# EFDA-Fed: una federación internacional para investigación en fusión basada en PAPI

## EFDA-Fed: A PAPI-based international fusion research federation

**ASOCIACIÓN EURATOM/CIEMAT:** Rodrigo Castro, Jesús Vega, Ana Portas, Augusto Pereira. **RedIRIS:** Diego R. López

Resumen

En Europa se localizan diversos laboratorios que alojan dispositivos de fusión para la realización de diversos experimentos. Como resultado de los experimentos que se llevan a cabo en cada uno de los laboratorios, se generan una serie de datos que son almacenados y posteriormente analizados por los investigadores como base de sus investigaciones. Tanto para poder acceder y analizar los resultados experimentales, como para fijar los parámetros de experimentación y adquisición, se utilizan herramientas que en muchos casos son desarrolladas a propósito por cada laboratorio. Para dar respuesta a las necesidades de seguridad en el laboratorio de fusión del CIEMAT, se implantó PAPI [1] como sistema de autenticación y autorización para el control de acceso a sus sistemas de información. Gracias a los buenos resultados y facilidad de integración con las aplicaciones JAVA [2,3] desarrolladas, otros laboratorios de fusión, y la organización EFDA [4] , se han interesado en PAPI como infraestructura de autenticación y autorización distribuida para la integración y acceso remoto a aplicaciones y recursos. A lo largo del texto se describirá una solución basada en una estructura organizativa federada.

**Palabras clave:** PAPI, infraestructura de autenticación.

Summary

There are a number of laboratories in Europe that house fusion devices to conduct a variety of experiments. The results obtained through experimentation at each of the laboratories are used to generate data that are stored and subsequently analysed by researchers as the basis for their research. The tools used both to access and analyse the experiment results and to establish the experimentation and acquisition parameters are often developed specifically for that purpose by each laboratory. In response to the security needs at the CIEMAT fusion laboratory, PAPI was implemented as an authentication and authorisation system for access to the information systems. Thanks to the positive results and its easy integration with JAVA applications, other fusion laboratories and the EFDA organisation have taken an interest in PAPI as a distributed authentication and authorisation infrastructure for integration and remote access to applications and resources. The text describes a solution based on a federal organisational structure.

**Keywords:** PAPI, authentication infrastructure.

PAPI se implantó para dar respuesta a las necesidades de seguridad en el laboratorio de fusión del CIEMAT

## 1. Introducción

Con el avance en las comunicaciones y la integración de los sistemas informáticos en Internet, los usuarios han pasado de trabajar en sistemas cerrados, donde estaciones de trabajo, servicios y recursos se encontraban aislados a nivel de comunicación de otros sistemas, a sistemas abiertos donde la mayoría de sus elementos se encuentran conectados a Internet. En este tipo de entorno, muchos de los servicios a los que acceden los usuarios se encuentran deslocalizados y repartidos por diferentes organizaciones.

Este tipo de entornos abiertos ha disparado la necesidad de integrar y aplicar soluciones de seguridad a los sistemas de información. Dichas soluciones deben ser capaces de trabajar en sistemas que engloban a varias organizaciones, y por tanto deben ser suficientemente flexibles como para ser integrados en sus sistemas de informáticos y futuros desarrollos, deben escalar adecuadamente, ya que en muchos casos engloban a decenas de miles de usuarios y cientos de servicios, y deben permitir la movilidad de los usuarios. Por todo ello, soluciones de seguridad que resultaban prácticas en sistemas cerrados (normalmente soluciones centralizadas o basadas en la dirección IP origen de las conexiones), resultan poco flexibles, además de difíciles de mantener y escalar en este tipo de entornos.

En este trabajo se describe una solución distribuida de seguridad que permite autenticación y autorización, y se presenta la federación como estructura organizativa que permite integrar dichas soluciones de seguridad en un entorno multi-organización.

Trabajar en entornos abiertos ha disparado la necesidad de integrar y aplicar soluciones de seguridad a los sistemas de información

### 1.1. Descripción del problema

Las investigaciones en energía de fusión en Europa son realizadas en una serie de laboratorios y centros pertenecientes a diferentes países. EFDA es una organización responsable de potenciar la colaboración y coordinación entre estos centros. En cada laboratorio de fusión existe una unidad de control y adquisición de datos, responsable de gestionar los sistemas de control de la máquina de fusión de ese laboratorio, además de gestionar la adquisición, almacenamiento y recuperación de los datos generados en los experimentos realizados en dicha máquina. Los investigadores analizan constantemente los datos recogidos de diferentes experimentos. Para ello, las unidades de control y adquisición desarrollan, y ponen a disposición de los investigadores, herramientas que facilitan la recuperación y visualización de los datos almacenados.

Las máquinas de fusión y los instrumentos de diagnóstico (medición) en los diferentes laboratorios son diferentes y es muy típico que los investigadores viajen a otros laboratorios para poder trabajar con los datos de sus experimentos. Por otra parte, dentro de EFDA existen grupos de trabajo y coordinación, formados por miembros de los diferentes laboratorios, en los que se realizan proyectos en colaboración y en los que las herramientas de trabajo en grupo resultan esenciales. Todo ello hace de éste un entorno perfecto para el desarrollo de tecnologías que faciliten y potencien el trabajo en grupo, así como el acceso remoto a datos y aplicaciones que se encuentran distribuidos por diferentes organizaciones. De la misma forma, ITER [5] nace con la filosofía de ser un laboratorio abierto a los investigadores de diferentes países y se busca potenciar el acceso remoto a datos y aplicaciones.

EFDA es una organización responsable de potenciar la colaboración y coordinación en los laboratorios de fusión

**A nivel de seguridad,** es necesario que el acceso a las diferentes aplicaciones y datos quede restringido a aquellos usuarios que estén autorizados a utilizarlos. Para ello se deben poder establecer políticas de acceso basadas en criterios coherentes con el entorno de laboratorios de fusión. A su vez, se debe minimizar el número de claves diferentes que un usuario debe conocer, así como la cantidad de veces que se debe autenticar para acceder a los diferentes recursos. De esta forma aumenta la sensación de entorno de trabajo remoto, permitiendo con una sola autenticación, el acceso a aquellos recursos a los que el usuario esté autorizado.

**A nivel funcional,** se debe maximizar el conjunto de aplicaciones comunmente utilizadas. Cabe destacar en este sentido, que navegadores web como: Netscape, Mozilla, MS Explorer u Opera, son ampliamente utilizados por los investigadores. Así mismo, ha cobrado gran importancia la utilización de la tecnología Java Web Start (JNLP) [6] como sistema que facilita a los usuarios la instalación y actualización de aplicaciones multiplataforma (ya que están implementadas en JAVA). Con esta tecnología y utilizando un navegador web, el usuario puede lanzar automáticamente la última versión de una aplicación. Otro aspecto fundamental en este entorno de trabajo es la movilidad. Los investigadores tienen que moverse con cierta frecuencia de su lugar habitual de trabajo y es imprescindible para ellos poder seguir accediendo a los recursos a los que habitualmente están autorizados. Con este fin, se ha hecho en los últimos años un esfuerzo de desarrollo, para que los accesos a datos que realizan las aplicaciones los hagan a través del puerto 80 y utilizando como protocolo base el HTTP. Para ello se ha utilizado un modelo de desarrollo en tres capas, en los que los accesos a bases de datos y servicios internos se realizan a través de un servidor de aplicaciones basado en HTTP.

Dentro de EFDA existen grupos de trabajo y coordinación en los que se realizan proyectos en colaboración y en los que las herramientas de trabajo en grupo resultan esenciales

## 2. Federación

Cuando se aplica un sistema de autenticación y autorización a una estructura multi-organización, aunque dicho sistema resuelve aspectos técnicos para poder llevar a cabo un control de acceso adecuado, queda por cubrir una serie de aspectos (de carácter más organizativo y de coordinación) que resultan fundamentales para alcanzar una solución satisfactoria. Para poder cubrir estos elementos, se crea una estructura organizativa que engloba a las organizaciones implicadas y en la que se incluyen y definen una serie de políticas, procedimientos y criterios que terminan a definir la solución final.

## 2.1. Características de un modelo federado

**Identidad y privacidad:** Éste es un criterio básico de un modelo federado. Se trata de que se puedan asociar identidades a usuarios, recursos o componentes del sistema, y dichas identidades sean reconocidas por los diferentes elementos que forman parte de la federación y sirvan para poder identificar de forma unívoca a dichos elementos. Por ejemplo, a un usuario mediante un proceso de autenticación se le asocia una identidad y ésta le servirá para ser identificado frente a recursos u otros elementos de la federación.

Dentro de la federación las organizaciones pueden jugar principalmente dos roles:

**Proveedor de Identidad:** Es el caso de una organización que gestiona sus usuarios y se responsabiliza de su autenticación. También puede mantener un repositorio con información complementaria sobre el usuario, que suele resultar útil para el acceso a recursos cuya política de filtrado requieren de dicha información.

**Proveedor de Servicios:** Se trata de organizaciones que ofertan servicios a usuarios pertenecientes a organizaciones de la federación. Estos servicios normalmente poseen una política de acceso o filtrado que se implementa mediante una serie de reglas de acceso.

La identidad dentro de la federación debe ser válida dentro y no necesariamente hay que asociar a un usuario una identidad que vulnere su privacidad. En una federación pueden manejarse identificadores que resultan válidos como identidad dentro de la federación, pero que sólo el proveedor de identidad puede asociar al usuario real. Así, se protege la privacidad del usuario y a la vez, ante un caso de abuso en un servicio, se puede trazar el usuario que realizó dicho acceso.

**Confianza:** Éste es otro criterio básico en un modelo federado. Deben existir relaciones de confianza a varios niveles:

**Entre organizaciones:** Debe existir confianza a la hora de enviar datos sobre usuarios (por ejemplo que sean necesarios para implementar una cierta regla de control de acceso), y sobre el uso que la otra organización hará de ellos. Así mismo debe existir confianza a la hora de recibir información desde otra organización, en el sentido de que la información recibida se considere veraz.

Entre elementos del sistema: en el sentido de que un elemento debe confiar en que cuando establece una comunicación con un segundo elemento, éste es quien dice ser y además la información intercambiada es veraz e íntegra.

**Coherencia de atributos:** Debe existir una coordinación entre las diferentes organizaciones que conforman la federación para conseguir que la información que una organización posee sobre un usuario es coherente a nivel sintáctico y semántico con las políticas de acceso que implementan los proveedores de servicio dentro de la federación. Por ejemplo, si un recurso posee una regla de filtrado tipo "nivel de seguridad > 3", debe existir una coherencia, tanto a nivel sintáctico como semántico, del atributo "nivel de seguridad" entre las organizaciones cuyos usuarios quieren acceder a este recurso. Para conseguir esto se acuerdan políticas de atributos que permitan esta coordinación.

**Criterio de buen uso:** Es recomendable para mantener la confianza entre los usuarios, proveedores de identidad y los proveedores de servicio, que exista un conjunto mínimo de reglas referidas al uso de la federación. Por ejemplo, mecanismos de autenticación permitidos, utilización de ciertos servicios, tipos de dispositivos autorizados, criterios para preservar la información relativa a los usuarios.

**Criterio de incorporación:** Es recomendable que se concrete una serie de criterios y procedimientos para la incorporación de nuevos miembros a la federación, tanto nuevos proveedores de identidad, como nuevos proveedores de servicio. Esto permite fortalecer la confianza entre las diferentes entidades de la federación, y facilita la gestión de la federación.

Dentro de la federación las organizaciones pueden jugar principalmente dos roles: proveedor de Identidad y proveedor de Servicios

Es recomendable que exista un conjunto mínimo de reglas referidas al uso de la federación.

## 2.2. Elementos englobados en una federación

El concepto de federación dentro de un sistema de control de acceso que engloba a usuarios y recursos de varios centros, se basa en la idea de crear una estructura a nivel organizativo que coordine una serie de aspectos:

**Política de atributos:** Las reglas de control de acceso con las que implementa una política de control de acceso a un recurso puede contener propiedades referentes al usuario que está intentado acceder. A estas propiedades del usuario: edad, cargo, etc., se las llama atributos del usuario. Los atributos del usuario suelen estar almacenados en un repositorio que normalmente coincide con el utilizado para realizar la autenticación. Para que las reglas de control de acceso tengan sentido, sus atributos tienen que coincidir en nombre, sintaxis y semántica, con aquellos almacenados en los de los repositorios de usuario. Para conseguir esta coherencia hay que establecer una política común de atributos que maximice la coordinación entre repositorios de usuario y políticas de control de acceso.
**Política de adhesión:** Se debe establecer un conjunto de reglas que regulen qué organizaciones o bajo qué procedimiento una nueva organización puede ser admitida en la federación. Así mismo se pueden regular otros aspectos como tipo de usuarios, tipo de recursos, etc.
**Infraestructura de autenticación y autorización:** Debe existir una solución tecnológica que soporte las funciones de autenticación y autorización par los usuarios y recursos de las organizaciones federadas.
**Estructura de confianza:** Es necesario implementar una estructura que posibilite la confianza entre los diferentes elementos del sistema que soporta la federación, es decir, que diferentes elementos que conforman la federación crean unos en otros. Para ello, cuando un elemento recibe información de otro, el primero puede autenticar al emisor y comprobar la integridad de los datos recibidos, y por supuesto, asume que la información que el otro le envía es veraz.
**Centro repositorio:** Se trata de un elemento que coordine los recursos disponibles dentro de la federación. Para cada uno de los recursos, es interesante conocer: su localización (URL), organización propietaria, aplicación cliente necesaria para su utilización, así como información referente a los atributos del usuario necesarios para acceder a dicho recurso.

Hay que establecer una política común de atributos que maximice la coordinación entre repositorios de usuario y políticas de control de acceso

## 3. La federación basada en PAPI

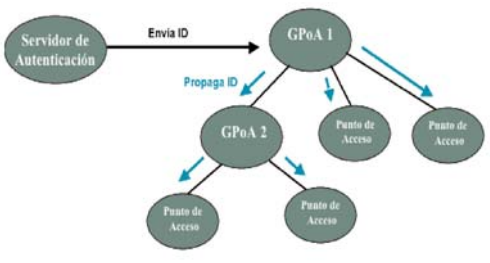
Como se comenta en el punto anterior, se elige PAPI como IAA para soportar la federación EFDA. Esta decisión no es irreversible, ya que por la naturaleza tan similar entre todas las soluciones que se manejan hoy en día como IAA, se podría, a un coste aceptable, cambiar de IAA manteniendo todos los demás elementos y funcionalidades de la federación.

### 3.1. Gestión de la identidad

Con el sistema de manejo de identidad de PAPI, los accesos que realiza un usuario en la federación quedan completamente diferenciados de los que realiza otro usuario

Mediante el sistema de manejo de identidad proporcionado por PAPI se consigue, en un entorno multi-organización, por un lado identificar a un usuario en todos los elementos de la federación. Es decir, que los accesos que realiza un usuario en la federación quedan completamente diferenciados de los que realiza otro usuario. Por otro lado, se pueden manejar identificadores anonimizados. Es decir, identificadores que se corresponden de forma biunívoca con usuarios de la federación, pero que sólo la organización origen de un usuario es capaz de saber a qué usuario corresponde un identificador. Se pueden crear incluso identificadores únicos por sesión.

FIG. 1 MODELO DE IDENTIFICADOR ÚNICO EN PAPI



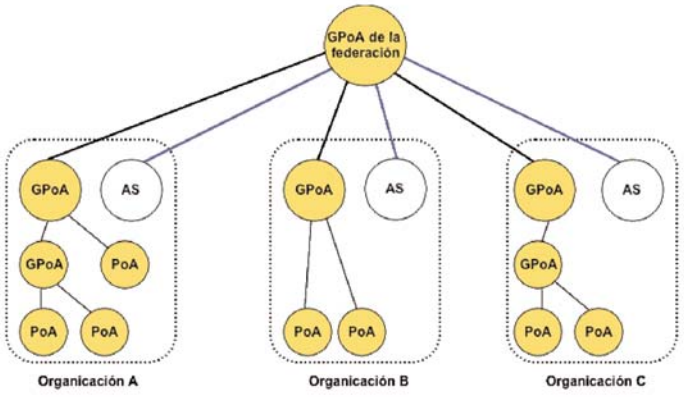

En PAPI, como muestra la figura 1, el identificador es generado por el Servidor de Autenticación de la organización origen y utilizado por los PoAs y GPoAs de las organizaciones destino (propietarias de los recursos). En este caso los GPoAs son capaces de propagar un identificador de usuario a PoAs o

GPoAs por debajo jerárquicamente. Esta propagación no es inmediata, sino que se produce cuando un PoA así lo requiere.
El modo de propagar los identificadores y la posibilidad de estructurar los PoAs y GPoAs de forma jerárquica consiguen un modo de gestionar la federación y los identificadores más sencilla y más flexible.

### 3.2. Estructura federativa

A la hora de montar una federación basada en PAPI, existen dos alternativas. La primera se fundamenta en disponer de un GPoA y un servidor de autenticación en cada organización, y relacionar cada AS los GPoAs de las organizaciones federadas. Cuando un usuario se autenticara en una organización, adquiriría credenciales de cada uno de los GPoAs de las organizaciones federadas. A nivel de gestión, cuando se incluye una nueva organización en la federación, su GPoA debe ser configurado en cada uno de los ASs del resto de organizaciones. Aún así si se quisiera incorporar un nuevo servicio, sólo la organización propietaria tendría que configurar su GPoA, el resto no tendría que tocar nada.
La segunda opción es instalar un GPoA por organización y a su vez un GPoA que los englobe, como muestra la figura 2. De esta forma si un usuario se autentica, obtendría una sola credencial, la credencial del GPoA de la federación. De la misma forma a nivel de gestión es más sencillo, ya que nuevas organizaciones sólo representa un cambio en la configuración del GPoA de la federación. No habría que tocar el resto.

FIG. 2. ESTRUCTURA FEDERATIVA DE PAPI CON GPOA ÚNICO




Finalmente se optó por esta segunda alternativa, debido a la facilidad de gestión, aprovechando al máximo el potencial de las estructuras jerárquicas GPoA.

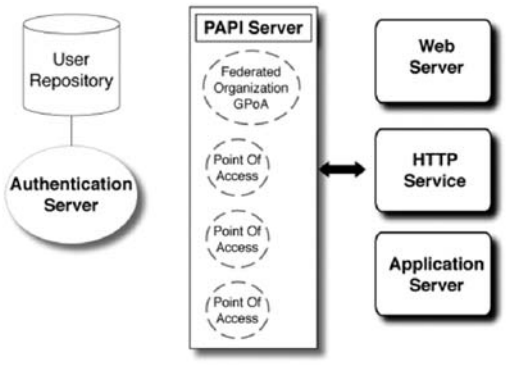
### 3.3. Configuración a nivel de organización

Para facilitar la instalación de PAPI en las diferentes organizaciones, se optó por una configuración tipo. Esta se compone de un servidor de autenticación, configurable en aspecto para cada una de las organizaciones mediante plantillas HTML, y un PAPI Proxy compuesto por un GPoA a nivel de organización y tantos PoAs como sean necesarios colgando de él, dependiendo del número de servicios a cubrir. Gracias a esta configuración, las organizaciones no tuvieron que tocar sus sistemas, sólo la configuración del PAPI proxy.

El modo de propagar los identificadores y la posibilidad de estructurar los PoAs y GPoAs de forma jerárquica consiguen una gestión de la federación y de los identificadores más sencilla y más flexible

Una federación basada en PAPI se puede montar de dos formas

FIG. 3. CONFIGURACIÓN BASE PARA LAS ORGANIZACIONES DE LA FEDERACIÓN EFDA




Para facilitar la instalación de PAPI en las diferentes organizaciones se optó por una configuración tipo

### 3.4. Espacio web para coordinación

Para poder coordinar la federación, se ha desarrollado un espacio web "http://efdafed.fusion.ciemat.es", donde se gestionan diferentes aspectos de la federación:

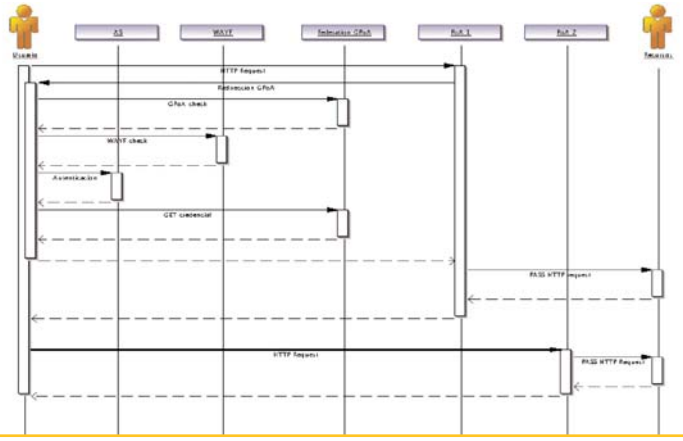
- Recursos disponibles: Se describen los recursos disponibles en la federación.
- Organizaciones adscritas a la federación: Describiendo para cada una de ellas:
- Servio WAYF para la federación: Sirve para redireccionar al usuario al servidor de autenticación de su organización. Este servicio posee registro de todos los servidores de autenticación de la federación.
- Repositorio de documentación y enlaces de interés: Enlaces a documentos e información de interés tanto para los usuarios de la federación y así poder entender cómo funciona, como para los administradores de las diferentes organizaciones, con información más técnica.

### 3.5. Funcionamiento de la federación

Un usuario, para acceder a la federación, tiene dos vías. La primera consiste en intentar acceder a un recurso federado, bien a través de la web de la federación, o bien directamente mediante su URL. En este caso el usuario será rechazado, como muestra el diagrama de secuencia de la figura 4 y de forma transparente será redirigido al servicio WAYF de la federación, donde se le facilita un listado de organizaciones federadas, para que el usuario elija su organización origen donde posteriormente será autenticado. Si la autenticación es correcta, será redirigido de forma automática y transparente al recurso que primeramente el usuario intentó acceder. A partir de aquí el usuario tendrá acceso automático a todos los recursos federados y locales a los cuales está autorizado.

Para poder coordinar la federación se ha desarrollado un espacio web

FIG. 4. DIAGRAMA DE SECUENCIA DEL PROTOCOLO PAPI EN LA FEDERACIÓN EFDA



La segunda vía es, primero el usuario accede a su servidor de autenticación, y una vez autenticado, visualiza una lista de todos los recursos accesibles, tanto federados como locales.

## 4. Conclusiones

Desde el mes de Junio de 2007 está en funcionamiento la federación EFDA en la que participan a fecha de hoy seis laboratorios de fusión: CIEMAT (España), CEA (Francia), JET (Inglaterra), IST (Portugal), EFDA (Europa), HAS-KFKI (Hungría). Para su implantación se optó por utilizar PAPI, que a pesar de su falta de estandarización a nivel de protocolo, tenía un nivel de desarrollo más avanzado y permitía la integración de más tipos de aplicaciones, como aplicaciones JAVA que son utilizadas en los laboratorios de fusión para el análisis de señales. A su vez, gracias al modelo simplificado de PAPI y su servidor PAPI Proxy, se han conseguido unos tiempos de instalación bastante reducidos y con un mínimo soporte.

Actualmente, se ha logrado integrar con éxito algunas aplicaciones JAVA para visualización y análisis de señales, así como un servidor Wiki utilizado por la comunidad EFDA para sus grupos de trabajo. Así mismo, existen laboratorios como el TJII perteneciente al CIEMAT (Centro de investigaciones energéticas, medioambientales y tecnológicas), en el que PAPI se está utilizando como sistema de autenticación y autorización para el control de acceso a sus sistemas de adquisición.

En la última reunión organizada entre miembros de la federación, se acordó la integración de nuevas herramientas y recursos gestionados por diferentes organizaciones miembro de la federación. Además se va a trabajar en los próximos meses en el desarrollo de las políticas de: admisión de nuevas organizaciones, de buen uso de la federación, y en la política de atributos.

Todo este trabajo espera ser un buen banco de pruebas para la utilización de modelos federados en grandes instalaciones de fusión futuras, como ITER, en el que se hace prioritario sistemas de participación remota y experimentación a nivel multi-organización.

Se va a trabajar en los próximos meses en el desarrollo de las políticas de: admisión de nuevas organizaciones, de buen uso de la federación, y en la política de atributos

Este trabajo espera ser un buen banco de pruebas para la utilización de modelos federados en grandes instalaciones de fusión futuras

### Referencias

[1] *"PAPI home page". http://papi.rediris.es*
[2] *R. Castro, D.R. López and J. Vega. "An authentication and authorization infrastructure: The PAPI system". Fusion Engineering and Design, Volume 81, Issues 15-17, July 2006, Pages 2057-2061.*
[3] *J. Vega, E. Sánchez, A. Portas, et al. "Overview of the TJ-II remote participation system". Fusion Engineering and Design, Volume 81, Issues 15-17, July 2006, Pages 2045-2050.*
[4] *"European Fusion Development Agreement". http://www.efda.org"*
[5] *International Thermonuclear Experimental Reactor". http://www.iter.org*
[6] *"JAVA Web Start Technology". http://java.sun.com/products/javawebstart/index.jsp*

**Rodrigo Castro**
**Jesús Vega**
**Ana Portas**
**Augusto Pereira**
CIEMAT

**Diego R. López**
RedIRIS