Módulo de autenticación PAPI para DokuWiki

Área web y comercio electrónico

Autor: **Luis Marco Giménez**
Consultor: **Francisco Javier Noguera Otero**

Junio de 2011

Licencia de la memoria

Resumen

Cuando se evalúan soluciones de autenticación de usuarios se suele mirar hacia dos tipos de enfoques: centralizados y distribuidos, y en cada situación uno u otro se suele presentar como más adecuado al problema que se desea resolver.

En general, un esquema centralizado de autenticación de usuarios resulta funcional cuando el número de usuarios es reducido, pero no tanto cuando intervienen diversas organizaciones con un gran número de usuarios. En estos casos se presentan problemas de escalado, y una solución a estos problemas suelen proporcionarla las soluciones distribuidas. PAPI es una de esas soluciones para la autenticación de usuarios de forma distribuida.

Por otro lado, DokuWiki es un wiki orientado a la creación de documentación de cualquier tipo. Sus usuarios pueden ser anónimos o autenticados y, en función del tipo de privilegio necesario, unos u otros podrán acceder a sus contenidos. Del mismo modo, su acceso se puede realizar remotamente desde cualquier punto u organización, es decir de forma distribuida, y aunque DokuWiki proporciona múltiples métodos de autenticación por defecto, y en la red se pueden encontrar otros tantos conectores adicionales que permiten su integración con este wiki en una amplia variedad de escenarios y lenguajes de programación, en la actualidad no existe ningún módulo de autenticación basado en PAPI.

El motivo por el que se ha escogido PAPI como solución distribuida para la autenticación de usuarios y acceso a recursos en DokuWiki se encuentra determinado por las ventajas que aporta PAPI frente a otras soluciones distribuidas, como es su simplicidad e independencia de la tecnología subyacente, la independencia de IP, la delegación de la gestión de los usuarios a las organizaciones origen permitiéndole a éstas el empleo de esquemas de autenticación propios, la transparencia para el usuario final, y la facilidad con la que los proveedores de información pueden obtener de estadísticas de acceso.

En definitiva, además de enriquecer a DokuWiki y a su comunidad con un nuevo método de autenticación, la publicación de este módulo de autenticación PAPI para DokuWiki bajo licencia GPL permite su libre uso por cualquier persona u organización interesada en él, realizar contribuciones para mejorarlo y, por tanto, garantizar su continuidad en el tiempo.

Tabla de Contenidos

Lista de figuras

1. Introducción

Desde finales del siglo pasado, y con más fuerza en el actual siglo XXI, los sistemas informáticos han pasado de su tradicional arquitectura de comunicaciones basada en entornos cerrados a la actual, y predominante, arquitectura basada en comunicaciones abiertas y distribuidas principalmente sobre la red de redes, es decir sobre Internet.

Internet es, en la actualidad, la red pública de comunicaciones más ampliamente usada en el mundo entero, indistintamente del tamaño y tipo de organización, como son multinacionales, universidades, gobiernos, o usuarios en general. Es, por tanto, un hecho de facto que cualquier clase de comunicación o negocio que se desee realizar de forma distribuida deberá transitar a través de esta red de comunicaciones, y es por ello que este predominio de Internet ha forzado, aunque ofreciendo a su vez una ventaja competitiva, a que muchos negocios usen Internet para establecer sus estrategias de negocio.

No obstante, y sin adentrarnos en los problemas de seguridad que puede representar la transmisión de datos a través de una red pública, y que se suelen solucionar de forma eficiente mediante algoritmos y protocolos de encriptación de datos, el carácter distribuido de las soluciones basadas en los protocolos TCP/IP de Internet con frecuencia presentan problemas de autenticación y autorización a recursos de información entre los extremos, habitualmente difíciles de gestionar en sistemas multi-organización o en aquellos donde el número de usuarios es relativamente alto, y en especial en sistemas donde la ubicuidad de estos suele ser alta, y aunque existe multitud de soluciones que proporcionan mecanismos fiables de autenticación, como pueden ser el filtrado de direcciones IP, sistemas de usuario y contraseña, certificados electrónicos, etc., la mayoría presenta dificultades en aspectos como la flexibilidad, movilidad o escalado.

Por todo ello, y tras evaluar las soluciones clásicas de autenticación y autorización a recursos de información de forma distribuida, se ha optado en este trabajo por el uso de una tecnología abierta para usar en entornos distribuidos a través de Internet, y que presenta las ventajas de ser libre, de sencilla implantación, flexible, escalable, y transparente para el usuario. Esta tecnología se denomina PAPI [1] (Punto de Acceso a Proveedores de Información), y ha sido desarrollada íntegramente por la institución española RedIRIS [2], por lo que además de los beneficios enumerados anteriormente, podemos añadir el soporte al usuario por una entidad de reconocido prestigio, no solo en España sino a nivel internacional.

Además, al ser PAPI una tecnología abierta con un protocolo bien definido, permite de forma sencilla su integración con cualquier proveedor de información que desee prestar servicios a través de la red independiente de su localización, y necesite poder autenticar a los usuarios de forma flexible, eficiente, independiente de la tecnología subyacente, y transparente para ellos, debido a que todos sus mensajes son transmitidos a través del protocolo HTTP mediante el uso de un navegador web.

Y cuando hablamos de cualquier proveedor de información, nos referimos a cualquier software o sistema capaz de publicar y compartir información en Internet, con recursos tanto públicos como restringidos a ciertos usuarios u organizaciones. En este caso optamos por el uso de un proveedor de información libre denominado DokuWiki [3], ampliamente utilizado como wiki para el almacenamiento de documentación de cualquier tipo. Por ello el desarrollo realizado en el ámbito de este trabajo se denomina "**Módulo de autenticación PAPI para DokuWiki**", ya que su objetivo ha sido la integración de la tecnología PAPI con DokuWiki como solución de autenticación de

usuarios y autorización de estos a los recursos de información almacenados en dicho wiki.

1.1. Objetivos

Como se ha anticipado anteriormente, el objetivo principal que se pretende alcanzar con el desarrollo de este proyecto es la implementación de un módulo, también denominado conector, que permita integrar DokuWiki con una infraestructura de autenticación de usuarios basada en PAPI.

Aunque DokuWiki proporciona múltiples métodos de autenticación por defecto [4], y en la red se pueden encontrar otros tantos conectores adicionales que permiten su integración con este wiki en una amplia variedad de escenarios y lenguajes de programación, incluyendo módulos que se integran dentro de un servidor Apache [5], en la actualidad no existe ningún módulo de autenticación basado en PAPI, motivo por el que se ha decidido abordar su desarrollo en este proyecto, además de los beneficios que esta tecnología aporta y que posteriormente serán descritos.

No obstante, y antes de abordar el objetivo principal del proyecto, existen otros objetivos previos que se deberán conseguir:

- Entender PAPI y el diseño de su protocolo de autenticación
- Conocer DokuWiki y el diseño de su arquitectura de autenticación
- Seleccionar una licencia libre para la publicación del módulo

1.2. PAPI y el diseño de su protocolo de autenticación

PAPI es un sistema que facilita el acceso a través de Internet a recursos de información que están restringidos únicamente a ciertos usuarios autorizados. Los mecanismos de autenticación empleados para identificar a los usuarios han sido diseñados para ser lo más flexibles posible, permitiendo que cada organización emplee un esquema de autenticación propio, manteniendo así los datos dentro de su propio ámbito, a la vez que los proveedores de información disponen de datos suficientes para realizar estadísticas. Desde el punto de vista del usuario, los mecanismos de control de acceso son transparentes para él y compatibles con los navegadores comúnmente empleados en cualquier sistema operativo, utilizando procedimientos HTTP estándar, por lo que no se requiere de ningún hardware o software específico, garantizando a los usuarios un acceso ubicuo a cualquier recurso de información al que tengan derecho.

Además, PAPI es una tecnología abierta que cuenta con el soporte de RedIRIS, así como de empresas que colaboran activamente en su comunidad [6], y con una arquitectura que consta de 4 componentes diferentes que se describen a continuación:

- Servidor de autenticación (**AS**): También denominado Proveedor de Identidad. Componente cuya responsabilidad es la de autenticar al usuario en su propia organización y asociarle un conjunto de atributos asociados al resultado de la autenticación.

- Punto de Acceso (**PoA**): Componente también conocido como Proveedor de Servicio, que realiza la autorización efectiva del acceso a un recurso protegido comprobando la autenticación del usuario y sus atributos, datos que habrán sido obtenidos previamente de un AS.

- Grupo de Puntos de Acceso (**GPoA**): Es un componente opcional en una arquitectura PAPI que permite agrupar de forma organizada varios PoA en un solo punto.

- **Proxy PAPI**: Es una funcionalidad opcional de un PoA. Implementa un proxy HTTP con re-escritura de los enlaces con respecto a un recurso web externo, de forma que cuando se accede a una URL bajo éste, el proxy edita los contenidos HTML para que los enlaces hagan referencia a él mismo, en lugar de al servicio final que protege.

Una arquitectura típica de una infraestructura basada en PAPI se muestra en la figura siguiente. En ella se puede observar cómo un GPoA agrupa dos PoA.

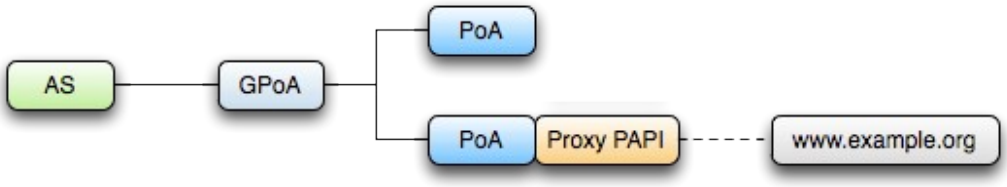

***Figura 1.1**: Arquitectura PAPI*

En una arquitectura PAPI básica, el módulo de autenticación desarrollado se situaría entre el proveedor de información (DokuWiki en este caso) y el punto de acceso (PoA) para controlar el acceso a los recursos almacenados en DokuWiki, de modo que el módulo sería el responsable de la comunicación con el PoA, y éste a su vez se comunicaría con el servidor de autenticación local (AS) para identificar a los usuarios de la organización. No obstante es más habitual encontrar soluciones basadas en PAPI en las que el PoA no se comunica directamente con el AS, sino que se inserta un controlador de un grupo de puntos de acceso (GPoA) con el fin de flexibilizar la arquitectura. Este enfoque es el que se va a adoptar en el sistema a desarrollar, y es el que se muestra en la siguiente figura.

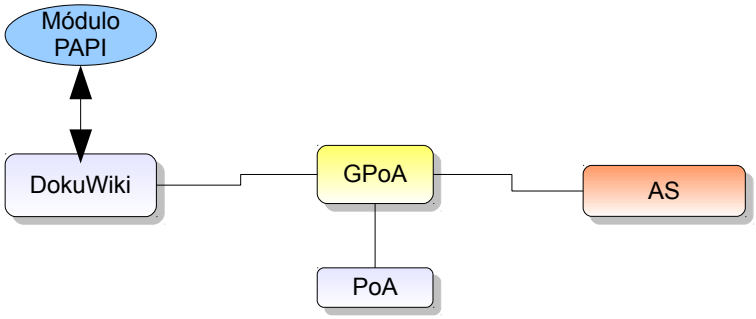

***Figura 1.2**: Arquitectura del sistema a desarrollar*

En este caso se deberá analizar cómo funcionan los mecanismos de PAPI para la autenticación y autorización a recursos protegidos y distribuidos en red, estudiando los mensajes del protocolo transmitidos mediante métodos GET o POST sobre HTTP, y teniendo en cuenta que la filosofía de PAPI es mantener la autenticación como una cuestión local a la organización a la que pertenece el usuario, delegando en los proveedores de información el proceso de autorización y acceso de dichos usuarios, previamente autenticados, a sus recursos de información.

1.3. DokuWiki y la arquitectura de su autenticación

DokuWiki es un wiki de uso sencillo, de código abierto y compatible con estándares, orientado a crear documentación de cualquier tipo dentro de un grupo de desarrolladores, grupos de trabajo y pequeñas empresas. Su sencilla y potente sintaxis facilita la creación de textos estructurados, permitiendo que los archivos generados sean legibles incluso fuera del wiki. Todos sus datos se almacenan en archivos de texto plano, tanto los relativos a su configuración como los de contenido, no siendo necesario el uso de ninguna base de datos para su funcionamiento, lo que simplifica su instalación y configuración.

Por otro lado, DokuWiki proporciona unos mecanismos de control de acceso a sus recursos extremadamente sencillos desde el punto de vista de la programación, lo que redunda en la simplificación del desarrollo del componente de autenticación.

Además, DokuWiki dispone de una amplia documentación y comunidad de usuarios y desarrolladores en Internet que le presta soporte, lo que facilita el desarrollo y adaptación de componentes software para este wiki.

El sistema de autenticación proporcionado por DokuWiki es completamente abierto y configurable a través de diferentes módulos denominados *backends* [7]. Se pueden utilizar los mecanismos de autenticación básicos que proporciona DokuWiki en su instalación básica, cualquiera de los disponibles en Internet, o incluso desarrollar uno propio a partir de los incluidos en su instalación por defecto. Esta última alternativa es la que se va a emplear en este proyecto.

En cualquier instalación de DokuWiki los *backends* se encuentran en la ruta *inc/auth* como clases independientes implementadas en PHP. La nomenclatura de estas clases sigue la sintaxis *nombre_de_clase.class.php*, de modo que una clase que implemente mecanismos de autenticación basados, por ejemplo, en directorios LDAP se denominará ldap.class.php. Siguiendo esta sintaxis, la clase que implementará la autenticación basada en PAPI se denominará:

```
papi.class.php
```

El *backend* que DokuWiki utilizará para realizar la autenticación se configura a través de un fichero de texto plano ubicado en la ruta *conf/dokuwiki.php*, estableciendo en la variable *$conf['authtype']* el nombre de la clase a utilizar. En nuestro caso se utilizará el nombre *'papi'*, quedando la configuración de la autenticación de la siguiente forma:

```
$conf['authtype'] = 'papi';
```

En este mismo fichero se podrá especificar otras opciones de configuración específicas para el *backend*, como pueden ser rutas a otros componentes utilizados, valores iniciales de variables, etc. La forma general de establecer estos parámetros de configuración se realiza a través de variables PHP con la sintaxis: *$conf['nombre_de_clase] ['parámetro'] = 'valor_parámetro'*. En nuestro módulo los parámetros de configuración seguirán dicha notación, como por ejemplo para establecer la ruta del PAPI PoA que la clase a implementar utilizará:

```
$conf['papi'] ['path'] = '/usr/share/php5/papi_poa/';
```

1.4. Elección de una licencia libre para la publicación del módulo

El módulo a desarrollar se va a situar entre otros componentes software con licencias libres, de modo que será necesario evaluar las licencias de cada uno de ellos de forma individual para escoger una licencia compatible.

DokuWiki posee dos tipos de licencias diferenciadas: una que protege el software propiamente dicho, y otra que protege los contenidos de su sitio web. En lo relativo al desarrollo de componentes para DokuWiki únicamente se deberá tener en consideración la licencia que protege el software, y que en este caso es la GNU General Public License GPL [8].

De forma resumida, esta licencia establece que:

a) El usuario tiene derecho a:
   1. Obtener el software y su código fuente
   2. Puede usar el software de la manera que desee
   3. Tiene permiso para modificar el código fuente y adaptarlo a sus necesidades

b) El usuario debe aceptar los siguientes términos:
   1. No se proporciona ninguna garantía de ningún tipo con el software
   2. Si se desea redistribuir el software, se debe hacer bajo los términos de la licencia GPL, lo que significa que se debe redistribuir el código fuente completo, incluyendo sus modificaciones
   3. No se puede redistribuir este software atribuyéndose la autoría

Por otro lado, la tecnología PAPI es un estándar abierto, y los módulos software que distribuye RedIRIS, y que implementan diversos componentes de esta tecnología, se encuentran también protegidos por licencias GPL.

Tal y como se ha expuesto, los dos componentes principales con los que el módulo de autenticación se va a integrar se encuentran licenciados bajo la licencia GPL. Esta licencia se diseñó cuidadosamente para promover la producción de cada vez más software libre, prohibiendo explícitamente algunas acciones sobre el software que podrían conducir a la integración de software protegido por la GPL en programas propietarios. La GPL usa como base legal la legislación sobre copyright, haciendo de esa forma un uso muy interesante de ella ya que se usa el copyright para promover la distribución de software que garantiza mucha más libertad a los usuarios que los trabajos habitualmente protegidos por copyright. Por lo tanto, algunas veces se dice que el software cubierto por la GPL está *copylefted*, un interesante juego de palabras en inglés.

Debido a las restricciones de la GPL, la integración completa sólo es posible con software cubierto por la misma licencia, por lo que el componente de autenticación PAPI se distribuirá bajo licencia GNU GPL.

Otro aspecto que se deberá tener en cuenta es la licencia de la documentación que acompañará al módulo de autenticación. En este caso, y siguiendo la tendencia de publicar bajo una licencia libre, se opta por una licencia Creative Commons [9], más adecuada para contenidos que la GPL, en concreto la licencia Attribution-Share Alike 3.0 (CC BY-SA 3.0). Esta licencia establece que se permite el uso comercial de la obra y de sus posibles obras derivadas, aunque la distribución de éstas se debe realizar con una licencia igual a la que regula la obra original:

- BY - Attribution (Reconocimiento): En cualquier explotación de la obra autorizada por la licencia hará falta reconocer la autoría.

- SA - Share Alike (Compartir Igual): La explotación autorizada incluye la creación de obras derivadas siempre que mantengan la misma licencia al ser divulgadas.

En el siguiente capítulo se hace un análisis de las alternativas disponibles en la actualidad frente a PAPI para abordar el problema que se desea resolver, describiendo y justificando la solución escogida, para a continuación, en el capítulo 3, establecer los requisitos que el sistema debe cumplir. Debido a que el sistema a implementar requiere cierta interactividad con el usuario, en el capítulo 4 se detallan las interfaces de usuario necesarias para realizar dicha interacción.

Antes de comenzar con el diseño y desarrollo del sistema es conveniente, como en cualquier proyecto de otras disciplinas, realizar un análisis de riesgos a fin de minimizarlos o, incluso, evitarlos completamente. Este análisis se realiza en el capítulo 5. Tras esta evaluación se establece el plan de pruebas que el sistema deberá superar para considerarlo válido, es decir que cumple con los requisitos establecidos. Este plan de pruebas es descrito en el capítulo 6 del documento.

En el capítulo 7 se realiza una descripción del software necesario para el desarrollo del proyecto, así como la elección de licencias para el módulo a desarrollar, ya que ésta se puede ver afectada por el software con el que se deberá integrar.

En el capítulo 8 se establece una planificación temporal preliminar donde se estima el coste que supondrá el desarrollo del módulo de autenticación, mientras que en capítulo 9 se hace una breve revisión del presupuesto necesario para completar el proyecto.

En los capítulos 10 y 11 siguientes se realiza el diseño completo del sistema, considerando todos los elementos que intervendrán así como su arquitectura lógica, y se profundiza en el proceso de desarrollo del módulo de autenticación, indicando con precisión el coste real que se ha empleado en el proyecto, los elementos necesarios para su implementación, así como el resultado de las pruebas unitarias y de integración que finalmente han conducido a un módulo que cumple con las especificaciones iniciales.

Para finalizar, los capítulos 12, 13, 14 y 15, contienen información sobre cómo realizar una implantación del módulo en un sistema real y cómo se debería enfocar su mantenimiento, las conclusiones finales tras el desarrollo del proyecto, anexos de interés, y una lista de referencias utilizadas durante el proceso de creación del módulo.

2. Alternativas y solución escogida

Como se ha expuesto en la introducción, DokuWiki proporciona múltiples métodos de autenticación por defecto, y en la red se pueden encontrar otros tantos conectores adicionales que permiten su integración con este wiki, sin embargo actualmente no existe ningún módulo de autenticación basado en PAPI.

En cualquier caso, cabría considerar la elección de PAPI como método de autenticación y autorización a recursos protegidos en Internet frente a otras alternativas disponibles. Para ello, a continuación se realizará una enumeración de algunas de ellas junto con una breve descripción, detallando en cada caso las razones por las que se considera más adecuado la utilización de PAPI en cada escenario:

Alternativas a valorar	
Nº 1	Nombre de usuario y contraseña
Nº 2	Filtrado por direcciones IP
Nº 3	Servidores centralizados de autenticación
Nº 4	Mecanismos de clave pública

***Figura 2.1**: Alternativas a PAPI para la autenticación*

2.1. Alternativa 1: Nombre de usuario y contraseña

El esquema de autenticación basado en usuario y contraseña es un sistema de implantación sencilla, pero tiene el principal inconveniente de los problemas de escala, especialmente importantes cuando los recursos que han de ser accedidos son proporcionados por otra organización, típicamente un proveedor de información. En este caso lo habitual es que el proveedor de información no esté dispuesto a mantener un registro detallado de los usuarios individuales de la organización cliente, ni a atender las diferentes incidencias relacionadas con el acceso de cada usuario. Por otro lado, tampoco suele resultar aceptable el empleo de un par usuario y contraseña general para toda la organización cliente, dado que esto limita la capacidad de obtener estadísticas significativas sobre el uso de los recursos y, más aún, lleva casi indefectiblemente a que se multiplique el uso de los recursos por medio de personas no autorizadas. PAPI, por el contrario, además de no presentar los problemas de escala de estos sistemas, permite liberar a los proveedores de información de la gestión de los usuarios, así como permite disponer a estos de suficientes datos para la obtención de estadísticas de acceso a los recursos por organización y usuarios.

2.2. Alternativa 2: Filtrado por direcciones IP

Los esquemas de autorización basados en la dirección IP origen permiten el acceso a los recursos únicamente a un rango de direcciones IP definidas por la organización cliente. Este sistema presenta el inconveniente de que limita seriamente la movilidad de los usuarios. Es habitual que las organizaciones doten, cada vez más, de soluciones de movilidad a sus empleados, y que estos puedan acceder a todos sus servicios de forma remota y ubicua. En estos escenarios el filtrado de direcciones IP no funciona, mientras que soluciones como PAPI resuelven este problema de forma sencilla y eficaz al no depender de ningún rango determinado de direcciones IP.

2.3. Alternativa 3: Servidores centralizados de autenticación

Ejemplos ampliamente utilizados son Radius y Kerberos. Estos servidores se caracterizan por ser soluciones de autenticación centralizadas en la misma organización propietaria de los servicios y gestora del sistema de seguridad, mientras que PAPI, por el contrario, tiene un carácter distribuido permitiendo delegar la gestión de los usuarios en las organizaciones origen de los mismos. En general, un esquema centralizado resulta funcional cuando el número de usuarios es reducido y asumible para la organización gestora, pero cuando intervienen varias organizaciones con un número considerable de usuarios, los sistemas centralizados presentan problemas de escalado. Desde el punto de vista del registro y actualización de los datos de los usuarios, es más lógico que dicha información sea gestionada por las organizaciones origen de los usuarios, que son quienes mejor conocen dicha información y tienen derechos legales para su gestión, por lo que, bajo esta perspectiva, una solución basada en PAPI se adapta mejor que una solución centralizada.

2.4. Alternativa 4: Mecanismos de clave pública

Desde el punto de vista de la gestión de usuarios que pertenecen a diferentes organizaciones, las soluciones distribuidas como PAPI o las apoyadas en mecanismos de clave pública basadas en certificados electrónicos son claramente ventajosas. En este sentido, la puesta en marcha y mantenimiento de una autoridad de certificación que englobe a varias organizaciones requiere un nivel de recursos a tener en cuenta, debido a que hay que gestionar tareas de registro, firma y revocación de certificados, además de estar conforme con los requisitos legales aplicables, por lo que en este sentido PAPI se posiciona como una alternativa más sencilla y económica que los habituales mecanismos de clave pública basados en certificados electrónicos.

2.5. Conclusiones

En la siguiente figura se muestra un resumen de las ventajas que ofrece la solución escogida frente al resto de las alternativas valoradas:

Alternativa	Ventajas de PAPI
1 – Nombre de usuario y contraseña	• No presenta problemas de escalado • Se libera al proveedor de información del mantenimiento de los pares usuario / contraseña • Facilita la obtención de estadísticas a los proveedores de información
2 – Filtrado por direcciones IP	• No limita la movilidad de los usuarios
3 – Servidores centralizados de autenticación	• Carácter distribuido • Delegación de la gestión de los usuarios en las organizaciones origen de los mismos • No presenta problemas de escalado
4 – Mecanismos de clave pública	• Reducida complejidad y bajo coste

***Figura 2.2**: Comparación de PAPI frente a otras alternativas*

En resumen, se considera PAPI como una alternativa viable frente a otras soluciones por los siguientes motivos:

- Es un sistema distribuido que no presenta problemas de escalado
- Proporciona mayor flexibilidad frente a otras soluciones al permitir que cada organización emplee un esquema de autenticación propio
- Permite a los proveedores de información disponer de los datos suficientes para la obtención de estadísticas de acceso a sus recursos
- Garantiza a los usuarios un completo acceso ubicuo a los recursos de información a los que tengan derecho
- Los mecanismos de control y acceso son transparentes para el usuario
- Es compatible con los navegadores comúnmente utilizados en cualquier sistema operativo
- Es independiente de la tecnología utilizada
- Reducida complejidad y bajo coste

2.6. Lenguaje de programación

Debido a que DokuWiki se encuentra íntegramente desarrollado en PHP [10], y que existen módulos PAPI desarrollados por RedIRIS en este mismo lenguaje de programación, el lenguaje escogido para la implementación del módulo de autenticación también será PHP. Esta elección pretende reducir, e incluso eliminar, posibles problemas de integración entre ambos sistemas, además de prescindir de herramientas complejas para su desarrollo, tales como compiladores, enlazadores, entornos de desarrollo integrados, librerías externas, etc.

Del mismo modo, al ser PHP un lenguaje interpretado y multiplataforma como sucede con el resto de la infraestructura utilizada por PAPI: Apache, OpenSSL [11], etc., el desarrollo, las pruebas y la depuración se podrán realizar en cualquier sistema operativo y plataforma hardware.

Por tanto, para la implementación del módulo de autenticación se utilizará el sistema de autenticación modular que DokuWiki dispone y que permite su integración con cualquier *backend* desarrollado en PHP, en este caso con un *backend* basado en PAPI.

3. Requisitos, Casos de uso

3.1. Requisitos del sistema

El desarrollo de cualquier componente que use PAPI deberá basarse en un conjunto de requisitos establecidos por esta arquitectura y que definen las principales características del sistema a nivel funcional [12], por lo que los requisitos de PAPI son aplicables al conector a desarrollar en este trabajo:

- **Acceso independiente de la IP origen**: El sistema de control de acceso debe ser independiente de la IP origen de la conexión.

- **Acceso autenticado a recursos durante un período limitado de tiempo:** Una vez realizada la autenticación por un AS, el usuario debe tener acceso a todos los recursos durante un período limitado de tiempo sin requerírsele nuevas autenticaciones (mecanismo de *Single-Sign-On*). Estas sesiones deberán tener un límite temporal que podrá ser configurado en cada instalación concreta.

- **Garantía de movilidad del usuario**: Los usuarios podrán acceder a los recursos a los que están autorizados independientemente del sistema de conexión empleado o su localización en red. Además, los procedimientos para el acceso deberán ser idénticos para los usuarios locales y remotos.

- **Transparencia para el usuario:** El sistema debe ser lo más transparente posible para el usuario, de forma que la intervención de éste sea mínima.

- **Compatibilidad con otros sistemas de control de acceso**: El sistema debe poder ser utilizado en conjunción con otros sistemas de control de acceso existentes.

- **Independencia tecnológica:** El sistema debe poder ser compatible con cualquier plataforma hardware y software capaz de ejecutar un servidor web con soporte PHP, mcrypt [13] y OpenSSL.

- **Compatibilidad con los navegadores más utilizados:** La solución debe ser compatible con los navegadores web más extendidos: Mozilla Firefox, Google Chrome, Microsoft Internet Explorer, Opera y Safari.

- **Garantía de la privacidad del usuario**: Se deben implementar mecanismos que garanticen el anonimato en el acceso a ciertos servicios.

- **Facilidad para la obtención de estadísticas por los proveedores:** El sistema debe garantizar que los accesos puedan ser discriminados por usuario u organización, para así poder obtener estadísticas de acceso fiables.

3.2. Casos de uso

Caso de Uso: Sistema
Este caso de uso presenta una visión general del sistema, y describe la petición que un usuario haría al proveedor de información con DokuWiki para obtener un recurso de información protegido por PAPI.

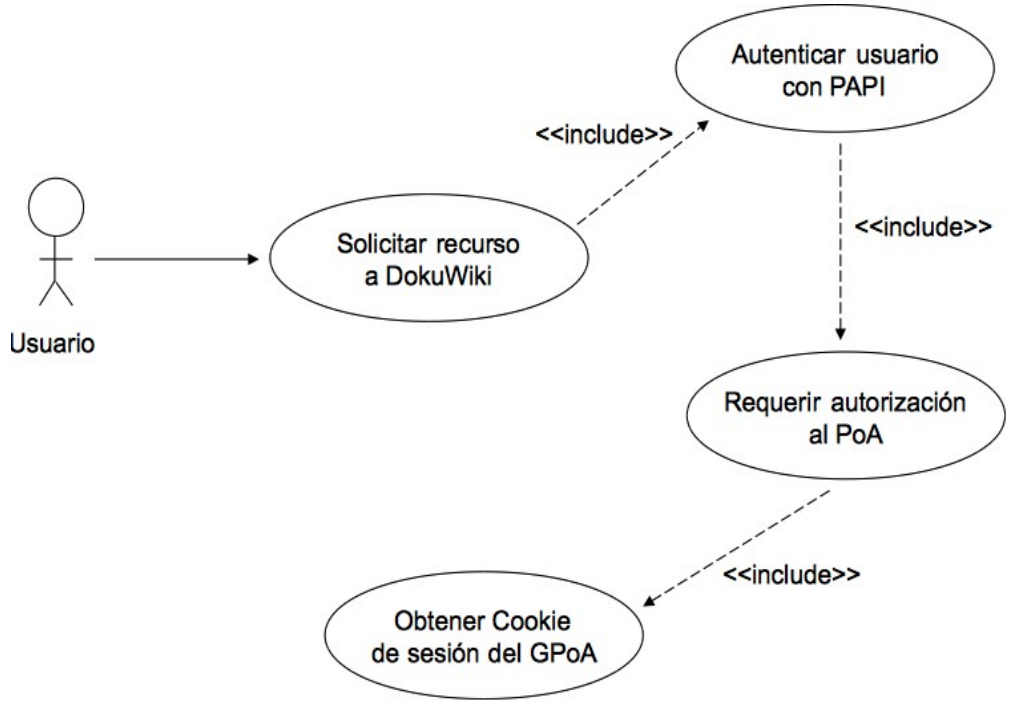

***Figura 3.1**: Caso de uso del sistema*

Caso de Uso: Obtener Cookie de Sesión del GPoA
Mediante este caso de uso se muestra el proceso a través del cual se solicitaría la cookie de sesión del GPoA para verificar si el usuario se autenticó con anterioridad. En caso contrario se solicitaría un mensaje WAYF del protocolo PAPI.

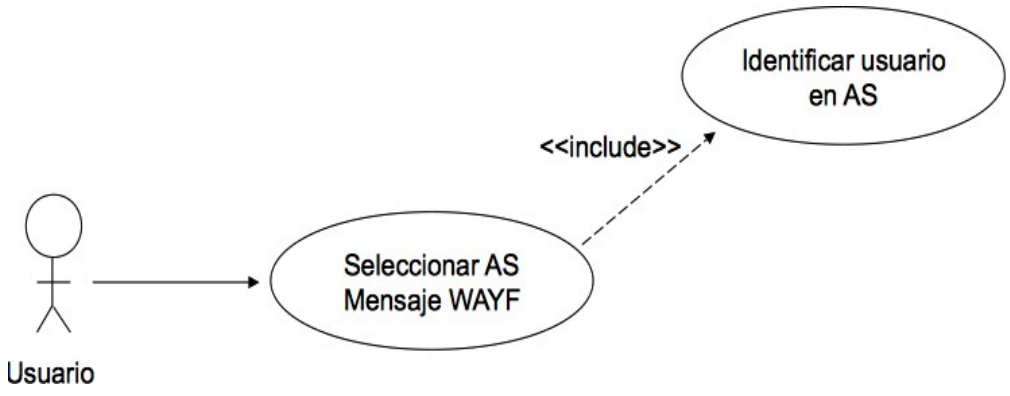

***Figura 3.2**: Caso de uso "Obtener Cookie de Sesión del GPoA"*

4. Interfaces de usuario

Debido a que el desarrollo del proyecto es un módulo que proporciona mecanismos de autenticación integrado en un wiki, no se dispondrán de interfaces de usuario propiamente dichas, ya que su funcionalidad se basará en el intercambio de mensajes entre los componentes con los que interviene: PAPI y DokuWiki. En este caso las interfaces de usuario utilizadas serán las que ambos productos proveerán para su funcionamiento. No obstante, y para facilitar el desarrollo del módulo y sus pruebas, así como para ilustrar su operativa, se va a definir un escenario ficticio de funcionamiento en el que se mostrarán las diferentes interfaces web con las que el usuario debería interactuar para completar su acceso como usuario autenticado.

En este escenario se definen dos organizaciones con sus respectivos usuarios, dos AS, un GPoA, y un PoA. En la siguientes tablas se resumen los datos del escenario completo:

Organización	Usuarios	Descripción
AEAT	aeat1, aeat2	Agencia Estatal de Administración Tributaria
INEM	inem1, inem2	Instituto Nacional de Empleo

Proveedor de información	Wiki	URL de acceso a la información
luismarco	DokuWiki con módulo de autenticación PAPI	http://dokuwiki.papi.luismarco

Componente PAPI	Descripción	URL de acceso al componente PAPI
PoA	Punto de acceso	http://poa.papi.luismarco
GPoA	Agrupación de PoA	http://gpoa.papi.foo.com
AS	AS de AEAT	http://as.papi.aeat.com
AS	AS de INEM	http://as.papi.inem.com

Con este escenario, y con los casos de uso definidos anteriormente, el funcionamiento del proceso de autenticación desde que un usuario se conecta por primera vez al proveedor de información (DokuWiki con autenticación PAPI), hasta que se le concede o deniega el acceso es el siguiente:

1. Al acceder al proveedor de información mediante el navegador web a través de la URL *http://dokuwiki.papi.luismarco*, el módulo de autenticación creado para DokuWiki efectuará la conexión con el PoA en *http://poa.papi.luismarco*, y éste a su vez redireccionará a su GPoA (definido en este caso en la dirección *http://gpoa.papi.foo.com*). Según el protocolo definido por PAPI, cuando no exista una clave de sesión para el usuario, o ésta haya expirado, el GPoA preguntará al usuario a través del mensaje *Where Are You From?* (WAYF) para que el usuario seleccione su servidor de autenticación (AS), es decir el de su organización, de entre los definidos en el GPoA. En el caso de que ya exista una clave de sesión para el usuario, porque ya fue autenticado con anterioridad y sus credenciales siguen siendo válidas, el GPoA devolverá un mensaje de acuerdo al PoA para que éste pueda continuar con la validación del acceso a los recursos solicitados por el usuario.

2. La selección del AS se realizará mediante una lista desplegable en la que el GPoA ofrecerá una lista de los AS disponibles para su autenticación (en este caso AEAT AS e INEM AS para las organizaciones AEAT e INEM, respectivamente), tal y como se muestra en la figura.

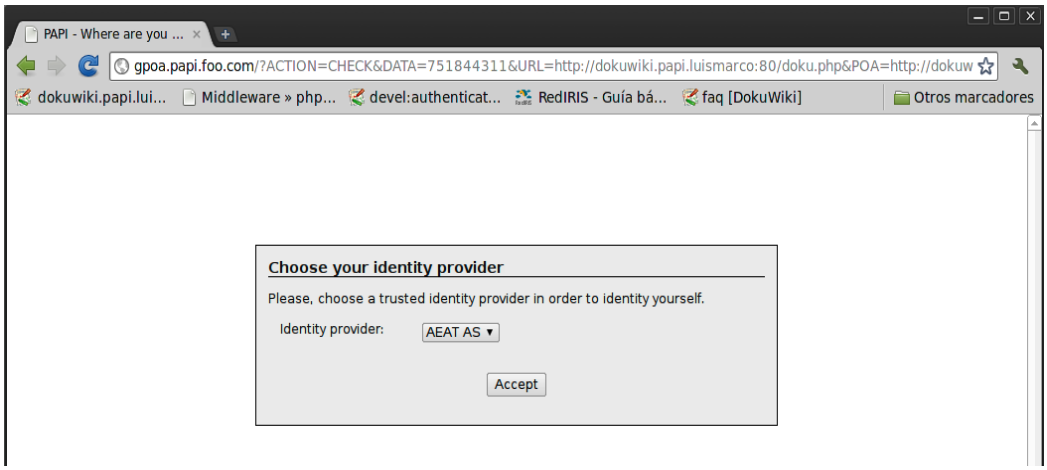

***Figura 4.1**: Selección del AS – Mensaje WAYF de PAPI*

3. Una vez que el usuario haya seleccionado el servidor de autenticación (AS) de la organización a la que pertenece, será dicha entidad la responsable de su autenticación y establecimiento de los atributos correspondientes al usuario. Éste escenario es el mostrado en la siguiente figura.

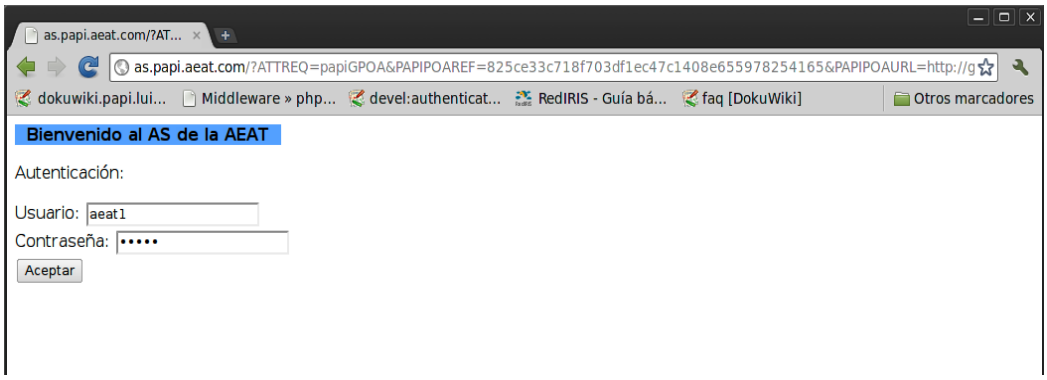

***Figura 4.2**: Autenticación en el AS de la organización del usuario*

4. Si la autenticación se completó con éxito, el AS redirigirá la petición al GPoA, y éste a su vez al PoA. El módulo de autenticación obtendrá y verificará del PoA los atributos de autenticación que el AS ha devuelto, y procederá a autorizar o denegar el acceso a los recursos de información que protege.

   En la siguiente figura se muestra la pantalla que el proveedor de contenidos con DokuWiki mostrará una vez el usuario se encuentre autenticado. En este ejemplo el usuario autenticado es *aeat1,* el cual pertenece a la organización AEAT.

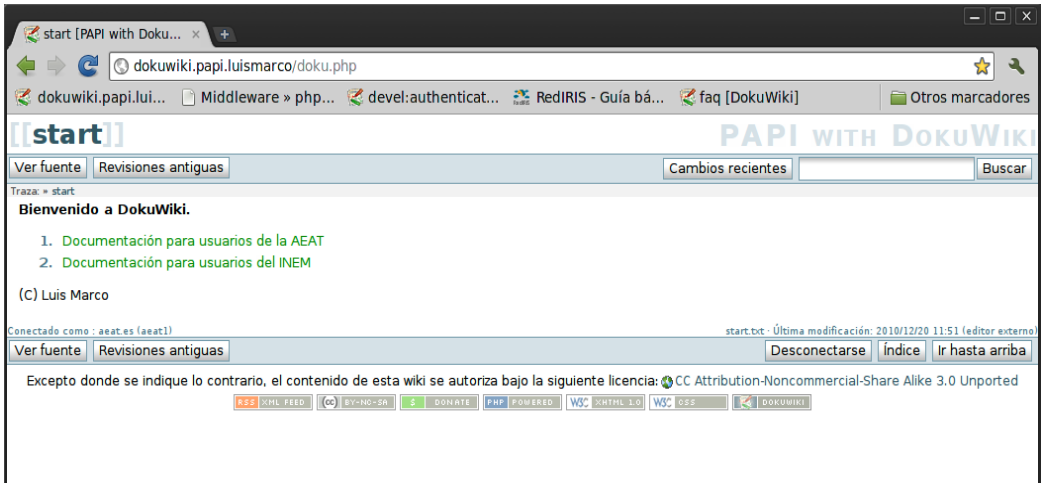

***Figura 4.3**: Acceso a DokuWiki una vez autenticado por el AS*

5. Acceso autenticado: En la figura se muestra cómo el usuario autenticado podrá acceder a los contenidos restringidos a los que está autorizado.

***Figura 4.4**: Acceso a los contenidos restringidos para el usuario autenticado*

6. Acceso no autorizado: En el caso de que el usuario no se haya acreditado correctamente ante el AS seleccionado, el PoA impedirá su acceso a los contenidos a los que no está autorizado. En el ejemplo mostrado en la siguiente figura, el usuario *aeat1* no puede acceder a los contenidos que se encuentran restringidos únicamente a los usuarios de la organización INEM.

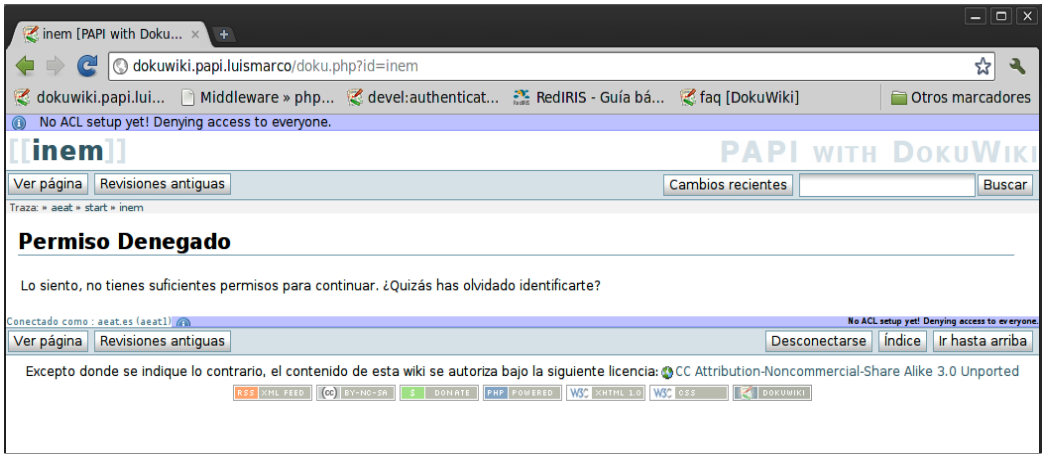

***Figura 4.5**: Denegación de acceso a usuarios sin privilegios*

5. Análisis de riesgos

Como en cualquier proyecto, incluso en aquellos de reducido tamaño, es importante realizar una prevención temprana de los riesgos con el objetivo de minimizar el impacto que estos pudieran ocasionar, y que podrían conducir al fracaso del proyecto.

Entre los riesgos que pueden aparecer durante el desarrollo del proyecto, y que deberán tratarse adecuadamente, se encuentran los siguientes:

- **Desconocimiento de los conceptos que justifican las iniciativas:** Para evitar o minimizar este riesgo será conveniente antes de emprender el proyecto, conocer con detalle el problema que se quiere abordar y las soluciones que se pretenden cubrir con el sistema a desarrollar. Será necesario conocer con detalle las posibilidades y limitaciones que ofrece la tecnología PAPI, y los beneficios que se esperan obtener con el proyecto.

- **Aumento de costes y retardos sobre el plan de implantación:** En este caso retardos en el plan no afectarán significativamente a su desarrollo al no ser un proyecto surgido sobre una necesidad específica, sino más bien sobre una contribución a la comunidad de software libre, aunque habrá que tener en cuenta que un retardo considerable en su ejecución podría ser un síntoma de una errónea estimación de su viabilidad, aspecto que en este caso debería revisarse. Por otro lado, al ser un trabajo académico no existen costes de carácter económico.

- **Discontinuidad de su desarrollo:** Uno de los problemas más frecuentes a los que se enfrenta cualquier proyecto es la discontinuidad del soporte software. En muchas ocasiones, un producto depende de otros y éstos pueden dejar de desarrollarse por motivos varios. Una alternativa para minimizar este riesgo consiste en publicar el desarrollo como software libre en alguna forja, de forma que cualquier persona pueda continuar con el desarrollo del producto aunque los desarrolladores originales lo hayan abandonado. En este caso el producto software resultante, y su documentación asociada, se publicarán en alguna de las forjas de software libre más populares.

- **Riesgos de interoperabilidad:** La disponibilidad del código fuente minimiza, si no diluye, los riesgos de no interoperabilidad, dado que su posesión permite realizar o contratar las modificaciones oportunas para conseguirla e incluso retroalimentar positivamente el producto para otros usuarios. Si alguien se encuentra con un software que presenta algún problema de interoperabilidad puede trasladar las mejoras desde otro software para soslayar el problema. Este riesgo se minimizará con la publicación del proyecto en una forja de software libre.

6. Plan de pruebas

Las pruebas que servirán para establecer si el sistema cumple con los requisitos establecidos anteriormente, se basarán en el escenario ficticio descrito en el apartado 4 y en sus casos de uso. Debido a la reducida dimensión del módulo de autenticación a desarrollar, las pruebas descritas en este apartado servirán para cubrir todos los diferentes niveles de pruebas posibles: unitarias, de integración, de sistema, de implantación y de aceptación.

Para recrear el ambiente de pruebas definido previamente, se crearán varios tipos de usuarios en DokuWiki: *aeat1, aeat2, inem1* e *inem2*, y se definirán los contenidos a los que cada uno de ellos podrá acceder en exclusividad. Para el acceso a estos contenidos se creará una página de inicio [start] desde la que se podrá acceder a dicha información mediante enlaces de hipertexto.

Para completar el escenario de pruebas se deberá configurar cada uno de los componentes PAPI a utilizar, y crear sus claves públicas y privadas mediante OpenSSL para el intercambio seguro de mensajes del protocolo PAPI.

Los requisitos necesarios para el entorno de pruebas serán:

- Sistema operativo: Aunque la elección del sistema operativo carece de importancia para el éxito de las pruebas, en este caso se realizarán con la distribución GNU/Linux Mint Debian Edition.

- Servidor web: Será necesario un servidor web con soporte PHP, mcrypt y OpenSSL. Para garantizar el correcto funcionamiento de las pruebas, se recomiendan las siguientes versiones de productos: Apache v2.2.16 (Debian) + PHP 5.3.2-2 + php5-mcrypt 2.5.8 + php-openssl 0.9.8o.

- Navegador web: No se requiere ninguno en especial. Se podrán utilizar navegadores como Mozilla Firefox, Google Chrome u otros con soporte JavaScript y cookies.

- Conexión a Internet: Sin restricciones.

- DokuWiki: En cualquiera de sus versiones con la recomendación de las más recientes, aunque las pruebas aquí descritas se han realizado con éxito con la versión 2010-11-07a.

- Componentes PAPI en PHP: Para la implementación del PoA, GPoA y los AS. En este caso se recomiendan las versiones phpPoA v2.1 para la implementación del PoA, papi-easygpoa v1.0 para el GPoA y papi-icgpoa v1.0 para los AS.

- Soporte de OpenSSL: Para la generación de las claves públicas y privadas de los componentes PAPI. Se recomienda la versión 0.9.8o de OpenSSL.

El resultado de las pruebas será evaluado en función del acceso obtenido por cada usuario a los contenidos creados en DokuWiki, de forma que el conjunto de pruebas válidas se configura como:

Usuarios	Acceso garantizado	Acceso denegado
aeat1, aeat2	Contenidos creados para los usuarios de la AEAT	Contenidos creados para los usuarios del INEM
inem1, inem2	Contenidos creados para los usuarios del INEM	Contenidos creados para los usuarios de la AEAT
Otros	A ningún contenido	A todos los contenidos

***Figura 6.1**: Conjunto de pruebas de acceso*

Además de las pruebas de autenticación descritas previamente, y de acuerdo con los casos de uso especificados en el apartado 3.2, se deberá verificar el correcto funcionamiento del sistema cuando se realice una petición al PoA y no exista un contexto de seguridad en el GPoA, es decir cuando no exista una cookie de autenticación previa porque el usuario no se haya autenticado con anterioridad o esta autenticación hubiera expirado. En este caso el GPoA deberá solicitar al usuario la selección de su proveedor de identidad (AS) donde autenticarse, es decir se deberá activar el protocolo *Where Are You From*? (WAYF).

Para realizar estas últimas pruebas se deberán verificar los siguientes escenarios y resultados:

Escenario	Condiciones		Resultado esperado
	Usuario autenticado con anterioridad	Existe contexto de seguridad (cookie)	
1	NO	N/A	WAYF
2	SÍ	SÍ	OK Usuario autenticado
3	SÍ	NO	WAYF

***Figura 6.2**: Conjunto de pruebas de autenticación*

El escenario número 3 se podrá verificar fácilmente una vez el usuario se encuentre autenticado, simulando la caducidad de la cookie de autenticación (contexto de seguridad del GPoA) al eliminar las cookies en el navegador.

7. Software a utilizar y Licencias

Además del software imprescindible para poner en funcionamiento el sistema (sistema operativo, servidor web, DokuWiki, etc.), y poder realizar las pruebas de validación y aceptación del sistema, se hará necesario contar con una serie de componentes que implementen las funciones básicas de la arquitectura PAPI. Para tal fin se utilizarán los componentes publicados por RedIRIS.

En la siguiente figura se describen los componentes PAPI disponibles en PHP y distribuidos por RedIRIS:

Componente	Versión en distribución oficial	GPoA	PoA	AS	Tecnología	Licencia
easyGPoA	1.0	X			PHP	GPL
icGPoA	1.0	X		X		
phpPoA	2.0		X			

***Figura 7.1**: Componentes PAPI disponibles en PHP*

En el ámbito de este proyecto se usarán los siguientes componentes PAPI:

- **icGPoA** para la implementación de los AS, debido a su dualidad para actuar tanto como GPoA como AS, siendo extremadamente sencillo su uso en este último caso.
- **phpPoA** para la implementación del PoA.
- **easyGPoA** como GPoA.

Todos estos componentes PAPI se distribuyen bajo licencia GPL por lo que, siguiendo la línea argumental expuesta en el apartado 1.4 acerca de la licencia, el componente de autenticación PAPI a desarrollar también se publicará bajo licencia GPL.

8. Planificación temporal

La distribución temporal del proyecto se deberá ajustar a las horas totales de dedicación incluidas en el convenio de cooperación educativa para la realización de prácticas universidad-empresa, firmadas en este caso con la empresa PriSE, y que comprenden 185 horas de dedicación en modalidad 100% virtual.

El proyecto dará comienzo en octubre de 2010, estimándose un coste temporal de cinco meses con fecha de finalización prevista para principios de marzo de 2011.

Las tareas que conducirán a la finalización del sistema final son las siguientes:

1. Estudio del protocolo de autenticación PAPI
2. Estudio del proceso de autenticación de DokuWiki
3. Análisis de viabilidad del sistema
4. Análisis del sistema de autenticación a desarrollar
5. Determinación de la licencia de publicación del módulo de autenticación PAPI y de su documentación
6. Diseño del sistema de autenticación
7. Diseño del plan de pruebas
8. Instalación y configuración de una infraestructura web con soporte para la ejecución de scripts PHP, mycrpt, y soporte OpenSSL
9. Instalación y configuración de DokuWiki
10. Generación en DokuWiki de usuarios con diferentes privilegios de acceso a los recursos alojados en el wiki
11. Desarrollo del módulo de autenticación PAPI
12. Pruebas de unidad del módulo de autenticación PAPI
13. Integración del módulo de autenticación PAPI con DokuWiki
14. Pruebas de integración del sistema completo
15. Publicación y despliegue del módulo de autenticación

Algunas de estas tareas se deberán completar secuencialmente, mientras que otras se podrán llevar a cabo de forma paralela. La planificación detallada de estas tareas se muestra en el diagrama de Gantt de la figura, y en la siguiente tabla:

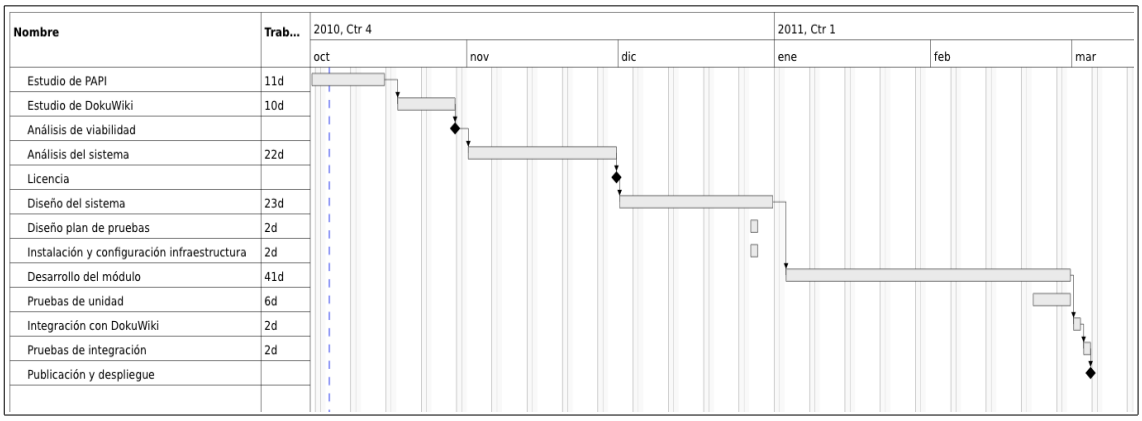

***Figura 8.1**: Planificación temporal del desarrollo del sistema*

Nombre	**Inicio**	**Fin**	**Trabajo**	**Duración**
Estudio de PAPI	oct 1	oct 15	11d	11d
Estudio de DokuWiki	oct 18	oct 29	10d	10d
Análisis de viabilidad	oct 29	oct 29	N/D	N/D
Análisis del sistema	nov 1	nov 30	22d	22d
Licencia	nov 30	nov 30	N/D	N/D
Diseño del sistema	dic 1	dic 31	23d	23d
Diseño plan de pruebas	dic 27	dic 28	2d	2d
Instalación y configuración infraestructura	dic 27	dic 28	2d	2d
Desarrollo del módulo	ene 3	feb 28	41d	41d
Pruebas de unidad	feb 21	feb 28	6d	6d
Integración con DokuWiki	mar 1	mar 2	2d	2d
Pruebas de integración	mar 3	mar 4	2d	2d
Publicación y despliegue	mar 4	mar 4	N/D	N/D

***Figura 8.2**: Planificación temporal de las tareas*

9. Presupuesto

El proyecto utilizará varias soluciones existentes en el mercado publicadas bajo licencias libres, por lo que su desarrollo no supondrá ningún coste económico en cuanto a la adquisición de licencias software o equipos hardware se refiere.

No obstante, se deben valorar los costes de propios del análisis, desarrollo, pruebas e integración del módulo de autenticación, como en cualquier proyecto de desarrollo software. En este caso, y debido a la reducida dimensión del componente de autenticación, no se hace necesario contar con más de una persona para completar todas las tareas propias de la ingeniería del software, por lo que un perfil de analista-programador es suficiente para su realización.

El precio medio/hora de un analista-programador a jornada completa (8 horas/día) se sitúa en 40€[1]. Atendiendo a la planificación temporal realizada en el apartado anterior con un total de 185 horas de trabajo, el coste económico estimado para el proyecto ascendería a 7.400€.

[1] Precio medio para 2011 obtenido mediante la consulta de presupuestos de desarrollo software realizados por empresas privadas a administraciones públicas autonómicas (Comunidad de Madrid y Generalitat de Catalunya).

10. Diseño del sistema

La arquitectura general del sistema a construir se definirá especificando los distintos subsistemas que lo componen, así como los mensajes que se intercambiarán entre ellos para realizar su cometido.

10.1. Arquitectura de PAPI

PAPI es un sistema que facilita el acceso, a través de Internet, a recursos de información que están restringidos a usuarios autorizados. Sus mecanismos de autenticación empleados para identificar a los usuarios se han diseñado para ser lo más flexibles posible, permitiendo que cada organización emplee un esquema de autenticación propio, manteniendo así los datos dentro de su propio ámbito, a la vez que los proveedores de información disponen de datos suficientes para realizar estadísticas.

La arquitectura de PAPI a nivel conceptual ya ha sido descrita en el apartado 1.2 de este documento, por lo que a continuación se detallará su arquitectura a nivel lógico, es decir definiendo las interfaces y mensajes de comunicción entre cada uno de sus componentes.

Los mecanismos de control de acceso son transparentes para el usuario y compatibles con los navegadores comúnmente empleados en cualquier sistema operativo. Dado que PAPI emplea procedimientos HTTP estándar, su uso para proveer servicios de identidad digital y control de acceso no requiere de ningún hardware o software específico, garantizando a los usuarios un acceso ubicuo a cualquier recurso de información al que tengan derecho.

Los mensajes del protocolo de PAPI se transmiten utilizando métodos GET o POST sobre HTTP mientras que, por otro lado, las respuestas serán redirecciones 302 de HTTP, incluyendo además cookies en el caso de que el usuario deba almacenar algún tipo de información útil para el protocolo.

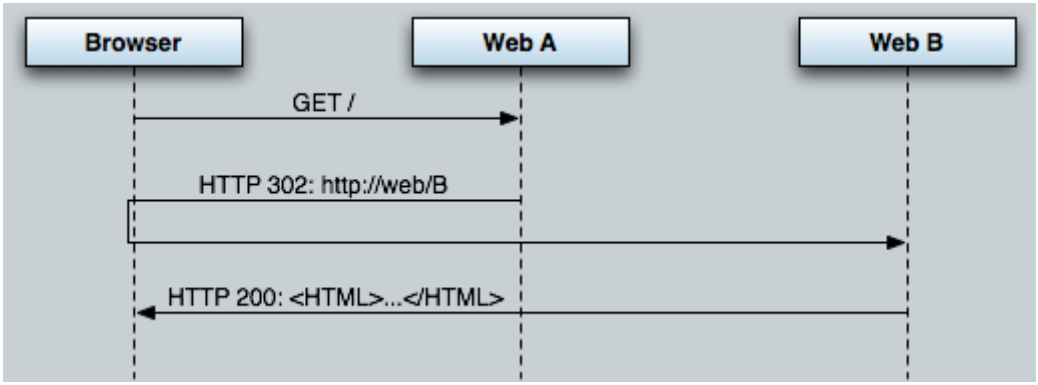

Figura 10.1: *Redirecciones HTTP 302 en mensajes PAPI*

En el siguiente diagrama podemos ver el conjunto de mensajes que definen el protocolo de PAPI:

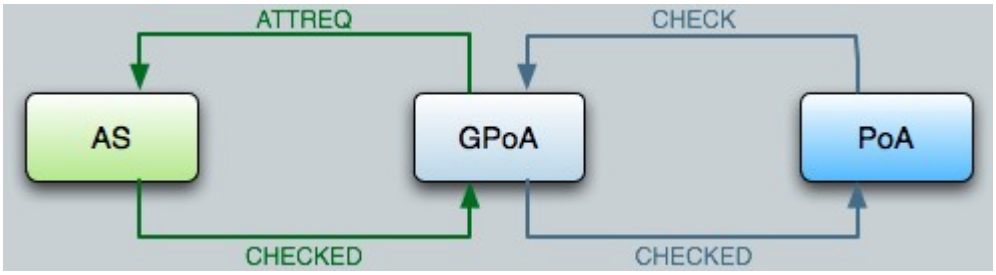

Figura 10.2: *Conjunto de mensajes del protocolo PAPI*

Todos estos mensajes no son enviados directamente entre los diferentes componentes, sino que la comunicación siempre pasa por el navegador del usuario. De esta forma, el usuario, al acceder a un componente (en el ejemplo lo llamaremos A), si éste quiere mandar un mensaje a otro componente (en el ejemplo lo llamaremos B), el navegador haría las siguientes peticiones:

- El navegador envía una petición al componente A:

```
http://web/A?arg1=X&arg2=Y
```

- El componente A devuelve la siguiente respuesta:

```
HTTP/1.1 302 Found
Date: Sun, 02 Mar 2008 10:16:02 GMT
Server: Apache/1.3.31 (Unix
Location: http://web/B?arg3=Z
Transfer-Encoding: chunked
```

- El navegador, al recibir un mensaje de respuesta 302, vuelve a enviar automáticamente una nueva petición, la indicada en la cabecera Header (Location), siendo en este caso:

```
http://web/B?arg3=Z
```

10.2. Mensajes del protocolo PAPI

1) Petición de autenticación: ATTREQ – CHECKED

Corresponde a una petición de atributos por parte de un componente PAPI, normalmente un GPoA o un PoA. En el caso de que el usuario no se hubiese autenticado previamente, realiza su autenticación de cara a obtener sus atributos.

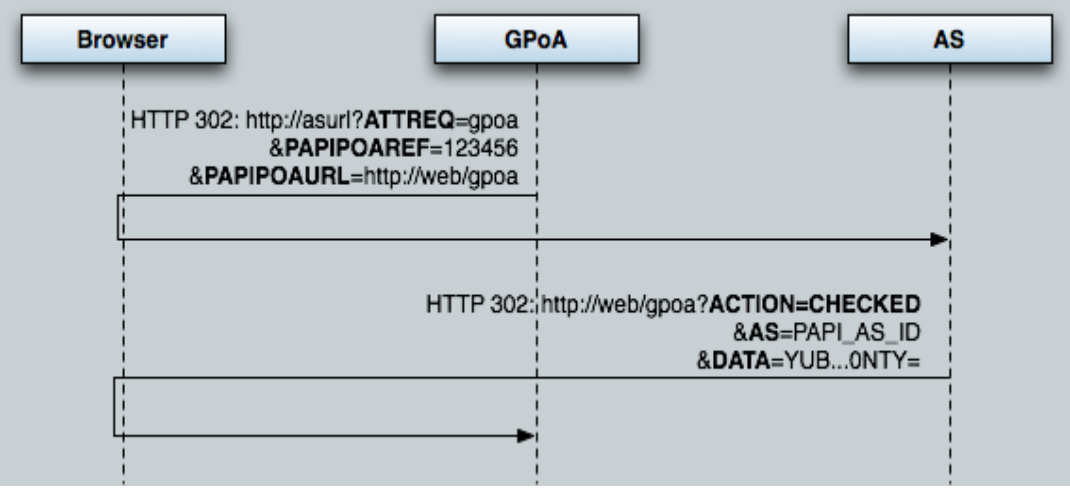

Figura 10.3: *Petición de autenticación – Mensaje ATTREQ-CHECKED*

2) Mensaje ATTREQ

El formato del mensaje es el siguiente:

```
http://asurl?ATTREQ=%PoA-Service-ID%&PAPIPOAREF=%value%
&PAPIPOAURL=%value
```

Donde,

- **ATTREQ** tendrá el valor del identificador (ID) del GPoA que ha realizado la petición.
- **PAPIPOAREF** es un valor que establece el GPoA y que le será devuelto en la respuesta.
- **PAPIPOAURL** es la URL original que ha generado la redirección al AS. Este parámetro es muy importante ya que permite al AS establecer qué aserción devolver y a qué URL debe generar la respuesta (mediante una redirección HTTP).

3) Respuesta CHECKED a un ATTREQ

Las respuestas que emite un AS a este tipo de mensaje son:

- En el caso de que el usuario se haya autenticado correctamente, se devuelve una redirección 302 de HTTP con el siguiente formato:

```
%PAPIPOAURL%?AS=%AS-ID%&ACTION=CHECKED&DATA=%value%
```

  Donde,
  - **AS** es el ID del AS que ha enviado la respuesta.
  - **ACTION** es el tipo de respuesta que envía, en este caso CHECKED.
  - **DATA** es el valor que contiene la información que requería el PoA.

- En el caso de que el usuario no se haya autenticado correctamente o hubiera ocurrido algún tipo de error, se devuelve una redirección 302 de HTTP con el mismo formato pero el campo DATA contiene un valor que informa al PoA del error. Como se observa, en el parámetro DATA de una respuesta se devuelven los atributos del usuario, también llamado como aserciones de usuario. El AS de PAPI permite que la aserción sea diferente para cada uno de los PoAs, con lo que se evita enviar más atributos y más información de la necesaria por el control de acceso en el recurso protegido. El valor de DATA se obtiene tras pasar a base 64 el valor obtenido de cifrar la siguiente cadena de texto con la clave privada RSA del AS:

```
userAssertion:expiryTime:currentTime:KEY
```

  Donde,
  - **userAssertion**: la aserción del usuario para el componente que ha enviado la petición. El formato de la aserción es la siguiente:

```
%LISTA_ATRIBUTOS%@%AS-ID%
```

  - **expiryTime**: tiempo en segundos desde el 1 de Enero de 1970 en el que la aserción deja de ser válida.
  - **currentTime**: tiempo en segundos desde el 1 de Enero de 1970 en que ha sido generada la aserción.
  - **KEY**: es el valor del parámetro PAPIPOAREF que se recibió en el mensaje ATTREQ.

En caso de que el Proveedor de Identidad o AS quiera indicar que el usuario no tiene autorización para acceder a GPoA, o para indicar que ha ocurrido algún tipo de error a la hora de su identificación, el valor de userAssertion debe ser 'ERROR'.

La lista de atributos (**%LISTA_ATRIBUTOS%**) en una aserción no tiene un formato definido aunque la información que contiene sigue la siguiente estructura:

- Nombre de atributo
  - Lista de valores del atributo

Dentro de una misma federación o Single Sign-On ha de establecerse un acuerdo sobre los separadores de cada uno de los elementos que componen la aserción. No obstante se recomienda utilizar los siguientes separadores:

- Separador de atributos: ,
- Separador atributo-valor: =
- Separador de valores en un atributo: |

De esta forma quedaría una aserción de la siguiente manera:

```
name1=valorA,name2=valorB|valorC@PAPI_AS_ID
```

4) Petición de decisión de autorización: CHECK - CHECKED

Un PoA envía un mensaje CHECK a un GPoA para comprobar si el usuario tiene **potencialmente** derechos de acceso en dicho PoA. En caso afirmativo, obtiene información de autenticación y una aserción de atributos, por lo que además puede realizar su propia política de autorización en base a ello.

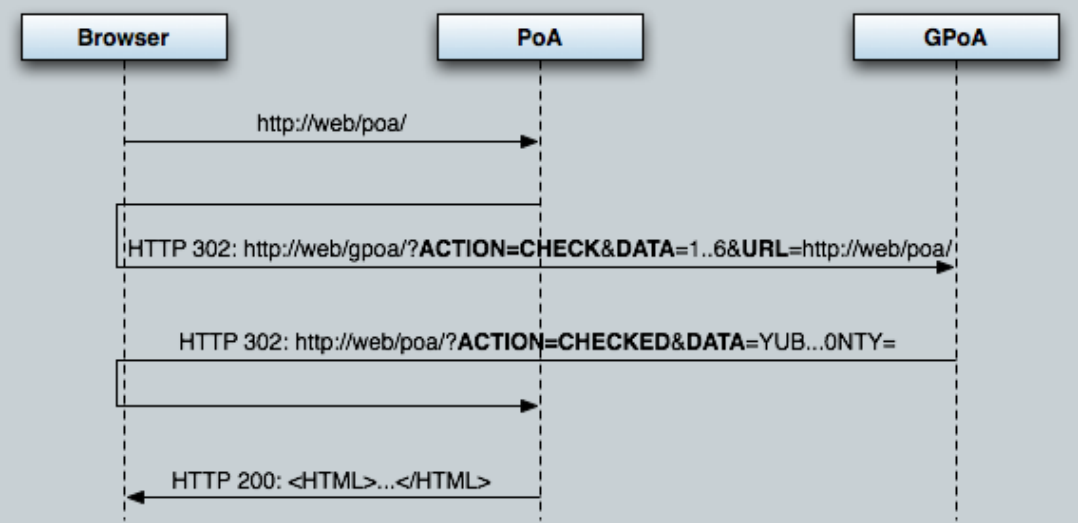

Figura 10.4: *Petición de decisión de autorización: CHECK – CHECKED*

5) Mensaje CHECK

El formato del mensaje es:

```
http://%gpoa-url%/AuthLocation?ACTION=CHECK&DATA=%value%
&URL=%PoA-url%
```

Donde,

- **gpoa-url**: es la dirección web del GPoA al que se le manda el mensaje.
- **ACTION**: es el tipo de mensaje que se envía al GPoA.
- **DATA**: es una cadena alfanumérica que debe ser devuelto en la respuesta.
- **URL**: es la dirección de respuesta a la que debe hacer la redirección 302 de HTTP en el GPoA.

6) Respuesta CHECKED a un CHECK

El GPoA envía un mensaje CHECKED como respuesta al mensaje anterior:

- En el caso de que el usuario tenga una cookie de sesión (Hcook) en el GPoA, se le envía una respuesta correcta con el siguiente formato:

  ```
  %PoA-url%?ACTION=CHECKED&DATA=%value%
  ```

  Donde,

  - **PoA-url:** es la dirección web que el PoA ha enviado en el campo URL del mensaje CHECK.
  - **ACTION**: es el tipo de respuesta que envía, en este caso CHECKED.
  - **DATA**: es el valor que contiene la información que requería el PoA. El valor de DATA se obtiene tras pasar a base 64 el valor obtenido de cifrar la siguiente cadena de texto con la clave privada RSA del GPoA:

    ```
    userAssertion:expiryTime:currentTime:KEY
    ```

    Donde,

    - **userAssertion**: la aserción del usuario para el PoA que ha enviado la petición.
    - **expiryTime**: tiempo en segundos desde el 1 de Enero de 1970 en el que la aserción deja de ser válida.
    - **currentTime**: tiempo en segundos desde el 1 de Enero de 1970 en que ha sido generada la aserción.

- **KEY**: es el valor del parámetro PAPIPOAREF que se recibió en el mensaje ATTREQ.

En caso de que el GPoA quiera indicar que el usuario no tiene autorización para acceder a dicho PoA o para indicar que ha ocurrido algún tipo de error a la hora de su identificación, el valor de userAssertion debe ser 'ERROR'.

7) Selección de Proveedor de Identidad

En el caso de que el usuario no tuviera un contexto de seguridad en el GPoA, éste debe mostrar una página web a través de la cual el usuario puede elegir en qué Proveedor de Identidad (AS) quiere autenticarse. Esta página se le conoce como *Where Are You From? (WAYF)*, y su función es redirigir al usuario a su Proveedor de Identidad a través de un mensaje ATTREQ.

Figura 10.5: *Selección de proveedor de identidad – Mensaje WAYF*

Para indicarle al GPoA cuál es el proveedor de identidad donde se ha de autenticar el usuario, se utilizará dentro del mensaje CHECK el siguiente parámetro opcional:

- **PAPIHLI**: es el identificador del AS o proveedor de identidad PAPI donde se ha de redirigir al usuario en caso de que no exista contexto de seguridad en el GPoA.

Así, cuando el GPoA no recibe este parámetro PAPIHLI en una petición, ha de mostrar la página *WAYF?,* el cual terminará repitiendo la misma petición que recibió aunque añadiéndole dicho parámetro.

10.3. Arquitectura de la autenticación proporcionada por DokuWiki

El sistema de autenticación proporcionado por DokuWiki es completamente abierto y configurable a través de diferentes módulos denominados *backends*.

En cualquier instalación de DokuWiki los *backends* se encuentran en la ruta *inc/auth* como clases independientes implementadas en PHP. La nomenclatura de estas clases sigue la sintaxis *nombre_de_clase.class.php*, de modo que ajustándose a esta sintaxis la clase que implementará la autenticación basada en PAPI se denominará ***papi.class.php***.

El *backend* que DokuWiki utilizará se deberá configurar a través de un fichero de texto plano ubicado en la ruta *conf/dokuwiki.php*, estableciendo para ello en la variable *$conf['authtype']* el nombre de la clase a utilizar. En este caso se utilizará el nombre *'papi'*, de la forma ***$conf['authtype'] = 'papi';***

En este mismo fichero se especificarán otras opciones de configuración específicas para el *backend PAPI*, como será la ruta al PoA, variables PAPI a utilizar por DokuWiki, etc. Estos parámetros de configuración se realizarán a través de variables PHP del modo ***$conf['nombre_de_clase] ['parámetro'] = 'valor_parámetro'***.

10.4. Arquitectura del módulo de autenticación

El módulo de autenticación se situará entre DokuWiki (el proveedor de información) y el punto de acceso (PoA), para controlar el acceso a los recursos almacenados en el wiki, de modo que el módulo tendrá la responsabilidad de la comunicación con el PoA, y éste a su vez con el servidor de autenticación local (AS) para identificar a los usuarios de la organización. Aunque esta arquitectura general funcionaría sin problemas, lo más habitual es encontrar soluciones en las que el PoA no se comunica directamente con el AS, sino que lo hace a través de un controlador de un grupo de puntos de acceso (GPoA) con el fin de flexibilizar la arquitectura. Este enfoque es el que se va a adoptar en este proyecto.

11. Desarrollo del sistema

11.1. Coste del desarrollo

En el apartado ocho de este documento se realizó una planificación temporal del desarrollo del sistema, estimando en ella un coste de cinco meses para completar el proyecto. Esta planificación ha sido ajustada a la realidad ya que el desarrollo real del proyecto ha tenido un coste temporal inferior a lo inicialmente previsto, pero con un coste económico equivalente al estimado debido a la redistribución de la carga de trabajo diaria, y por consiguiente de las horas trabajadas en cada jornada, siendo el cómputo de horas totales las mismas 185 horas inicialmente previstas.

En el diagrama de Gantt de la figura, así como en el cuadro de tareas realizadas, se muestra la situación real de la etapa de desarrollo del proyecto:

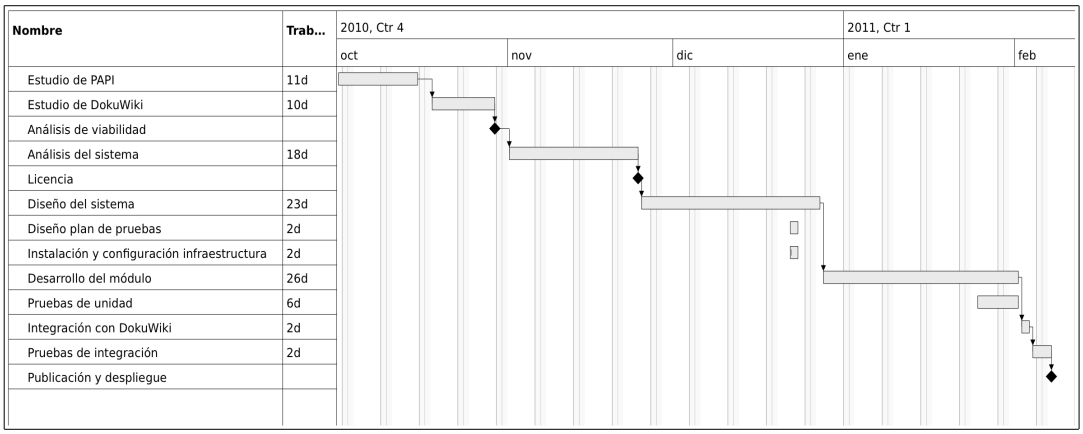

Figura 11.1: *Diagrama de Gantt del coste temporal real del proyecto*

Nombre	Inicio	Fin	Trabajo	Duración
Estudio de PAPI	oct 1	oct 15	11d	11d
Estudio de DokuWiki	oct 18	oct 29	10d	10d
Análisis de viabilidad	oct 29	oct 29	N/D	N/D
Análisis del sistema	nov 1	nov 24	18d	18d
Licencia	nov 24	nov 24	N/D	N/D
Diseño del sistema	nov 25	dic 27	23d	23d
Diseño plan de pruebas	dic 22	dic 23	2d	2d
Instalación y configuración infraestructura	dic 22	dic 23	2d	2d
Desarrollo del módulo	dic 28	feb 1	26d	26d
Pruebas de unidad	ene 25	feb 1	6d	6d
Integración con DokuWiki	feb 2	feb 3	2d	2d
Pruebas de integración	feb 4	feb 7	2d	2d
Publicación y despliegue	feb 7	feb 7	N/D	N/D

Figura 11.2: *Coste temporal real de las tareas del proyecto*

11.2. Entorno y elementos necesarios para el desarrollo

Los elementos necesarios para el desarrollo, prueba y configuración del módulo de autenticación son los siguientes:

- Servidor web con soporte PHP, mcrypt y OpenSSL, donde se alojará DokuWiki, la infraestructura PAPI, y el módulo de autenticación a desarrollar.
- OpenSSL para la creación de las parejas de claves públicas y privadas necesarias por los componentes PAPI.
- DokuWiki en cualquiera de sus últimas versiones estables.
- Editor de texto plano, preferentemente con reconocimiento de sintaxis PHP.
- Navegador web con soporte de JavaScript y cookies.

En la relación de elementos anteriores no se ha hecho mención explícita en el tipo de sistema operativo a utilizar debido a que la tecnología sobre la que se va a trabajar permite el desarrollo del módulo en cualquiera de los existentes actualmente, libre o privativo, aunque en este proyecto se utilizará una distribución GNU/Linux.

La elección del entorno y elementos necesarios para el desarrollo del módulo de autenticación PAPI ha sido, en este caso, la siguiente:

- Sistema operativo: **Linux Mint Debian Edition**
- Servidor web con soporte PHP: **Apache v2.2.16 (Debian) + PHP 5.3.2-2 + php5-mcrypt 2.5.8 + php-openssl 0.9.8o**
- **OpenSSL v0.9.8o**
- **DokuWiki v2010-11-07a**
- Editor de textos **gEdit v2.30.4**
- Navegadores **Google Chrome v7.0.517.41** y **Mozilla Firefox v3.6.8**
- Componentes de la infraestructura PAPI:
  - **phpPoA v2.1** para la implementación del PoA
  - **papi-icgpoa v1.0** para la implementación de los AS
  - **papi-easygpoa v1.0** para la implementación del GPoA

Para el desarrollo del módulo y sus consiguientes pruebas de unidad e integración se hizo necesario montar una infraestructura completa en una máquina de pruebas local, donde *convivirían* dos servidores de autenticación (AS), un GPoA, un PoA, y un proveedor de información (DokuWiki). Para simular una situación real en la que estos componentes se encontrarían en diferentes máquinas y en ubicaciones remotas, se modificó el archivo del sistema */etc/hosts* para crear diferentes nombres de dominio. En concreto:

- *gpoa.papi.foo.com* para el GPoA
- *as.papi.aeat.com* para el AS “AEAT”
- *as.papi.inem.com* para el AS “INEM”
- *poa.papi.luismarco* para el PoA
- *dokuwiki.papi.luismarco* para el proveedor de información con DokuWiki

Del mismo modo, se crearon servidores virtuales en Apache2 para las URL definidas anteriormente (fichero */etc/apache2/sites-available/default*):

```
<VirtualHost *:80>
        ServerName dokuwiki.papi.luismarco
        DocumentRoot /var/www/dokuwiki
</VirtualHost>

<VirtualHost *:80>
        ServerName poa.papi.luismarco
        DocumentRoot /var/www/papi_poa
</VirtualHost>

<VirtualHost *:80>
        ServerName gpoa.papi.foo.com
        DocumentRoot /var/www/papi_gpoa
</VirtualHost>

<VirtualHost *:80>
        ServerName as.papi.aeat.com
        DocumentRoot /var/www/papi_as_aeat
</VirtualHost>

<VirtualHost *:80>
        ServerName as.papi.inem.com
        DocumentRoot /var/www/papi_as_inem
</VirtualHost>
```

***Figura 11.3**: Servidores virtuales de Apache2*

Se crearon las parejas de claves públicas-privadas para los componentes PAPI mediante openSSL a través de comandos:

- `openssl genrsa -out mykey.pem 1024`
- `openssl rsa -in mykey.pem -pubout`

Por último se configuraron los componentes PAPI mediante sus respectivos ficheros de configuración en cuanto a rutas y claves públicas-privadas se refiere:

Componente PAPI	Ficheros de configuración
Servidores de autenticación (AS)	*index.php*
GPoA	*config.php*
PoA	*PoA.conf* *PAPI_PoA.conf*

***Figura 11.4**: Ficheros de configuración de los componentes PAPI*

Durante el desarrollo y las pruebas se detectaron dos problemas en uno de los componentes PHP de la implementación de PAPI proporcionados por RedIRIS y por la empresa PriSE.

El primero de ellos condujo a la modificación del componente **phpPoA v2.1** (módulo *papi_poa/lib/authn/PAPIAuthnEngine.php*) de la implementación de un PoA de PAPI en PHP realizada por RedIRIS, debido a que no se comportaba correctamente en conjunción con DokuWiki, principalmente debido a que las reescrituras de URL realizadas por los componentes de PAPI eran gestionadas erróneamente por DokuWiki al sustituir éste último en las direcciones los separadores de parámetros '*&*' por su carácter de referencia '*&*'. Aunque esta técnica de sustitución se usa en muchos sistemas cuando existen reescrituras de URL y sesiones PHP (se puede leer un artículo del W3C sobre este tema en la URL *http://www.w3.org/QA/2005/04/php-session*), en este caso producía que los componentes de PAPI fallaran ya que sus mecanismos de paso de parámetros buscaban el separador '*&*' para obtener los *tokens* de información intercambiados entre sus componentes. Este efecto colateral, que no es exclusivo de la integración con DokuWiki sino que se puede producir en la integración con otros productos existentes, se solucionó añadiendo al módulo **phpPoA v2.1** la siguiente instrucción:

```
    // luismarco: Replace entity char '&amp;' for a single ampersand '&'
 $l = str_replace('&amp;','&',$l);             remote user id
```

***Figura 11.5**: Modificación del PoA phpPoa v2.1*

El segundo de ellos consistió en la modificación del fichero *utils.php* de **phpPoA v2.1** debido a que éste incluía un método llamado *msg()* cuyo nombre entraba en conflicto con otro método con el mismo nombre incluido en las distribuciones de DokuWiki. Para evitar el conflicto se optó, en este caso, por renombrar el método *msg()* del PoA por *poa_msg()*, así como sus respectivas llamadas, debido a que un método con este nombre resultaba demasiado genérico para ser compatible con cualquier integración de productos.

Ambas modificaciones fueron valoradas positivamente por el tutor de prácticas de la empresa PRiSE, que a su vez procedió a enviársela al autor del módulo para que las tuviera en consideración en las siguientes versiones del módulo, y de esta forma hacerlo más robusto.

11.3. Implementación del módulo de autenticación PAPI

A continuación se muestra el código fuente de la implementación PHP de la clase ***papi.class.php***, el cual no se describe con detalle al considerarse su código auto explicativo:

```
<?php

// Include PoA
global $conf;
require($conf['papi']['path']."PoA.php");

/**
 * auth/papi.class.php
 *
 * @author    Luis Marco Gimenez <lmarcogimenez@gmail.com>
 */

class auth_papi extends auth_basic {

  /**
   * Constructor.
   */
  function auth_papi() {

    // Capabilities
    $this->cando['external'] = true;
    $this->cando['logoff'] = true;

    // Check Auth with PAPI with the selected PoA ID
    global $conf;
    global $poa;
    $poa = new PoA($conf['papi']['poa_id']);
  }

  /**
   * Implements the PAPI authentication
   */
  function trustExternal($user,$pass,$sticky=false) {
    global $USERINFO;
    global $poa;
    global $conf;

    $sticky ? $sticky = true : $sticky = false; //sanity check

    $auth = $poa->authenticate();

    if ($auth) { // The user was authenticated
      $as_id = $poa->getAttribute(PROTO_ATTR_AS_ID, NS_PAPI_PROTOCOL);
      $attrs = $poa->getAttributes();

      // Dokuwiki auth info according the parameters defined
      // in dokuwiki.php and $conf['papi] attributes

      $USERINFO[$conf['papi']['sHO']] = $attrs['sHO'];                        // name
      $USERINFO[$conf['papi']['mail']] = $attrs['mail'];                      // mail
      $USERINFO[ $conf['papi']['grp']] = array($attrs['grp']);                // groups
      $_SERVER['REMOTE_USER'] = $attrs['uid'];                                // remote user id
      $_SESSION[DOKU_COOKIE]['auth'][$conf['papi']['uid']] = $attrs['uid'];   // user id

      $_SESSION[DOKU_COOKIE]['auth']['pass'] = __;                            // not used
      $_SESSION[DOKU_COOKIE]['auth']['info'] = __;                            // not used

      return true;
    }
    else { // Error, the user wasn't authenticated
            return false;
    }

  }
```

(continuación de la clase ***papi.class.php***)

```
/**
  * Log off the current user from PAPI Auth
  */
  function logOff() {
    global $poa;

    $poa->logout();

    $USERINFO['name'] = __;
    $USERINFO['mail'] = __;
    $USERINFO['grps'] = __;
    $_SERVER['REMOTE_USER'] = __;
    $_SESSION[DOKU_COOKIE]['auth']['user'] = __;
    $_SESSION[DOKU_COOKIE]['auth']['pass'] = __;
    $_SESSION[DOKU_COOKIE]['auth']['info'] = __;
  }

}
```

***Figura 11.6**: Clase de autenticación papi.class.php*

La configuración del módulo de autenticación se realiza a través del fichero de configuración ***dokuwiki.php***, disponible en cualquier instalación de DokuWiki:

```
  /* Authentication Options - read http://www.splitbrain.org/dokuwiki/wiki:acl */
$conf['authtype']    = 'papi';           //which authentication backend should be used

// PAPI auth configuration
$conf['papi']['path'] = '/usr/share/php5/papi_poa/';       // Path must be ended with a slash
$conf['papi']['poa_id'] = 'dokuwiki';                      // PoA's ID name

$conf['papi']['sHO'] = 'name';            // PAPI attribute sHO  -> Dokuwiki's user name
$conf['papi']['mail'] = 'mail';           // PAPI attribute mail -> Dokuwiki's user mail
$conf['papi']['grp'] = 'grps';            // PAPI attribute grp  -> Dokuwiki's user groups
$conf['papi']['uid'] = 'user';            // PAPI attribute uid  -> Dokuwiki's user id and
                                          //                        remote user id
```

***Figura 11.7**: Configuración de la clase de autenticación PAPI*

El detalle de las variables de configuración definidas en este fichero es:

- **authtype**: Backend de autenticación a usar en DokuWiki. En este caso 'papi'.
- **path**: A través de esta variable se establece la ruta absoluta del PoA en el servidor web. Esta ruta debe finalizar obligatoriamente con un carácter separador de directorios.
- **poa_id**: Se define el nombre lógico del PoA ubicado en la variable *path* anterior.
- **sHO**: Asignación del atributo *sHO* del protocolo PAPI (*schacHome-Organization del usuario de la aplicación*) a la variable ***name*** (nombre de usuario) de DokuWiki. Este atributo es devuelto por el AS al que pertenece el usuario.

- **mail**: Asignación del atributo *mail* del protocolo PAPI a la variable ***mail*** (correo electrónico del usuario) de DokuWiki. A Este atributo es devuelto por el AS al que pertenece el usuario.

- **grp**: Asignación del atributo *grp* del protocolo PAPI a la variable ***grps*** (grupos de pertenencia del usuario) de DokuWiki. Este atributo es devuelto por el AS al que pertenece el usuario.

- **uid**: Asignación del atributo *uid* del protocolo PAPI a la variable ***user*** (identificador [id] del usuario) de DokuWiki. Este atributo es devuelto por el AS al que pertenece el usuario.

11.4. Resultados de las pruebas unitarias y de integración

Se ha verificado la corrección del módulo desarrollado con el conjunto de pruebas especificadas en el plan de pruebas con los resultado siguientes:

a) Pruebas de autenticación

Escenario	Condiciones		Resultado esperado	Resultado de la prueba
	Usuario autenticado con anterioridad	Existe contexto de seguridad (cookie)		
1	NO	N/A	WAYF	**Éxito**
2	SÍ	SÍ	OK Usuario autenticado	**Éxito**
3	SÍ	NO	WAYF	**Éxito**

***Figura 11.8**: Resultados de las pruebas de autenticación*

b) Pruebas de acceso a recursos

Usuarios	Acceso garantizado	Acceso denegado	Resultado de la prueba
aeat1, aeat2	Contenidos creados para los usuarios de la AEAT	Contenidos creados para los usuarios del INEM	**Éxito**
inem1, inem2	Contenidos creados para los usuarios del INEM	Contenidos creados para los usuarios de la AEAT	**Éxito**
Otros	A ningún contenido	A todos los contenidos	**Éxito**

***Figura 11.9**: Resultados de las pruebas de acceso*

A la vista de estos resultados se puede concluir que el módulo de autenticación cumple con los requisitos especificados.

12. Implantación y Mantenimiento

12.1. Implantación

1. **Elementos necesarios para la implantación**
   a) Servidor web con soporte PHP, mcrypt y OpenSSL: Cualquier servidor que disponga de soporte para PHP con los módulos criptográficos php-mcrypt y php-openssl sería válido, aunque debido a la fiabilidad que ofrece *Apache*, además de las inherentes ventajas de ser software libre y multiplataforma, se aconseja su uso en cualquier implantación.

   b) OpenSSL: Paquete de utilidades multiplataforma necesario para la creación de las parejas de claves pública-privada utilizadas por todos los componentes de la arquitectura PAPI. Se recomienda siempre la instalación de la última versión disponible, ya que con ello se garantiza la máxima fiabilidad y robustez.

   c) DokuWiki: Por fiabilidad, siempre se aconseja la descarga e instalación de cualquiera de sus últimas versiones estables.

   d) PoA PAPI PHP: Debido a que el PoA se deberá integrar con el software utilizado por el proveedor de información, en este caso con DokuWiki, y debido a que dicho wiki se encuentra implementado íntegramente en lenguaje PHP, el PoA deberá encontrarse también disponible en el mismo lenguaje. Durante el desarrollo y pruebas de este proyecto se ha utilizado el componente *phpPoA v2.1* publicado en la forja de RedIRIS, motivo por el que se recomienda su implantación, aunque se aconseja utilizar siempre la última versión disponible.

   e) GpoA PAPI: Este componente es opcional, y únicamente se deberá instalar en aquellas implantaciones en las que se desee disponer de un GPoA por razones de escalabilidad u organizativas. Se recomienda el uso de *easyGPoA v1* por haber sido probado durante el desarrollo y pruebas de este proyecto con éxito, aunque cualquier implementación de un GpoA PAPI sería válido.

   f) Módulo de autenticación PAPI para DokuWiki: Se deberá utilizar el *backend* de autenticación desarrollado en este proyecto, es decir la clase *papi.class.php*.

   g) AS PAPI: La implantación de los servidores de autenticación es responsabilidad exclusiva de las organizaciones propietarias de los usuarios. En este caso se deja a criterio de cada organización la elección del software a implantar, así como el método de autenticación a utilizar, siempre y cuando los mensajes intercambiados entre el AS y el PoA, o el GPoA en su caso, se ajusten al protocolo PAPI. Para empezar con una implantación sencilla se puede instalar el componente *icGPoA v1*, el cual puede actuar tanto como GPoA como AS.

2. Creación de las parejas de claves pública-privada para los componentes PAPI

El siguiente paso, antes de empezar con la configuración de la infraestructura PAPI, es generar las parejas de claves pública-privada que cada componente utilizará para cifrar los mensajes enviados y descifrar los recibidos.

La creación de claves se realizará de forma sencilla con el paquete OpenSSL, aunque también se podría emplear cualquier otro software que soporte la generación de claves RSA de 1024 bits o superiores. Las claves que se obtendrán vendrán en formato texto plano, codificadas en base64, de la forma:

```
-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQC5UBT2JHLadBlQEwweKAGOhNY8lj8qeE88mM2MQTkpc1ew1H4x
Ko2b9r7q69dxrkRCWYYA2jq5KiwSfRDn00NIiv/WNCzmB8izmDmlxk/Bk2seTWtA
xVF2VOHOZwzaaX/E7FwYkknQFtKq+gtKFGFmxclVrb5trrz6oFeP4aV5KQIDAQAB
AoGAUvTQjWe/qp9yfXApao6KM9yvcyvnVwHIpt3YlkLUbgPea6CUZTohboJE8TFm
ntNeZz1gSZ1n0GBanmQyXzUp1tpn4Umpvb2NBdw+56mCrh2HEFSeOVeEfacJcu28
NLqAgjc2ccX1Q8bgrKnbHfZCkxMzBG3IdiK35n0mDvhVKiECQQDl4WfskDrqRF5F
p+GrK7UrE24NRpo3qeZlIbdlfEtiq2UkiTGeVMFK8P2b4s95W9KYFr7nKkE5dVbw
4LREHp/lAkEAzl5TCqBkDtDdS6/NJHUCr2VWRaK495sOe8GbxNKXlt2eCJBrdfJJ
CB8BuZt4YI2+SqY4Cl8EK00ts8mc9cd39QJACmO/oK98Gi5w3FEUH/pfu8yrAqqY
Ob/SC+wUL+AIQDNi5N3WgkNuYQa3T55WpjOCNyGAC06bmA83mLdvLkz8CQJAHliG
c4iUTg1ujSOj0dmW9H29Su4bruVRIuecZTvmaJvcEjxSYPyoupX8pfNzpxcQxV9d
3ECOl2N49fgOqaGURQJAJnSDN0k80RBFHS20norAhk2NMW+JsJwzR6Iipl4oY21+
R1iEzmyxvKZ9IEpV4KPk2WN6b7hWgiFfTuuey8524A==
-----END RSA PRIVATE KEY-----


-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5UBT2JHLadBlQEwweKAGOhNY8
lj8qeE88mM2MQTkpc1ew1H4xKo2b9r7q69dxrkRCWYYA2jq5KiwSfRDn00NIiv/W
NCzmB8izmDmlxk/Bk2seTWtAxVF2VOHOZwzaaX/E7FwYkknQFtKq+gtKFGFmxclV
rb5trrz6oFeP4aV5KQIDAQAB
-----END PUBLIC KEY-----
```

***Figura 12.1**: Ejemplo de clave RSA*

3. Configuración de los componentes PAPI

a) Configuración del PoA phpPoA:

La configuración y parametrización de este componente se realiza a través de dos ficheros: *PoA.conf* y *PAPI_PoA.conf*.

En el primero de ellos se configuran aspectos del propio PoA, tales como el fichero donde se almacenarán los *logs* del componente, opciones de depuración, idioma, nombre lógico del PoA, el motor de autenticación a usar, y la ubicación del fichero de configuración de dicho motor de autenticación: en este caso el fichero *PAPI_PoA.conf*. Esta configuración se realiza a través de un array PHP denominado *poa_cfg*.

La configuración del fichero *PAPI_PoA.conf* se realiza a través de otro array PHP denominado *papi_cfg*. En esta variable se parametrizan aspectos de seguridad como el tiempo de validez (*timeout*) de la cookie de autenticación, la clave privada para cifrar dicha cookie, o el fichero donde se almacena la clave pública del GPoA o del AS a utilizar, así como otros parámetros acerca del protocolo de autenticación PAPI, como son el tipo de recurso donde se deberá redirigir las peticiones

para solicitar la autenticación de los usuarios (GPoA o AS), la URL del GPoA o AS, o la URL donde se gestionará el *logout* del usuario.

b) Configuración del GPoA easyGPoA:
El software *easyGPoA* requiere un servidor web con intérprete de PHP que disponga de los siguientes módulos:

- Módulo mcrypt
- Módulo OpenSSL

Para instalar *easyGPoA* tan sólo hay que descomprimir el paquete descargado bajo un directorio del servidor web.

Una vez descomprimido nos encontramos con los siguientes ficheros y directorios:

- *index.php*: es el fichero que inicializa toda la lógica del GPoA y define la URL del GPoA que deberán incluir los PoA.
- *config.php*: es el archivo de configuración del GpoA.
- *wayf/*: este directorio contiene la página *Where Are You From? (WAYF)* o selector de proveedor de identidad del GpoA.
- *PAPI/*: este directorio contiene la librería PHP necesaria para funcionar.

La configuración del módulo se realiza a través del archivo *config.php* mediante variables y arrays PHP, donde:

```
'ID_GPOA' => "test_gpoa",
```

ID_GPOA: Es el identificador (ID) del componente dentro de una infraestructura basada en PAPI.

```
'PRIVATE_KEY_GPOA' => array( 'loader_mode' => 'file',
   'loader_value' => '/usr/share/papi/easygpoa/private.pem',
),
```

PRIVATE_KEY_GPOA: Es la clave RSA privada del GPoA, donde:

- *loader_mode* es 'file' si se le indica el valor a través de un fichero o 'text' si ponemos el valor directamente de dicha clave privada.
- *loader_value* es el valor de la clave privada en función de si el elemento anterior es 'file' o 'text'.

```
'PUBLIC_KEY_GPOA' => array( 'loader_mode' => 'text',
'loader_value' =>
'-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCoxwuS1HBd7wDWfTRIOpYD8ItX
YibnXJxU1M2i+xUTpW49LsCg0X+Cju2hpc1SWc1nO+4whnOMDxUUCZNLfAIuwmmR
Aw6FQ3ZkOrLGcjIssSU4UMfaxRUafEqJplrlH8NClY53C2bGOyvoXHBWlRqRS1kZ
HcnxmBG6P4EhrPR8DwIDAQAB
-----END PUBLIC KEY-----',
),
```

PUBLIC_KEY_GPOA: Es la clave RSA pública del GPoA, donde las claves *loader_mode* y *loader_value* tienen el mismo significado que en el caso anterior.

```
'FILTER_ATTRS' => array(
  array('reg_exp' => 'http:\/\/www.domain1.com\/PoA1\/poa.php.*',
        'attrs' => array('sHO','uid')),
  array('reg_exp' => 'http:\/\/www.domain1.com\/PoA2\/poa.php.*',
        'attrs' => array('sHO','uid','mail')),
 ),
```

FILTER_ATTRS: Esta directiva permite filtrar qué atributos enviar a los PoA. Se define como un conjunto de arrays de la siguiente forma:

- *reg_exp* es la expresión regular sobre la que comprobar si coincide con la URL del PoA que envió el mensaje a este componente.

- *attrs* es un array con la lista de atributos PAPI que se le enviará al PoA en la respuesta, en el caso de que el proveedor de identidad los haya emitido para el usuario.

```
  'LIST_AS' => array(
     'TEMPsirAS' => array (
         'pubkey' =>
            '-----BEGIN PUBLIC KEY-----
             ...
             -----END PUBLIC KEY-----',
         'name' => 'icGPoA en Dominio 1',
         'url' => 'http://www.domain1.com/icgpoa/icgpoa.php',
     ),

     'TEMPsirAS2' => array (
         'pubkey' =>
            '-----BEGIN PUBLIC KEY-----
             ...
             -----END PUBLIC KEY-----',
         'name' => 'icGPoA en Dominio 2',
         'url' => 'http://www.domain1.com/icgpoa/icgpoa.php',
     ),
  ),
```

LIST_AS: Indica qué proveedores de identidad están disponibles en el GPoA, siendo la clave del elemento dentro del array el identificador del proveedor de identidad. Cada uno de ellos está definido como un array con la siguiente información:

- *pubkey* es la clave pública del proveedor de identidad.
- *name* es el nombre del proveedor de identidad.
- *url* es la dirección donde se encuentra dicho proveedor de identidad.

c) Configuración del backend de autenticación PAPI para DokuWiki:
La configuración del módulo de autenticación PAPI para DokuWiki *papi.class.php*, se realizará a través del fichero de configuración del wiki *dokuwiki.php,* tal y como se describió en el apartado 11.3 de este documento.

4. Verificación y adaptación, en su caso, del PoA phpPoA
Como se ha detallado en el apartado 12.2, el PoA *phpPoA v2.1* presenta dos problemas de compatibilidad con DokuWiki: la gestión de los separadores de variables *ampersand* '&' en las URL, y el conflicto de su función *msg()* para la escritura de mensajes de la propia aplicación, por lo que cualquier implantación que desee adoptar el componente *phpPoA* deberá verificar que la última versión disponible corrige dichos problemas, o en caso contrario proceder a su adaptación para hacerlo compatible y funcional con DokuWiki.

12.2. Mantenimiento

El mantenimiento del módulo se podrá realizar publicándolo en una forja pública de software libre, como puede ser la forja de conocimiento libre de la comunidad de RedIRIS [14] donde actualmente se alojan varios proyectos relacionados con PAPI, con los objetivos de difundir el módulo, facilitar la cooperación activa entre desarrolladores de software interesados en el proyecto, realizar correcciones de errores, actualizaciones, y prestar soporte a sus usuarios.

13. Conclusiones

Uno de los grandes beneficios que aporta el módulo de autenticación PAPI es el permitir abstraerse de la complejidad que puede suponer la comprensión de los protocolos de autenticación y autorización a recursos mediante PAPI y DokuWiki, de forma que cualquier implementación que desee integrar este módulo en un sistema con DokuWiki, simplemente tendrá que, además de disponer de todos los elementos necesarios, parametrizar los ficheros de configuración necesarios para que el sistema funcione con PAPI. Es decir, con este desarrollo se persigue un doble objetivo: por un lado la divulgación del gran potencial que esta tecnología abierta brinda, y por otro el facilitar su adopción en un wiki de uso tan general como es DokuWiki, abriendo incluso la puerta a posibles adopciones de PAPI en otros wikis, gestores de contenidos, etc.

Adicionalmente, como todos los componentes utilizados además de poseer licencias libres o ser estándares abiertos se encuentran desarrollados en lenguaje PHP, cualquier implantación podrá independizarse de la plataforma final sobre la que se va a instalar, existiendo incluso la posibilidad de ser ejecutado en entornos heterogéneos, es decir, se podría tener DokuWiki en un sistema GNU/Linux, mientras que los servidores de autenticación, por ejemplo, podrían encontrarse implementados en otros sistemas operativos.

En lo relativo al desarrollo del módulo de autenticación PAPI, aunque se podría considerar como un proyecto de reducidas dimensiones comparado con otros tipos de desarrollo, las tareas de análisis y diseño previas han tenido un peso considerable debido a que la infraestructura PAPI, así como los mecanismos de autenticación de DokuWiki, aunque bien documentados, han supuesto un reto personal en cuanto a la comprensión de su funcionamiento e interacción entre sus distintos componentes. No obstante considero que este esfuerzo puede ser gratamente compensado, principalmente porque que el resultado final se ha materializado en la entrega de un módulo que no existía en el mercado (y que incluso podría cubrir una necesidad), bajo una licencia libre que permitirá su uso, estudio, adaptación, y distribución sin ningún tipo de restricción, a excepción del mantenimiento de la licencia en caso de redistribución.

No obstante, uno de los principales problemas de cualquier proyecto de software libre es su posterior mantenimiento. Es frecuente ver proyectos que una vez desarrollados se abandonan en forjas o repositorios de software donde nadie les presta atención ni los mantiene. Para evitar este riesgo, y con el objetivo de que el módulo de autenticación pueda ser usado, mantenido, y en consecuencia evolucionar a lo largo del tiempo, se considera oportuno realizar su publicación en una forja de software libre. En este caso el producto software resultante y su documentación asociada, se publicarán en la forja de conocimiento libre de la comunidad de RedIRIS donde actualmente se alojan varios proyectos relacionados con PAPI.

Por último, siempre que se desarrolla un nuevo sistema se hace con las expectativas de que éste pueda ser utilizado en entornos de producción, y este proyecto, aunque se trate de un trabajo académico, no es una excepción. El módulo de autenticación PAPI para DokuWiki es susceptible de implantación en un amplio abanico de escenarios donde exista un proveedor de información que desee prestar servicio a usuarios geográficamente dispersos, y cuya autenticación de estos usuarios sea responsabilidad única de las organizaciones a las que pertenecen. Como ejemplo de escenario de este tipo podría citarse un sistema bibliotecario de un campus universitario en el que sus usuarios acceden remotamente a los recursos de la biblioteca y se autentican en los servidores departamentales a los que pertenecen, o

incluso en un ámbito mayor mediante el acceso a bibliotecas interuniversitarias. Otros ejemplos de implantación podrían ser la consulta de historiales médicos entre hospitales de la Seguridad Social por médicos de diferentes hospitales, el acceso a información compartida entre administraciones públicas, o la consulta de publicaciones electrónicas mediante sistemas de suscripción. Como se puede observar, existe un amplio elenco de posibilidades donde este módulo podría resultar de utilidad.

De cualquier modo, antes de abordar una implantación del módulo se hará necesario revisar las versiones de los componentes que intervienen en su funcionamiento y que se desean integrar, como son los distintos componentes de la infraestructura PAPI o el propio DokuWiki, y verificar que los problemas de interoperabilidad encontrados durante el desarrollo del proyecto y enumerados en el apartado 11.2 de esta memoria, han sido resueltos, o en caso contrario se deberían adaptar para asegurar el correcto funcionamiento del módulo.

14. Anexos

14.1. Licencia GNU GPL

LICENCIA PÚBLICA GENERAL GNU
Versión 3, 29 de junio de 2007

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps:
(1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so.

This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the
public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If

the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free
programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require,
such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your
rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those

works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works
for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code;
keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no

permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not
used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the
Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately

under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains
a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a

lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would

receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

```
<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year>  <name of author>

This program is free software: you can redistribute it and/or modify it
under the terms of the GNU General Public License as published by the
```

```
Free Software Foundation, either version 3 of the License, or (at your
option) any later version.

This program is distributed in the hope that it will be useful, but
WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the GNU
General Public License for more details.

You should have received a copy of the GNU General Public License along
with this program.  If not, see <http://www.gnu.org/licenses/>.
```

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

```
<program>  Copyright (C) <year>  <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show
w'.

This is free software, and you are welcome to redistribute it  under
certain conditions; type `show c' for details.
```

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school, if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see <http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read:
<http://www.gnu.org/philosophy/why-not-lgpl.html>.

14.2. Licencia Creative Commons BY-SA

LA OBRA O LA PRESTACIÓN (SEGÚN SE DEFINEN MÁS ADELANTE) SE PROPORCIONA BAJO LOS TÉRMINOS DE ESTA LICENCIA PÚBLICA DE CREATIVE COMMONS (CCPL O LICENCIA). LA OBRA O LA PRESTACIÓN SE ENCUENTRA PROTEGIDA POR LA LEY ESPAÑOLA DE PROPIEDAD INTELECTUAL Y/O CUALESQUIERA OTRAS NORMAS QUE RESULTEN DE APLICACIÓN. QUEDA PROHIBIDO CUALQUIER USO DE LA OBRA O PRESTACIÓN DIFERENTE A LO AUTORIZADO BAJO ESTA LICENCIA O LO DISPUESTO EN LA LEY DE PROPIEDAD INTELECTUAL.

MEDIANTE EL EJERCICIO DE CUALQUIER DERECHO SOBRE LA OBRA O LA PRESTACIÓN, USTED ACEPTA Y CONSIENTE LAS LIMITACIONES Y OBLIGACIONES DE ESTA LICENCIA, SIN PERJUICIO DE LA NECESIDAD DE CONSENTIMIENTO EXPRESO EN CASO DE VIOLACIÓN PREVIA DE LOS TÉRMINOS DE LA MISMA. EL LICENCIADOR LE CONCEDE LOS DERECHOS CONTENIDOS EN ESTA LICENCIA, SIEMPRE QUE USTED ACEPTE LOS PRESENTES TÉRMINOS Y CONDICIONES.

1. Definiciones

a. La obra es la creación literaria, artística o científica ofrecida bajo los términos de esta licencia.
b. En esta licencia se considera una prestación cualquier interpretación, ejecución, fonograma, grabación audiovisual, emisión o transmisión, mera fotografía u otros objetos protegidos por la legislación de propiedad intelectual vigente aplicable.
c. La aplicación de esta licencia a una colección (definida más adelante) afectará únicamente a su estructura en cuanto forma de expresión de la selección o disposición de sus contenidos, no siendo extensiva a éstos. En este caso la colección tendrá la consideración de obra a efectos de esta licencia.
d. El titular originario es:
    i. En el caso de una obra literaria, artística o científica, la persona natural o grupo de personas que creó la obra.
    ii. En el caso de una obra colectiva, la persona que la edite y divulgue bajo su nombre, salvo pacto contrario.
    iii. En el caso de una interpretación o ejecución, el actor, cantante, músico, o cualquier otra persona que represente, cante, lea, recite, interprete o ejecute en cualquier forma una obra.
    iv. En el caso de un fonograma, el productor fonográfico, es decir, la persona natural o jurídica bajo cuya iniciativa y responsabilidad se realiza por primera vez una fijación exclusivamente sonora de la ejecución de una obra o de otros sonidos.
    v. En el caso de una grabación audiovisual, el productor de la grabación, es decir, la persona natural o jurídica que tenga la iniciativa y asuma la responsabilidad de las fijaciones de un plano o secuencia de imágenes, con o sin sonido.

vi. En el caso de una emisión o una transmisión, la entidad de radiodifusión.

vii. En el caso de una mera fotografía, aquella persona que la haya realizado.

viii. En el caso de otros objetos protegidos por la legislación de propiedad intelectual vigente, la persona que ésta señale.

e. Se considerarán obras derivadas aquellas obras creadas a partir de la licenciada, como por ejemplo: las traducciones y adaptaciones; las revisiones, actualizaciones y anotaciones; los compendios, resúmenes y extractos; los arreglos musicales y, en general, cualesquiera transformaciones de una obra literaria, artística o científica. Para evitar la duda, si la obra consiste en una composición musical o grabación de sonidos, la sincronización temporal de la obra con una imagen en movimiento (synching) será considerada como una obra derivada a efectos de esta licencia.

f. Tendrán la consideración de colecciones la recopilación de obras ajenas, de datos o de otros elementos independientes como las antologías y las bases de datos que por la selección o disposición de sus contenidos constituyan creaciones intelectuales. La mera incorporación de una obra en una colección no dará lugar a una derivada a efectos de esta licencia.

g. El licenciador es la persona o la entidad que ofrece la obra o prestación bajo los términos de esta licencia y le concede los derechos de explotación de la misma conforme a lo dispuesto en ella.

h. Usted es la persona o la entidad que ejercita los derechos concedidos mediante esta licencia y que no ha violado previamente los términos de la misma con respecto a la obra o la prestación, o que ha recibido el permiso expreso del licenciador de ejercitar los derechos concedidos mediante esta licencia a pesar de una violación anterior.

i. La transformación de una obra comprende su traducción, adaptación y cualquier otra modificación en su forma de la que se derive una obra diferente. La creación resultante de la transformación de una obra tendrá la consideración de obra derivada.

j. Se entiende por reproducción la fijación directa o indirecta, provisional o permanente, por cualquier medio y en cualquier forma, de toda la obra o la prestación o de parte de ella, que permita su comunicación o la obtención de copias.

k. Se entiende por distribución la puesta a disposición del público del original o de las copias de la obra o la prestación, en un soporte tangible, mediante su venta, alquiler, préstamo o de cualquier otra forma.

l. Se entiende por comunicación pública todo acto por el cual una pluralidad de personas, que no pertenezcan al ámbito doméstico de quien la lleva a cabo, pueda tener acceso a la obra o la prestación sin previa distribución de ejemplares a cada una de ellas. Se considera comunicación pública la puesta a disposición del público de obras o prestaciones por procedimientos alámbricos o inalámbricos, de tal forma que cualquier persona pueda acceder a ellas desde el lugar y en el momento que elija.

m. La explotación de la obra o la prestación comprende la reproducción, la distribución, la comunicación pública y, en su caso, la transformación.

n. Los elementos de la licencia son las características principales de la licencia según la selección efectuada por el licenciador e indicadas en el título de esta licencia: Reconocimiento, CompartirIgual.

o. Una licencia equivalente es:

    i. Una versión posterior de esta licencia de Creative Commons con los mismos elementos de licencia.

    ii. La misma versión o una versión posterior de esta licencia de cualquier otra jurisdicción reconocida por Creative Commons con los mismos elementos de la licencia (ejemplo: Reconocimiento-CompartirIgual 3.0 Japón).

    iii. La misma versión o una versión posterior de la licencia de Creative Commons no adaptada a ninguna jurisdicción (Unported) con los mismos elementos de la licencia.

    iv. Una de las licencias compatibles que aparece en http://creativecommons.org/compatiblelicenses y que ha sido aprobada por Creative Commons como esencialmente equivalente a esta licencia porque, como mínimo:

        a. Contiene términos con el mismo propósito, el mismo significado y el mismo efecto que los elementos de esta licencia.

        b. Permite explícitamente que las obras derivadas de obras sujetas a ella puedan ser distribuidas mediante esta licencia, la licencia de Creative Commons no adaptada a ninguna jurisdicción (Unported) o una licencia de cualquier otra jurisdicción reconocida por Creative Commons, con sus mismos elementos de licencia.

2. Límites de los derechos.

Nada en esta licencia pretende reducir o restringir cualesquiera límites legales de los derechos exclusivos del titular de los derechos de propiedad intelectual de acuerdo con la Ley de propiedad intelectual o cualesquiera otras leyes aplicables, ya sean derivados de usos legítimos, tales como la copia privada o la cita, u otras limitaciones como la resultante de la primera venta de ejemplares (agotamiento).

3. Concesión de licencia.

Conforme a los términos y a las condiciones de esta licencia, el licenciador concede, por el plazo de protección de los derechos de propiedad intelectual y a título gratuito, una licencia de ámbito mundial no exclusiva que incluye los derechos siguientes:

a. Derecho de reproducción, distribución y comunicación pública de la obra o la prestación.

b. Derecho a incorporar la obra o la prestación en una o más colecciones.

c. Derecho de reproducción, distribución y comunicación pública de la obra o la prestación lícitamente incorporada en una colección.

d. Derecho de transformación de la obra para crear una obra derivada siempre y cuando se incluya en ésta una indicación de la transformación o modificación efectuada.

e. Derecho de reproducción, distribución y comunicación pública de obras derivadas creadas a partir de la obra licenciada.

f. Derecho a extraer y reutilizar la obra o la prestación de una base de datos.

g. Para evitar cualquier duda, el titular originario:

    i. Conserva el derecho a percibir las remuneraciones o compensaciones previstas por actos de explotación de la obra o prestación, calificadas por la ley como irrenunciables e inalienables y sujetas a gestión colectiva obligatoria.

    ii. Renuncia al derecho exclusivo a percibir, tanto individualmente como mediante una entidad de gestión colectiva de derechos, cualquier remuneración derivada de actos de explotación de la obra o prestación que usted realice.

Estos derechos se pueden ejercitar en todos los medios y formatos, tangibles o intangibles, conocidos en el momento de la concesión de esta licencia. Los derechos mencionados incluyen el derecho a efectuar las modificaciones que sean precisas técnicamente para el ejercicio de los derechos en otros medios y formatos. Todos los derechos no concedidos expresamente por el licenciador quedan reservados, incluyendo, a título enunciativo pero no limitativo, los derechos morales irrenunciables reconocidos por la ley aplicable. En la medida en que el licenciador ostente derechos exclusivos previstos por la ley nacional vigente que implementa la directiva europea en materia de derecho *sui generis* sobre bases de datos, renuncia expresamente a dichos derechos exclusivos.

4. Restricciones.

La concesión de derechos que supone esta licencia se encuentra sujeta y limitada a las restricciones siguientes:

a. Usted puede reproducir, distribuir o comunicar públicamente la obra o prestación solamente bajo los términos de esta licencia y debe incluir una copia de la misma, o su Identificador Uniforme de Recurso (URI). Usted no puede ofrecer o imponer ninguna condición sobre la obra o prestación que altere o restrinja los términos de esta licencia o el ejercicio de sus derechos por parte de los concesionarios de la misma. Usted no puede sublicenciar la obra o prestación. Usted debe mantener intactos todos los avisos que se refieran a esta licencia y a la ausencia de garantías. Usted no puede reproducir, distribuir o comunicar públicamente la obra o prestación con medidas tecnológicas que controlen el acceso o el uso de una manera contraria a los términos de esta licencia. Esta sección 4.a también afecta a la obra o prestación incorporada en una colección, pero ello no implica que ésta en su conjunto quede automáticamente o deba quedar sujeta a los términos de la misma. En el caso que le sea requerido, previa comunicación del licenciador, si usted incorpora la obra en una colección y/o crea una

obra derivada, deberá quitar cualquier crédito requerido en el apartado 4.c, en la medida de lo posible.

b. Usted puede distribuir o comunicar públicamente una obra derivada en el sentido de esta licencia solamente bajo los términos de la misma u otra licencia equivalente. Si usted utiliza esta misma licencia debe incluir una copia o bien su URI, con cada obra derivada que usted distribuya o comunique públicamente. Usted no puede ofrecer o imponer ningún término respecto a la obra derivada que altere o restrinja los términos de esta licencia o el ejercicio de sus derechos por parte de los concesionarios de la misma. Usted debe mantener intactos todos los avisos que se refieran a esta licencia y a la ausencia de garantías cuando distribuya o comunique públicamente la obra derivada. Usted no puede ofrecer o imponer ningún término respecto de las obras derivadas o sus transformaciones que alteren o restrinjan los términos de esta licencia o el ejercicio de sus derechos por parte de los concesionarios de la misma. Usted no puede reproducir, distribuir o comunicar públicamente la obra derivada con medidas tecnológicas que controlen el acceso o uso de la obra de una manera contraria a los términos de esta licencia. Si utiliza una licencia equivalente debe cumplir con los requisitos que ésta establezca cuando distribuya o comunique públicamente la obra derivada. Todas estas condiciones se aplican a una obra derivada en tanto que incorporada a una colección, pero no implica que ésta tenga que estar sujeta a los términos de esta licencia.

c. Si usted reproduce, distribuye o comunica públicamente la obra o la prestación, una colección que la incorpore o cualquier obra derivada, debe mantener intactos todos los avisos sobre la propiedad intelectual e indicar, de manera razonable conforme al medio o a los medios que usted esté utilizando:

    i. El nombre del autor original, o el seudónimo si es el caso, así como el del titular originario, si le es facilitado.

    ii. El nombre de aquellas partes (por ejemplo: institución, publicación, revista) que el titular originario y/o el licenciador designen para ser reconocidos en el aviso legal, las condiciones de uso, o de cualquier otra manera razonable.

    iii. El título de la obra o la prestación si le es facilitado.

    iv. El URI, si existe, que el licenciador especifique para ser vinculado a la obra o la prestación, a menos que tal URI no se refiera al aviso legal o a la información sobre la licencia de la obra o la prestación.

    v. En el caso de una obra derivada, un aviso que identifique la transformación de la obra en la obra derivada (p. ej., "traducción castellana de la obra de Autor Original," o "guión basado en obra original de Autor Original").

    Este reconocimiento debe hacerse de manera razonable. En el caso de una obra derivada o incorporación en una colección estos créditos deberán aparecer como mínimo en el mismo lugar donde se hallen los correspondientes a otros autores o titulares y de forma comparable a los mismos. Para evitar la duda, los créditos requeridos en esta sección sólo serán utilizados a efectos de atribución de la obra o la prestación en la manera especificada anteriormente. Sin un permiso previo por

escrito, usted no puede afirmar ni dar a entender implícitamente ni explícitamente ninguna conexión, patrocinio o aprobación por parte del titular originario, el licenciador y/o las partes reconocidas hacia usted o hacia el uso que hace de la obra o la prestación.

d. Para evitar cualquier duda, debe hacerse notar que las restricciones anteriores (párrafos 4.a, 4.b y 4.c) no son de aplicación a aquellas partes de la obra o la prestación objeto de esta licencia que únicamente puedan ser protegidas mediante el derecho *sui generis* sobre bases de datos recogido por la ley nacional vigente implementando la directiva europea de bases de datos.

5. Exoneración de responsabilidad

A MENOS QUE SE ACUERDE MUTUAMENTE ENTRE LAS PARTES, EL LICENCIADOR OFRECE LA OBRA O LA PRESTACIÓN TAL CUAL (ON AN "AS-IS" BASIS) Y NO CONFIERE NINGUNA GARANTÍA DE CUALQUIER TIPO RESPECTO DE LA OBRA O LA PRESTACIÓN O DE LA PRESENCIA O AUSENCIA DE ERRORES QUE PUEDAN O NO SER DESCUBIERTOS. ALGUNAS JURISDICCIONES NO PERMITEN LA EXCLUSIÓN DE TALES GARANTÍAS, POR LO QUE TAL EXCLUSIÓN PUEDE NO SER DE APLICACIÓN A USTED.

6. Limitación de responsabilidad.

SALVO QUE LO DISPONGA EXPRESA E IMPERATIVAMENTE LA LEY APLICABLE, EN NINGÚN CASO EL LICENCIADOR SERÁ RESPONSABLE ANTE USTED POR CUALESQUIERA DAÑOS RESULTANTES, GENERALES O ESPECIALES (INCLUIDO EL DAÑO EMERGENTE Y EL LUCRO CESANTE), FORTUITOS O CAUSALES, DIRECTOS O INDIRECTOS, PRODUCIDOS EN CONEXIÓN CON ESTA LICENCIA O EL USO DE LA OBRA O LA PRESTACIÓN, INCLUSO SI EL LICENCIADOR HUBIERA SIDO INFORMADO DE LA POSIBILIDAD DE TALES DAÑOS.

7. Finalización de la licencia

a. Esta licencia y la concesión de los derechos que contiene terminarán automáticamente en caso de cualquier incumplimiento de los términos de la misma. Las personas o entidades que hayan recibido de usted obras derivadas o colecciones bajo esta licencia, sin embargo, no verán sus licencias finalizadas, siempre que tales personas o entidades se mantengan en el cumplimiento íntegro de esta licencia. Las secciones 1, 2, 5, 6, 7 y 8 permanecerán vigentes pese a cualquier finalización de esta licencia.

b. Conforme a las condiciones y términos anteriores, la concesión de derechos de esta licencia es vigente por todo el plazo de protección de los derechos de propiedad intelectual según la ley aplicable. A pesar de lo anterior, el licenciador se reserva el derecho a divulgar o publicar la obra o la prestación en condiciones distintas a las presentes, o de retirar la obra o la prestación en cualquier momento. No obstante, ello no supondrá dar por concluida esta licencia (o cualquier otra licencia que haya sido concedida, o sea necesario ser concedida, bajo los términos de esta licencia), que continuará vigente y con efectos completos a no

ser que haya finalizado conforme a lo establecido anteriormente, sin perjuicio del derecho moral de arrepentimiento en los términos reconocidos por la ley de propiedad intelectual aplicable.

8. Miscelánea

a. Cada vez que usted realice cualquier tipo de explotación de la obra o la prestación, o de una colección que la incorpore, el licenciador ofrece a los terceros y sucesivos licenciatarios la concesión de derechos sobre la obra o la prestación en las mismas condiciones y términos que la licencia concedida a usted.

b. Cada vez que usted realice cualquier tipo de explotación de una obra derivada, el licenciador ofrece a los terceros y sucesivos licenciatarios la concesión de derechos sobre la obra objeto de esta licencia en las mismas condiciones y términos que la licencia concedida a usted.

c. Si alguna disposición de esta licencia resulta inválida o inaplicable según la Ley vigente, ello no afectará la validez o aplicabilidad del resto de los términos de esta licencia y, sin ninguna acción adicional por cualquiera las partes de este acuerdo, tal disposición se entenderá reformada en lo estrictamente necesario para hacer que tal disposición sea válida y ejecutiva.

d. No se entenderá que existe renuncia respecto de algún término o disposición de esta licencia, ni que se consiente violación alguna de la misma, a menos que tal renuncia o consentimiento figure por escrito y lleve la firma de la parte que renuncie o consienta.

e. Esta licencia constituye el acuerdo pleno entre las partes con respecto a la obra o la prestación objeto de la licencia. No caben interpretaciones, acuerdos o condiciones con respecto a la obra o la prestación que no se encuentren expresamente especificados en la presente licencia. El licenciador no estará obligado por ninguna disposición complementaria que pueda aparecer en cualquier comunicación que le haga llegar usted. Esta licencia no se puede modificar sin el mutuo acuerdo por escrito entre el licenciador y usted.

Aviso de Creative Commons

Creative Commons no es parte de esta licencia, y no ofrece ninguna garantía en relación con la obra o la prestación. Creative Commons no será responsable frente a usted o a cualquier parte, por cualesquiera daños resultantes, incluyendo, pero no limitado, daños generales o especiales (incluido el daño emergente y el lucro cesante), fortuitos o causales, en conexión con esta licencia. A pesar de las dos (2) oraciones anteriores, si Creative Commons se ha identificado expresamente como el licenciador, tendrá todos los derechos y obligaciones del licenciador.

Salvo para el propósito limitado de indicar al público que la obra o la prestación está licenciada bajo la CCPL, ninguna parte utilizará la marca registrada "Creative Commons" o cualquier marca registrada o insignia relacionada con "Creative Commons" sin su consentimiento por escrito. Cualquier uso permitido se hará de conformidad con las pautas vigentes en cada momento sobre el uso de la marca registrada por "Creative Commons", en tanto que sean publicadas su sitio web (website) o sean proporcionadas a petición previa. Para evitar cualquier duda, estas restricciones en el uso de la marca no forman parte de esta licencia.

Puede contactar con Creative Commons en: **http://creativecommons.org/**.

15. Referencias

[1] http://papi.rediris.es
[2] http://www.rediris.es
[3] http://www.dokuwiki.org
[4] http://www.dokuwiki.org/auth
[5] http://www.apache.org
[6] http://www.prise.es
[7] http://www.dokuwiki.org/devel:authentication_backends
[8] http://www.gnu.org/licenses
[9] http://creativecommons.org
[10] http://www.php.net
[11] http://www.openssl.org
[12] http://e-spacio.uned.es:8080/fedora/get/tesisuned:IngInf-Rcastro/PDF
[13] http://mcrypt.sourceforge.net/
[14] https://forja.rediris.es