para enlazar múltiples cuentas locales dentro del círculo de confianza. Lo reconoce alguno de los dos proveedores de un círculo de confianza. Un «descriptor» es una secuencia aleatoria compleja de caracteres que cada proveedor asocia a su propio registro del usuario.

[13] En el proyecto Liberty Alliance se utiliza la federación de cuentas para que los usuarios puedan enlazar cuentas o cerrarlas. La federación automática puede plantear problemas específicos.

[14] Una entidad que funciona con Liberty que se dedica a generar, mantener y gestionar información para ordenantes y proporciona autenticación de ordenantes a otros proveedores de servicios dentro de un «círculo de confianza».

		de Microsoft	
Identificador de usuario y contraseña para cada sitio	Identificador de usuario y contraseña para cada sitio	Identificador de usuario y contraseña únicos	Identificador de usuario y contraseña para cada sitio
El usuario se identifica con su identificador y su contraseña	El usuario se identifica con su identificador y su contraseña	Identificador único para un usuario (PUID)	Descriptor diferente por cada par de sitios
No es preciso contrato	Contrato entre el usuario y el proveedor	Contrato entre Microsoft y el proveedor de servicios	Contrato dentro de cada sitio de un círculo de confianza
-	El protocolo de autenticación exige que el proveedor de servicios *proxy* sepa qué sitios con autenticación se visitan (almacenamiento de la combinación UID/contraseña en cada sitio)	Microsoft emplea un PUID único por usuario	Único descriptor para cada usuario por par federado de sitios. El proveedor de autenticación únicamente necesita conocer los sitios en los que la identidad está federada
Si el usuario emplea identificadores distintos puede impedir que los proveedores de servicios combinen los datos entre ellos	Si el usuario emplea identificadores distintos puede impedir que los proveedores de servicios combinen los datos entre ellos	El usuario se identifica mediante un PUID único. Los acuerdos contractuales impiden que los proveedores de servicios combinen sus datos	Los datos sobre los usuarios únicamente pueden combinarse por pares de sitios. Los sitios determinan sus propios contratos recíprocos.
El proveedor de servicios es el único responsable del tratamiento de los datos	Tanto el proveedor de servicios como el proveedor de servicios *proxy* son responsables del tratamiento de los datos	El proveedor de servicios que atiende las solicitudes de autenticación y Microsoft son los responsables del tratamiento de los datos	Los proveedores de servicios dentro de un círculo de confianza se convierten en responsables del tratamiento de los datos cuando los usuarios visitan sus sitios
Los responsables del tratamiento no se transmiten datos	La información de autenticación se transmite entre los responsables del tratamiento	Los responsables del tratamiento se transmiten información de autenticación y en algunos casos información de perfil	Los responsables del tratamiento se transmiten datos
El usuario controla toda comunicación	Es necesario el consentimiento del usuario	Es necesario el consentimiento del usuario (exigido por la aplicación y los	Normalmente es necesario el consentimiento dos veces por federación,

		contratos de los servicios para usuarios)	pero es posible la federación automática
El protocolo de autenticación no requiere *cookies*	El protocolo de autenticación no requiere *cookies*	En la aplicación actual se utilizan *cookies*	En la aplicación actual se utilizan *cookies*

5. CONCLUSIÓN

El Grupo de Trabajo desea hacer hincapié en que se ha de considerar que las conclusiones a las que se ha llegado a través de los dos casos prácticos pueden aplicarse de manera general a cualquier sistema de autenticación al enfrentarse a cuestiones análogas. Se han elegido esos dos casos teniendo en cuenta el desarrollo actual del mercado de la autenticación en línea, pero para cualquier servicio de este tipo deberán tenerse presente las mismas observaciones relativas a la protección de datos. Pueden resumirse del modo siguiente:

- Tanto quienes crean como quienes implementan de manera efectiva sistemas de autenticación en línea (proveedores de autenticación) son responsables de la protección de los datos, aunque a niveles diferentes. Los sitios web que utilizan dichos sistemas (proveedores de servicios) tienen también su responsabilidad en el proceso. Es aconsejable que los distintos participantes suscriban acuerdos contractuales entre ellos en los que se expongan explícitamente las obligaciones de cada uno.
- Deberá ponerse todo el empeño posible en que puedan utilizarse de manera anónima o seudónima sistemas de autenticación en línea. En caso de que esto impida que sean plenamente funcionales, deberán crearse sistemas que exijan una información mínima únicamente para la autenticación del usuario y permitan que el usuario controle absolutamente toda decisión relativa a la información suplementaria (como los datos de perfil). Deberá existir esta posibilidad de elección tanto respecto al proveedor de autenticación como de los proveedores de servicios (los sitios que utilizan el sistema).
- Es fundamental ofrecer a los usuarios información adecuada sobre las consecuencias para la protección de datos del sistema (identidad del responsable del tratamiento, fines, datos recogidos, destinatarios, etc.). Deberá facilitarse esta información permitiendo un fácil acceso y utilización, preferiblemente en forma de recopilación o mediante un cuadro indicador que se abra automáticamente en la pantalla del usuario, en todos los idiomas en los que se ofrezca el servicio.
- Cuando los datos personales deban transferirse a terceros países, los proveedores de autenticación deberán trabajar con los proveedores de servicios, que tomarán todas las medidas necesarias para prestar la protección adecuada[15] o establecerán suficientes salvaguardas para garantizar la protección de los datos personales de los usuarios del sistema, mediante contratos o normas empresariales vinculantes. Esta deberá ser la norma general. Si en casos concretos se emplea el consentimiento como base de la transferencia, deberá proporcionarse a los usuarios suficiente información y posibilidad de elección. Deberán tener la opción de aceptar o rechazar en cada caso la transferencia.
- La utilización de identificadores, en cualquiera de sus formas, acarrea riesgos para la protección de los datos. Deberán estudiarse a fondo todas las alternativas posibles. Si son

[15] Esto es posible, por ejemplo, en Estados Unidos para las empresas que reúnen los requisitos del puerto seguro, a las que se exhortará a que se incorporen a este sistema. Evidentemente, sólo es aplicable en los casos en que la empresa del tercer país no encaje en el ámbito de aplicación de la Directiva.

imprescindibles los identificadores de usuario, deberá analizarse la posibilidad de que el usuario pueda actualizar su identificador.
- Se valoraría la adopción de una arquitectura de *software* que reduzca al mínimo la centralización de los datos personales de los usuarios de Internet y se fomentaría como medio para intensificar las propiedades de tolerancia respecto a los fallos del sistema de autenticación, así como para evitar la creación de bases de datos de elevado valor añadido pertenecientes a una sola empresa o un reducido conjunto de empresas y organizaciones y gestionadas por dicha empresa o conjunto.
- Los usuarios deberán contar con un medio sencillo para ejercer sus derechos (incluido su derecho a autoexcluirse) y para que se destruyan todos sus datos si deciden dejar de usar un sistema de autenticación en línea. También deberían recibir información adecuada sobre el procedimiento que han de seguir si desean formular preguntas o reclamaciones.
- La seguridad desempeña un papel fundamental en este ámbito, por lo que deben tomarse las medidas organizativas y técnicas adecuadas a los riesgos que se corren.

Dado el carácter evolutivo del servicio .NET Passport, del proyecto Liberty Alliance y otros servicios análogos de autenticación, el Grupo de Trabajo continuará haciendo un seguimiento de las novedades futuras en este campo, **especialmente para cerciorarse de que Microsoft cumple sus compromisos en el plazo propuesto, como se menciona** en el capítulo 2 del presente documento.

Hecho en Bruselas, 29 de enero de 2003
Por el Grupo de Trabajo
El Presidente
Stefano RODOTA