tecnimap Murcia 2004

3

E-PARLAMENTOS: UN MODELO DE COOPERACIÓN PARA INTERCAMBIO DE DATOS ENTRE INSTITUCIONES LEGISLATIVAS

Francisco Chávez Gutiérrez
Ingeniero en Informática. Jefe de la Unidad de Informática
Parlamento de Canarias

Juan Ignacio Rodríguez de León
Ingeniero en Informática. Analista de la Unidad de Informática
Parlamento de Canarias

Elena Sánchez Nielsen
Doctora por la Universidad de La Laguna. Ingeniera en Informática.
Profesora del área de Ciencias de la Computación e Inteligencia Artificial
Universidad de La Laguna

1. INTRODUCCIÓN

La utilización de procedimientos que permitan la colaboración entre asambleas legislativas constituye una prioridad política de la COPREPA (Conferencia de Presidentes de Parlamentos Autonómicos de España) y la CALRE (Conferencia de Asambleas Legislativas Regionales Europeas). Al mismo tiempo, desde la Unión Europea se impulsa distintas iniciativas encaminadas al uso de las tecnologías de la información y comunicación (TIC) para gestionar los servicios de las administraciones a través del programa e-Europe2005 [1], donde una de las prioridades en el ámbito del gobierno electrónico se centra en la creación de un marco de interoperabilidad que relacione las diferentes administraciones e instituciones entre sí.

Actualmente, cada asamblea legislativa ha desarrollado en mayor o menor medida, sistemas de información que se encargan de llevar a cabo toda la actividad legislativa, así como ofrecer información a través de sus páginas Web. Al mismo tiempo, resulta de gran interés así como necesario compartir información entre las asambleas legislativas con el fin de mejorar la eficiencia y eficacia en la tramitación legislativa de cada una de las instituciones.

1.1 Objetivo

En esta comunicación, se presenta el proyecto *e-Parlamentos* basado en un modelo *e-Government* [2] que permite la cooperación, integración e intercambio de datos y servicios entre las diferentes asambleas legislativas españolas, con extensión a las asambleas europeas e incluso proveer información y servicios directamente a los ciudadanos. Entre los fines prioritarios iniciales de este proyecto se encuentra:

- Compartir e intercambiar información online entre las diferentes asambleas legislativas mediante la utilización de tres servicios básicos: (a) consulta de tramitación legislativa; (b) consulta de actividades legislativas y (c) consulta de fondos bibliotecarios.
- Resolución del problema de interoperabilidad entre los diferentes sistemas distribuidos de información perteneciente a cada institución, permitiendo complementar los sistemas actuales con la menor incidencia en ellos.
- El manejo de información en diferentes idiomas entre las distintas instituciones.
- El incremento de la productividad a través de una mayor eficiencia operacional.
- La oferta de servicios de mayor calidad e innovación de los mismos.

1.2 Análisis de Requisitos

Los retos esenciales de este proyecto se centra en: (1) la no modificación de los sistemas de información que utiliza actualmente cada una de las instituciones parlamentarias, (2) resolución de los problemas de interoperabilidad que surgen como consecuencia de la heterogeneidad existente entre las diferentes plataformas hardware/software utilizadas por cada una de las asambleas legislativas y (3) desarrollo de un modelo de seguridad eficiente y transparente a la arquitectura del sistema. En base a ofrecer una solución plausible a estos problemas, deben ser considerados los siguientes aspectos fundamentales:

- La solución propuesta debe ser una solución distribuida y no jerárquica. Es decir, ninguna institución participante debe jugar un papel diferente o rol superior respecto a cualquier otra institución. En el caso necesario que alguna institución debiese asumir

un rol distinguido, la elección debería ser realizada a través de un algoritmo democrático, en el sentido de que todos los participantes puedan tener las mismas opciones a ser elegidos.

- El sistema resultante debe ser un sistema abierto, en el sentido de no pertenecer a una arquitectura o lenguaje particular, como consecuencia de la utilización de tecnologías diferentes por cada una de las asambleas.
- La utilización de soluciones basadas en tecnologías de servicios web con la finalidad de resolver los problemas de interoperabilidad que surge entre los sistemas heterogéneos de información distribuidos pertenecientes a las diferentes asambleas así como facilitar el acceso e interacción entre los mismos.
- El modelo de seguridad a utilizar se caracteriza por una serie de consideraciones especiales. Cada asamblea debe ser responsable de poder añadir o eliminar sus propios usuarios, así como poder revocar y conceder los permisos cuando sea necesario. Por otra parte, es responsabilidad de cada asamblea disponer de un medio accesible por las otras asambleas con la finalidad de poder validar a los usuarios.
- Debe existir un nivel de acceso público o anónimo sin restricciones de uso para todas aquellas operaciones o información que no requieran consideraciones especiales de seguridad, tales como documentos públicos, anuncios, información bibliográfica, etc.
- Cada asamblea puede disponer de un firewall que proteja las redes y los sistemas internos. Es necesario incidir lo mínimo posible en la configuración de los firewalls de cada asamblea.

El resto de la presente comunicación se estructura de la siguiente manera. En el apartado 2, se ilustra una visión general de la tecnología de servicios web. El apartado 3 detalla la arquitectura general del proyecto y la descripción de cada uno de los componentes que la integra. Finalmente, en la sección 4 se comenta las principales conclusiones obtenidas.

2. TECNOLOGÍA DE SERVICIOS WEB

La utilización de soluciones basadas en tecnologías de servicios web ofrece una solución plausible en el intercambio de información entre las distintas asambleas legislativas debido al soporte tecnológico que ofrecen al problema de la interoperabilidad entre aplicaciones distribuidas utilizando tecnologías estándares basadas en XML y protocolos de transporte de Internet tales como TCP/IP y HTTP.

La arquitectura de los servicios web está basada en tres tipos de participantes: *proveedor del servicio, demandante del servicio y registro de los servicios*. De esta forma, los *proveedores de servicios* ofertan sus servicios, para ello *definen* sus servicios y los *publican* en el *registro de servicios*. Los *demandantes de servicios* utilizan una operación de *encontrar* con el fin de localizar los servicios de su interés. El *servicio de registro* devuelve la descripción de cada uno de los servicios relevantes, la cuál es utilizada por el *demandante de servicio* para *invocar* el servicio Web correspondiente. Dichas funcionalidades de los servicios Web se ilustran en la figura 1.

El soporte de las interacciones entre servicios web se realiza a través de tres iniciativas estándares basadas en tecnologías XML:

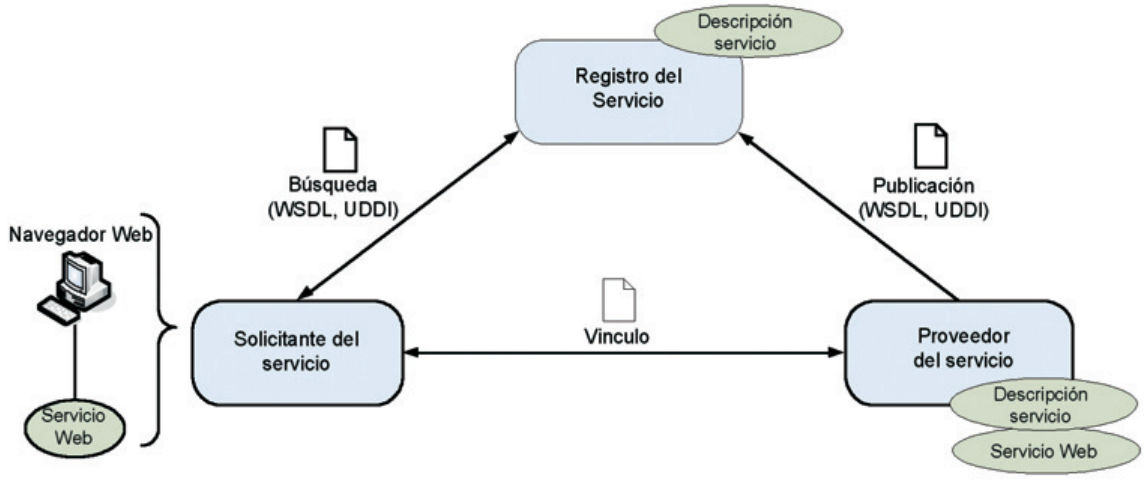

Figura 1. Modelo de referencia de los servicios web.

- WSDL (Web Services Description Languages) [3]: es un lenguaje basado en XML que se utiliza para describir las características operacionales de los servicios Web.
- UDDI (Universal Description, Discovery, and Integration) [4]: es un repositorio XML, en donde las diferentes empresas e instituciones pueden registrar la información acerca de sí mismos, sobre los servicios que ofrecen y la información técnica sobre cómo pueden acceder a estos servicios.
- SOAP (Simple Object Access Protocol) [5]: es un protocolo de comunicación que emplea los estándares actuales de Internet: XML para el formato de mensajes, HTTP y otros protocolos de Internet para el transporte de mensajes.

3. PROYECTO E-PARLAMENTOS

Una de las premisas fundamentales en la que se centra el diseño de la arquitectura del proyecto es el de mantener la independencia e igualdad entre todos los participantes. Ello conlleva que no existirá un coordinador o responsable central que gestione un directorio de los participantes.

La arquitectura general del proyecto *e-Parlamentos* para el intercambio de datos y servicios entre asambleas legislativas se muestra en la figura 2.

El diseño de la arquitectura incluye tres componentes o capas de funcionalidad: (1) *Capa de Manejador de Procesos,* que permite realizar las peticiones de información haciendo uso de los servicios web desplegados en cada asamblea legislativa. (2) *Capa de Servicios Web,* que describe la implementación de los servicios web en cada asamblea y permite realizar las consultas a las bases de datos de cada asamblea. Y (3) *Capa de Seguridad,* que desarrolla cual puede ser la política implementada en cada asamblea en cuanto a seguridad de los datos a compartir.

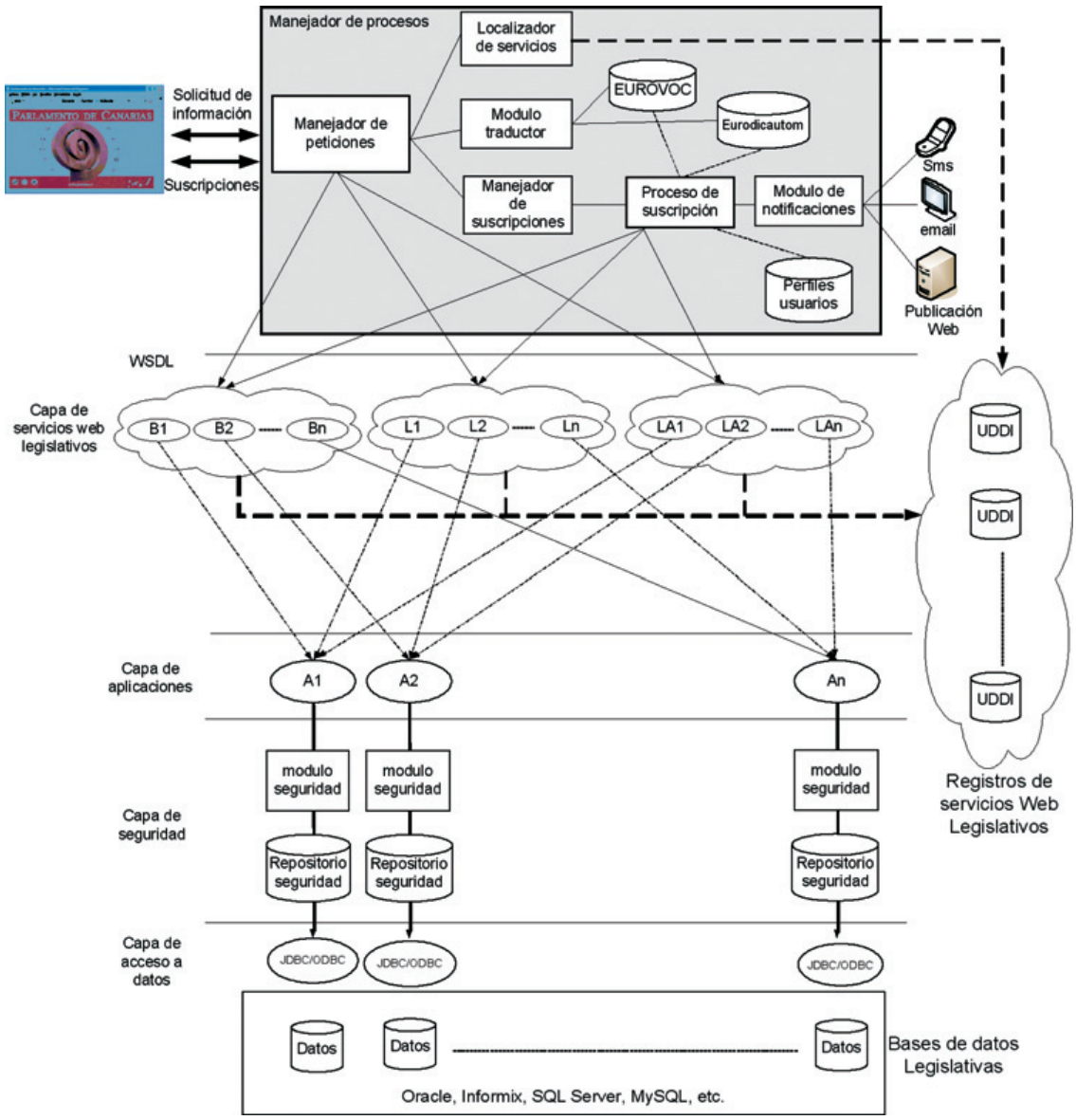

Figura 2. Arquitectura general del proyecto e-Parlamentos.

En primera instancia, se propone el desarrollo de tres módulos, que permitirán desarrollar tres servicios web, para permitir consultas a: (i) información legislativa (L), (ii) actividades legislativas (LA), así como (iii) fondos bibliográficos (B).

En el diseño de la arquitectura propuesta, se han considerado tres aspectos primordiales:

- No pretender cambiar los sistemas que cada asamblea dispone en la actualidad, sino complementarlos. La elección de sistemas estándares tales como el uso de tecnologías XML y el protocolo de Internet de transporte HTTP, permitirá complementar a los sistemas actuales de cada asamblea con la menor incidencia en ellos.

- No requerir una formación adicional en los usuarios, como consecuencia de que el sistema puede ser integrado dentro de la aplicación actual que realiza la búsqueda de información en las bases de datos locales.
- Proponer a cada asamblea el poder disponer de un Web Service Registry (UDDI), con el fin de que cada asamblea pueda publicar nuevos servicios o modificar los actuales de una forma autónoma. De esta forma, todas las modificaciones realizadas en cada Web Service Registry de cada asamblea, sería replicado de forma automática al resto de las asambleas. Esta condición no es indispensable, ya que se podría implementar un único Web Service Registry en una única asamblea, pero ello conllevaría que cualquier modificación en un servicio web de una asamblea, necesitaría de la solicitud de cambio a la asamblea que administre el Web Service Registry.

A continuación, se describe la funcionalidad de cada una de las capas que integra la arquitectura del sistema propuesto.

3.1 Capa de Manejador de Procesos

Se encarga de procesar todas las peticiones de los usuarios del sistema. Recibe dos tipos de peticiones: *solicitud de información* y *suscripción de peticiones.*

El *manejador de procesos* se ubicará en cada asamblea. Cada asamblea podrá realizar su propia implementación en función de la disponibilidad de los recursos.

Al hacer uso de los servicios web de las asambleas, la información consultada puede ser visualizada a través de una página Web, una aplicación específica, o una aplicación integrada dentro de alguna existente. De esta forma, no se requiere una formación añadida a los usuarios, sino que el nuevo sistema puede integrarse dentro de la aplicación existente de búsqueda de información de las bases de datos locales, resultando transparente para el usuario.

3.1.1 Manejador de Peticiones

Todas las peticiones son recibidas y procesadas por el módulo *manejador de peticiones.* Este módulo hace uso del módulo *localizador de servicios,* para determinar qué servicios están disponibles, donde y como invocarlos. El módulo localizador de servicios se encarga de interrogar al Web Service Registry (UDDI), que puede estar ubicado localmente, de forma centralizada en una asamblea legislativa, o de forma distribuida. De esta manera, este módulo averigua que servicios web están disponibles.

El módulo *manejador de peticiones* puede mejorar la consulta mediante la utilización del *módulo traductor.* Este módulo hace uso de las bases de datos *Eurovoc* [6] y *Eurodicautom* [7].

Eurovoc representa un tesauro multilingual que cubre los once países que integra la Unión Europea (Español, Danés, Alemán, Griego, Francés, Italiano, Holandés, Portugués, Finlandés y Sueco). Eurovoc provee un mecanismo de indexación de los documentos en los sistemas de documentación. Actualmente, es utilizado por el Parlamento Europeo, la Oficina para Publicaciones Oficiales de las Comunidades Europeas, parlamentos nacionales y regionales en Europa, departamentos gubernamentales nacionales y determinadas organizaciones Europeas.

Eurodicautom constituye el banco de términos multilingual de la Comisión Europea. Está compuesto por: (i) Dicautom, un diccionario automático de frases y (ii) Euroterm, un diccionario traductor en once idiomas diferentes, donde el latín está incluido.

De esta forma, a partir de la información que se desea buscar, se realiza una primera fase en la que se extraen los términos que son relevantes en la búsqueda. A continuación, en una segunda fase se buscan las correspondencias de esos términos en los otros idiomas. Obteniéndose de esta manera, una ampliación de la consulta a instituciones que dispongan su información en otro idioma, así como la ampliación de la búsqueda mediante la utilización de términos sinónimos.

3.2.2 *Manejador de Suscripciones*

Además de peticiones de información, el sistema permite que un usuario sea informado cuando en alguna asamblea legislativa se publique algo de su interés.

Cada usuario podrá elegir suscribirse a una colección de términos, establecidos en el tesauro Eurovoc, y podrá elegir la forma en que el sistema le notificará dicha información.

La finalidad del *módulo de proceso de suscripción* es doble, por una parte, se centra en el procesamiento de todas las suscripciones almacenadas en una base de datos que representa el *módulo de plantillas de perfiles de usuarios,* y por otra parte, se encarga de la interacción con los servicios web de las diferentes asambleas legislativas para determinar si sobre un determinado término se ha publicado algo recientemente. Con el fin de no sobrecargar los sistemas, este proceso podrá ser programado en un horario en el que no se esperen otras consultas.

El *módulo de notificaciones* se encargará de realizar la notificación al usuario mediante el método que cada usuario haya especificado en su perfil (sms, email, Web publishing, etc.)

3.2 Capa de Servicios Web Legislativos

Por cada servicio que se desee implementar en cada asamblea legislativa, se desplegará una aplicación que implementará un servicio web en esa asamblea y que permitirá consultar la información relativa a ese servicio, de forma remota por otras asambleas.

Dado que la arquitectura propuesta es totalmente descentralizada, permite que cada asamblea pueda decidir de forma autónoma la implementación de los servicios web o no hacerlo. De la misma forma, puede desplegar tan sólo un servicio web de todos los planteados, o realizarlo de forma progresiva. Así mismo, cada parlamento es libre de implementar los servicios en la plataforma y con el/los lenguajes de programación que desee.

En el momento en el que una asamblea legislativa decida publicar su nuevo servicio web con la finalidad de que las demás asambleas puedan hacer uso de él, tan sólo tendrá que publicarlo en un Web Service Registry (UDDI). Cada parlamento podrá disponer de un registro de servicios web, donde residirá toda la información de los servicios web de cada parlamento. La publicación de un nuevo servicio por parte de un parlamento en un registro de servicio web (UDDI), conllevará la replicación automática al resto de los registros de servicios web, con lo que pasará a estar disponible al resto de los parlamentos.

Se requerirá establecer entre todas las asambleas legislativas, la información mínima que contendrá un determinado servicio web. Por ejemplo, la información mínima requerida para la implementación de un servicio web de consultas legislativas, ilustrado como (L) en el gráfico de la figura 2, debería incluir la siguiente información: título, fecha, estado actual y proponente. De esta forma, se podrá obtener información de cómo ha sido la tramitación de una ley en cada una de las asambleas, unificándose tanto las consultas como la información recuperada.

Toda la información relativa a cuales son los datos necesarios para invocar el servicio web, así como la lista de datos de retorno, vendrán especificados en el fichero WSDL del servicio web implementado por cada asamblea, y que se ha publicado en el Web Service registry (UDDI).

En el gráfico de la figura 2 se han representado tres servicios web distintos: consultas al fondo bibliográfico (B), consultas a la tramitación legislativa (L) e información sobre actividades legislativas en general (LA); donde el índice en cada una de ellas indica el servicio web implementado por cada asamblea legislativa.

Los servicios web de cada asamblea legislativa, serán desarrollados acorde con la estructura interna de la información, y dependiendo de la tecnología de sus sistemas informáticos. En definitiva, tendrá que ser desarrollado a medida de cada asamblea legislativa.

En el caso en que varias asambleas legislativas compartiesen un mismo sistema informático, entonces el desarrollo realizado para implementar el servicio web en una de ellas se podrá aprovechar en la otra asamblea legislativa.

El punto de entrada a la invocación de los servicios web implementados en cada asamblea es representada por la *capa de aplicaciones*.

3.3 Capa de Seguridad

La seguridad del sistema debe permitir desarrollar servicios web que aseguren que la información compartida entre parlamentos es confidencial.

El sistema de seguridad debe cumplir igualmente las siguientes características:

- **Flexibilidad.** El sistema debe ser capaz de acomodar distintas exigencias y escenarios de seguridad, en un espectro que abarca desde la libertad más absoluta – servicios web sin ninguna restricción – a escenarios extremadamente restrictivos, pasando por todas las gamas intermedias – validaciones por listas de acceso (ACL), validaciones por IP, restricciones de uso a una franja horaria, etc... En general, el sistema permitirá que cada parlamento establezca los criterios de seguridad para el uso de los servicios que ésta ofrezca.
- **Modularidad.** El sistema se ha dividido en varios módulos buscando un diseño que mantenga aislados cada uno de los componentes del sistema. Se ha optado por subdividir el módulo de seguridad en tres componentes, cada uno de ellos responsable de una parte de la seguridad. Estos componentes, que se detallarán más adelante, los hemos denominado Módulo de identificación, *Módulo de validación y autorización y Módulo de invocación*.
- **Ubicuidad.** El sistema de seguridad debe obligar al usuario a identificarse ante el sistema una única vez, independientemente de si las operaciones que va a ejecutar son en uno, varios o en todos los componentes de la red. Normalmente, el usuario debería poder acceder al sistema como a un todo, dando la impresión de estar conectado a una única máquina que le proporciona los servicios que necesita.

La figura 3 ilustra de forma gráfica el esquema del modelo de seguridad propuesto en el proyecto e-Parlamentos.

El proceso para invocar un servicio es el siguiente:

a) El proceso solicitante (cliente) se dirige al *Módulo de invocación*, indicando todos los parámetros del servicio a invocar y la identificación de sesión del usuario.

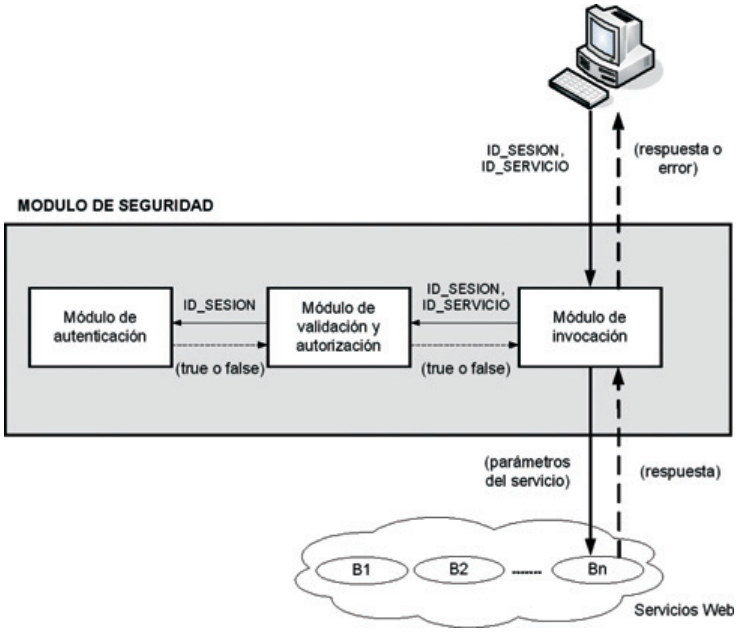

Figura 3. Modelo de seguridad de e-Parlamentos.

b) Si el servicio a invocar es público (es decir, no se requiere estar identificado ante el sistema para llamarlo) el módulo de invocación se limita a llamar al procedimiento indicado, suministrándole los parámetros necesarios, y retorna el resultado del mismo sin más.
c) Si el servicio no es público, se le exigirá al usuario como mínimo estar identificado en el sistema (identificador de sesión). El identificador de sesión incluirá datos como: nombre de usuario, login, parlamento de origen, dirección IP y correo electrónico. Cada parlamento desarrollará los módulos de autenticación, validación y autorización, en función de las condiciones que establezca para el uso de los servicios que suministra.

Las políticas de seguridad se definen utilizando unos componentes activos, que denominaremos *centinelas*. Cada servicio web, se asocia con uno o más centinelas. Cuando el módulo de invocación comprueba, según sus registros, que determinado método web está custodiado por uno o varios centinelas, ejecuta el método check de cada uno de ellos, pasando dos parámetros: el identificador de sesión y el identificador del servicio a ejecutar. Contando con esta información, cada centinela debe tomar la decisión de si el usuario puede o no ejecutar el método indicado.

Si cualquiera de los centinelas deniega la operación, ésta se aborta y se le retorna un mensaje de error al cliente, indicando la causa de la denegación, pudiendo informarle del mecanismo a usar para resolver esta situación, si procede. Si todos los centinelas aprueban la operación, ésta se ejecuta y los resultados son devueltos al cliente.

Se proponen distintos tipos de centinelas, cada uno de los cuales implementará un esquema de seguridad habitual. El centinela más sencillo sólo comprueba que el usuario esté autenticado. Para ello, simplemente verifica que el identificador de sesión suministrado sea una sesión válida. Si es así, aprueba la operación, en caso contrario, la cancela. Otros esquemas habituales son el uso de ACL (*Access Control List*).

La potencia del sistema, radica en la facilidad de escribir sus propios centinelas por parte de cada parlamento. Únicamente se tiene que reescribir la implementación del método check para que se ajuste a sus propósitos. Por ejemplo, se puede definir un centinela que sólo permita conexiones desde una determinada IP, en un rango de horas determinado, y que notifique de dicho acceso al usuario usando su correo electrónico, para prevenir posibles robos de cuentas.

Normalmente, una de las tareas que todo centinela tendrá que realizar es obtener, a partir del identificador de sesión, los datos de sesión propiamente dichos. En el caso de que tanto la sesión del usuario como el servicio a ejecutar, pertenezcan al mismo parlamento, no presenta ningún problema. Sin embargo, es posible que los datos de la sesión estén almacenados en un parlamento diferente. En ese caso, se solicita al parlamento propietario de la sesión que le transfiera todos los datos de la misma, *validación de sesión,* de forma que se puede crear una copia local.

Evidentemente, la *validación de sesión* es un procedimiento crucial desde el punto de vista de la seguridad, por lo que deben verificarse los requisitos de autenticación y seguridad, sólo que ahora a nivel de parlamentos. Por esta razón, el envío de los datos usa criptografía asimétrica. Cada parlamento cuenta con dos claves, una clave privada y una pública.

Para garantizar que el parlamento del destino del mensaje, sea el único que pueda leer los datos de la sesión, se encriptan los datos con su clave pública. Por otro lado, para garantizar la autenticidad del mensaje (no repudio), el mensaje encriptado anteriormente, se encripta nuevamente con la clave privada del parlamento que envía los datos de la sesión.

Para obtener los datos de la sesión, el parlamento que recibe el mensaje, invierte las operaciones.

En cualquier caso, toda la sobrecarga implícita en esta transferencia de sesiones es responsabilidad única del submódulo de autenticación. Para el resto de los componentes del módulo de seguridad, todo este trasvase de información será transparente.

La utilización de este esquema de seguridad, presenta varias ventajas:

a) Los servicios web propiamente dichos, no necesitan conocer las políticas de seguridad definidas para ellos. El sistema garantiza que no se llegarán a invocar a menos que todas las garantías de seguridad exigidas, se cumplan (todos los centinelas han dado el visto bueno a la petición). De igual forma, los centinelas, no necesitan conocer las interioridades de cada servicio.
b) Un mismo servicio web puede ser utilizado en varios parlamentos, pudiendo desarrollar centinelas que apliquen criterios de seguridad distintos en cada parlamento.
c) El *proceso de validación de sesión,* nos permite que una vez que un usuario esté identificado en un parlamento, sea automáticamente identificado en el resto.
d) Las distintas responsabilidades están claramente diferenciadas, lo que simplifica el desarrollo y las modificaciones en el sistema. Si una persona está accediendo a un servicio indebidamente, el problema está en la política de seguridad que está aplicando ese parlamento.
e) Los accesos a servicios públicos, sufren una sobrecarga mínima de seguridad, basado en un único nivel de indirección.

4. CONCLUSIONES

Un modelo de sistema de información cooperativo para el intercambio de información y servicios entre asambleas legislativas se ha descrito en esta comunicación a través del proyecto e-

Parlamentos. El desarrollo e implementación de este proyecto se centra en tres aspectos fundamentales: (1) un modelo descentralizado para la resolución del problema de cooperación entre las asambleas legislativas, donde ninguna entidad participante puede asumir un rol distinto o más importante que el restos de las entidades, (2) la utilización de soluciones basadas en el uso de la tecnología de servicios web que permiten ofrecer una solución plausible al problema de la interoperabilidad entre parlamentos y (3) un modelo flexible, modular y ubicuo de seguridad.

REFERENCIAS

1. eEurope 2005 Action Plan. 2002. http://europa.eu.int/information_society/eeurope/2005/index_en.htm
2. A. K. Elmagarmid and W.J. McIver, editors. 2002. Advances in Digital Government: Technology, Human Factors and Policy. Kluwer Academic Publishers.
3. W3C: World Wide Web Consortium. 2003. Web Services Description Language (WSDL). http://www.w3.org/TR/wsdl
4. W3C: World Wide Web Consortium. 2003. Universal Description, Discovery, and Integration. http://www.uddi.org/
5. W3C: World Wide Web Consortium. 2003. Simple Object Access Protocol. (SOAP). http://www.w3.org/TR/soap/
6. The Office for Official Publications of the European Communities. Eurovoc Thesaurus. http://europa.eu.int/celex/eurovoc/
7. The Office for Official Publications of the European Communities. 1973 Eurodicautom http://europa.eu.int/eurodicautom