

Implantación de Servicios de PKI en el Canal Web de Internet del Banco de España

A lo largo de este artículo se describe cómo el Banco de España, tras implantar su Infraestructura de Clave Pública, ha abordado la integración de los servicios de PKI en las aplicaciones corporativas. Con este objetivo, a lo largo del presente año, se ha llevado a cabo el proyecto de implantación de una arquitectura orientada a servicios basada en el producto TrustedX Web Services de Safelayer. El trabajo ha sido ejecutado por la Unidad de Seguridad Informática del Departamento de Sistemas de Información y Procesos de la entidad, con la colaboración de Indra.

electrónica y cifrado de correo electrónico y documentos ofimáticos.

Por otra parte, debido a la relación del BDE con diversidad de entidades externas, se incluyó en el alcance del proyecto la configuración de la Autoridad de Validación (VA, Validation Authority) de la PKI para informar también sobre el estado de los certificados de Prestadores de Servicios de Certificación (PSCs) como CERES-FNMT y el DNI electrónico; además se definió una Política de Certificación que instrumentaba la emisión de certificados para usuarios externos, exclusivamente para sus relaciones con el Banco.

La necesidad de dotar al Banco de España (BDE) de un sistema informático capaz de emitir certificados electrónicos basados en tarjeta criptográfica para sus usuarios internos, llevó a esta entidad a implantar una Infraestructura de Clave Pública corporativa durante el año 2004.

Como objetivos de dicho proyecto, que se denominó PKIBDE, además de la emisión de 3 certificados por usuario (para autenticación, firma electrónica y cifrado, respectivamente) se incluyeron funcionalidades básicas fundamentadas en la tarjeta como el inicio de sesión en el puesto de trabajo, el acceso remoto a la red utilizando dicho dispositivo, y la firma

Sin embargo, ya en las fases preliminares del proyecto, se intuyó la necesidad de facilitar la integración con la PKI a las aplicaciones informáticas desarrolladas ad hoc en el BDE. Era necesario que tareas requeridas por muchas de ellas como firmar electrónicamente un formulario en el puesto del usuario, verificar una firma o validar y extraer información de un certificado, no fueran complejas. Se pretendía evitar a las aplicaciones tener que lidiar con las estructuras de datos y protocolos específicos de la tecnología de clave pública, como X.509, CMS/PKCS#7, SMIME, OCSP, XAdES, XML/DSIG, etc. A esto se unió la creciente demanda por parte de los departamentos verticales del



Banco de un canal web que incluyera firma electrónica y autenticación basada en certificados, por medio del cual se pudieran ofrecer servicios en Internet. Todo ello llevó a los responsables de Seguridad Informática del BDE a iniciar una segunda fase del proyecto PKIBDE que diera solución a dichas necesidades.

requisitos a cubrir por el nuevo proyecto

En el Banco de España, como ocurre en gran número de organizaciones, existe una gran variedad de entornos tecnológicos (IBM z/OS, Microsoft Windows, IBM AIX,...), con diversas arquitecturas de ejecución de aplicaciones (COBOL/DB2, .NET, J2EE,...). Además, dichas aplicaciones pueden ejecutarse tanto en la intranet del BDE como en las redes perimetrales de acceso a las diversas redes de área extensa con las que existe conexión (Internet, SwiftNet, Intranet Administrativa,...)

Por tanto, en el estudio previo que se llevó a cabo, se determinó que la integración con PKI no podía orientarse a desarrollos particulares para cada plataforma susceptible de requerir funcionalidades de clave pública a corto o medio plazo. Más bien había que buscar una solución global con visibilidad a largo plazo, fundamentada en una Arquitectura Orientada a Servicios (Service-Oriented Architecture, o SOA) tan en boga en la actualidad.

Los requisitos fundamentales que se pretendían cubrir por la plataforma a desplegar en esta segunda fase eran los siguientes:

- Firma electrónica en el puesto cliente para entornos web en formato CMS/PKCS#7, con capacidad de elección transparente para el usuario del certificado a utilizar.
- Validación de certificados emitidos por PSC externos.
- Recolección de la información contenida en los certificados (ej.: DNI, nombre, apellidos, etc.), independientemente del PSC.
- Verificación de firma electrónica en formato CMS/PKCS7.

Además, existían otros requisitos que se pretendían cubrir, pero cuya prioridad no era tan alta como la de los anteriores:

- Verificación de firma electrónica en otros formatos (XAdES, XMLDSIG, PDF, SMIME,...)
- Diferenciación por aplicación de los PSC y tipos de certificados aceptados.

Por último, se quiso aprovechar el trabajo para cubrir una necesidad que, si bien no estaba directamente relacionada con la integración de las aplicaciones con la PKI, era de importancia en el marco global de dicha infraestructura:

- Desarrollo de una aplicación de Internet a través de la cual las enti-

dades externas pudieran solicitar un certificado a PKIBDE, exclusivamente para sus relaciones con el Banco.

Dada la envergadura del nuevo proyecto, se decidió llevar a cabo una licitación, resultando adjudicataria la empresa Indra Sistemas.

servicios infraestructurales de PKI

La solución implantada por Indra se ha basado en la plataforma TrustedX® WS de Safelayer. TrustedX es una plataforma diseñada para permitir la integración rápida y eficiente de servicios de seguridad (autenticación, firma electrónica y protección de datos) en las aplicaciones. Su arquitectura orientada a servicios (SOA) garantiza mayor flexibilidad y adaptabilidad a la vez que mantiene las propiedades de escalabilidad, alta disponibilidad y la facilidad de gestión necesarias en los procesos críticos de negocio. Un análisis más detallado del producto puede consultarse en el número 70 de esta publicación en su apartado de Laboratorio.

La plataforma TrustedX® WS requiere un conjunto de componentes mínimos que constituyen el sistema común de gestión (configuración, monitorización y

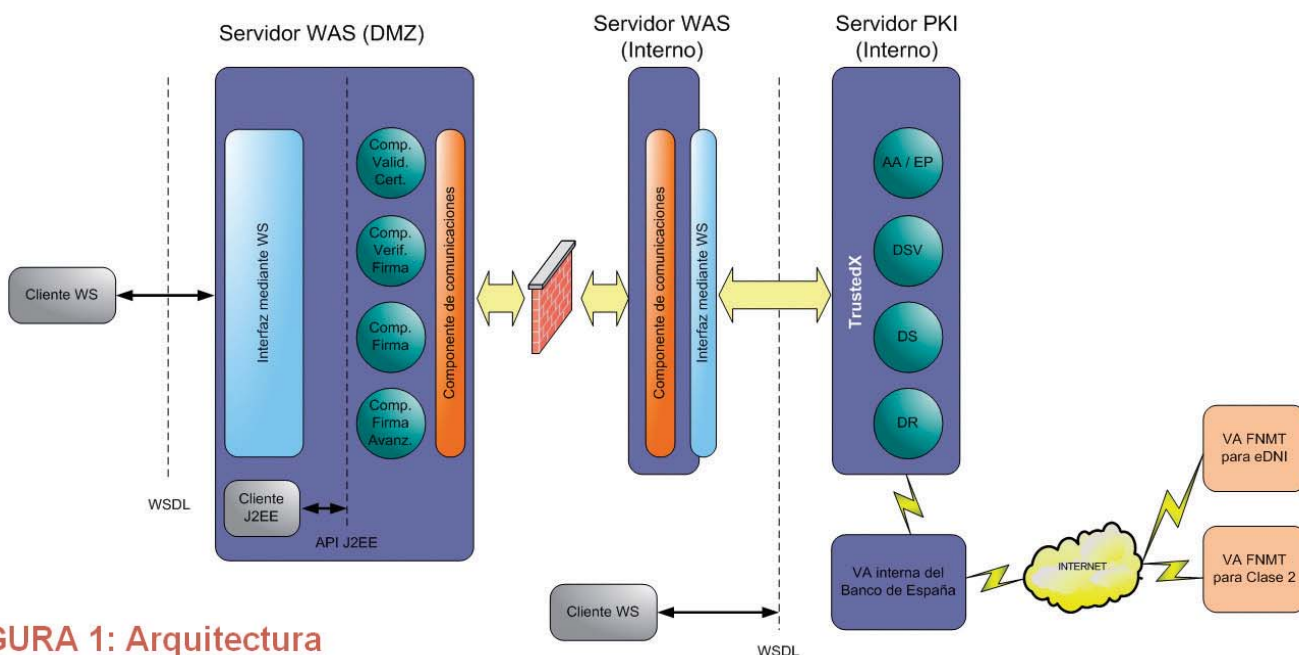


FIGURA 1: Arquitectura

control de acceso de cada componente de servicio) y un conjunto de componentes de servicio que son opcionales y que suministran los servicios de seguridad PKI y de firma electrónica. En el proceso de implantación llevado a cabo en el Banco de España se ha procedido a la configuración y despliegue de los siguientes módulos:

- **TrustedX® WS Authentication & Authorization (TWS-AA).** Servicio de Autenticación y Autorización con mecanismos basados en login/password y certificado digital (TLS/SSL), o a través de WS-Security (tokens seguros en mensajes SOAP).
- **TrustedX® WS Entity Profiler (TWS-EP).** Servicio de gestión de información que uniformiza perfiles de objetos y/o entidades: usuarios, aplicaciones, servicios web, políticas, certificados, logs/auditoría, etc.
- **TrustedX® WS Digital Signature Verification (TWS-DSV).** Servicio de verificación de firmas electrónicas (incluidas firmas avanzadas o longevas) independiente del prestador, del mecanismo de verificación de certificados y del formato de firma.

El proceso de implantación de la solución final se ha desarrollado en dos líneas de actuación diferenciadas. Por una parte ha sido necesario un análisis de las necesidades del Banco de España para una correcta definición de los diferentes componentes de TrustedX. Pero por otra parte, ha sido necesario analizar el mecanismo de acceso de las aplicaciones a los servicios proporcionados por la plataforma, debido a la arquitectura definitiva de implantación.

TWS proporciona una gran variedad de mecanismos de autenticación, desde los anónimos o basados en usuario y contraseña, como basados en SSL/TLS o firma digital, bien de manera directa o mediante la utilización de agentes. Concretamente, debido a los condicionantes de la arquitectura de los servidores alojados en la DMZ de Internet, se ha desarrollado un agente de tipo autoritativo, que se encargará de gestionar la autenticación de las aplicaciones ante TWS.

Los recursos de validación y verificación de TrustedX son proporcionados mediante servicios web. Para facilitar a las aplicaciones el consumo de los mismos, de forma que no necesiten preocuparse del canal de comunicaciones específico empleado, Indra ha proporcionado un interfaz J2EE que encapsula los diferentes tipos de peticiones posibles, abstrayéndose del canal.

En el estudio previo se determinó que la integración con PKI no podía orientarse a desarrollos particulares para cada plataforma susceptible de requerir funcionalidades de clave pública a corto o medio plazo

Por otra parte, se ha estimado conveniente establecer un interfaz de servicios web en la propia DMZ para su utilización por parte de los elementos de infraestructura existentes en dicha red, que así lo requieran.

configuración y despliegue de la plataforma

El primer paso para la configuración y despliegue de TWS es identificar claramente los posibles actores que intervienen. Básicamente, la plataforma se sustenta en la definición de tres pilares. Por una parte **las entidades usuarias**, i.e., las entidades que van a consumir los servicios proporcionados. Por otro lado **las entidades de confianza**, esto es, aquellas entidades que forman parte de una infraestructura de clave pública (CAs, VAs y TSAs). Por último, ambos tipos de entidades se interrelacionan mediante **políticas y reglas**, que a su

vez pueden estructurarse en políticas de autenticación, de autorización, de contabilidad, de firma digital y de cifrado.

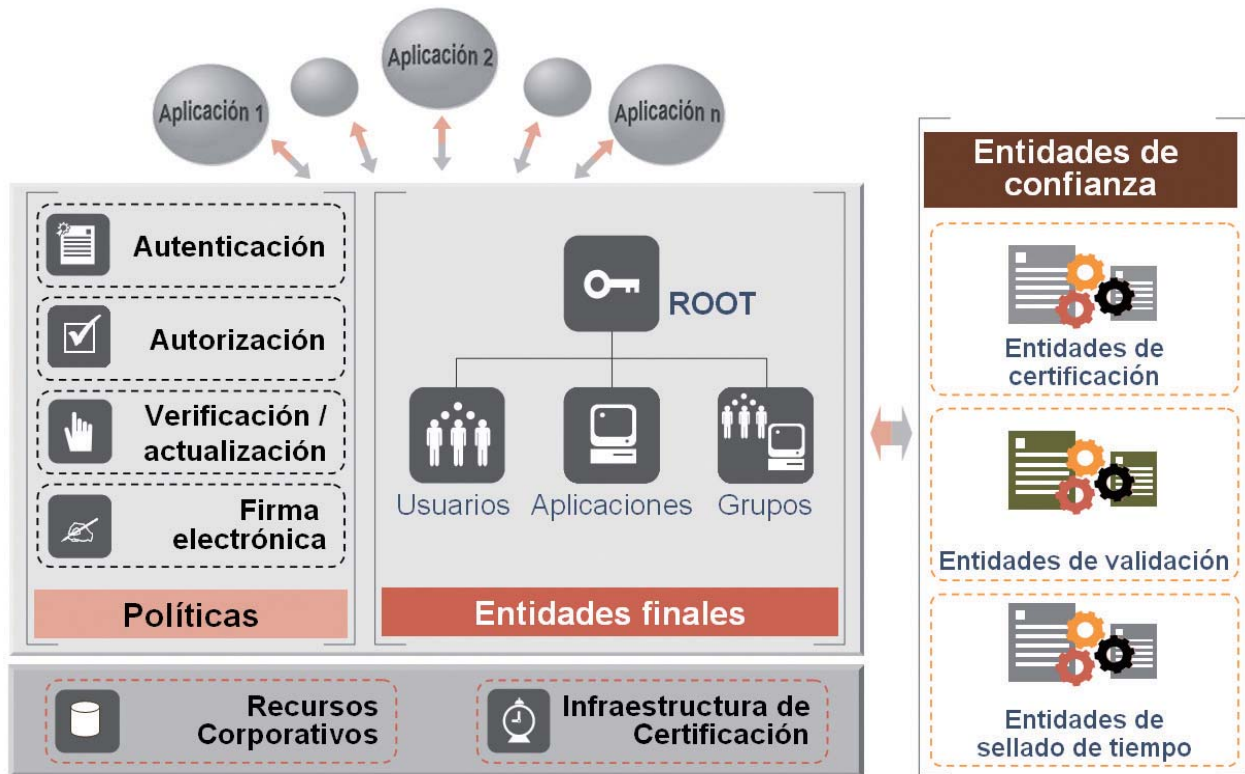
Dentro del Banco de España, las entidades usuarias no han sido lo que se entiende normalmente como usuarios, sino las aplicaciones. Se pretendía que las diferentes aplicaciones pudieran diferenciarse en cuanto a los PSC y certificados que pueden utilizar, por lo que se ha realizado una primera clasificación y agrupación de las mismas en **grupos de aplicaciones** según dicho criterio.

A la hora de definir las **entidades de confianza**, el Banco de España, en su despliegue inicial ha aceptado dentro de su plataforma la utilización de certificados de CERES-FNMT, tanto de persona física como jurídica, certificados emitidos por su propia Autoridad de Certificación (CA) corporativa, así como el DNI electrónico. Dentro de las entidades de confianza se recogen también las Autoridades de Validación (VA) que se van a emplear, configurándose para ello la propia VA del Banco de España y las de la FNMT y el Ministerio de Administraciones Públicas para la validación del DNI electrónico.

Una vez definidas las diferentes entidades se ha procedido al análisis de las necesidades de validación y verificación de certificados y firmas por parte de las aplicaciones. TWS soporta diferentes formatos de firma, estructurados en base a perfiles, uno de los cuales es el de validación de estado de un certificado. El mecanismo para lograr que diferentes entidades (o grupos de ellas) accedan a los mismos servicios básicos, aunque discriminando por tipo de certificado se ha logrado mediante una adecuada definición de reglas y políticas de validación y verificación.

A nivel de regla, se permite definir las CA permitidas en la aplicación de la regla, los mecanismos de validación que se prefieren para la misma, y el formato de la información de respuesta que se desea. Así por ejemplo, mientras que los certificados de CERES-FNMT y del DNI se van a validar mediante el uso de VA exclusivamente, los certificados corporativos se evaluarán en primera instancia contra CRL, y en segunda instancia contra la VA corporativa.

FIGURA 2: Elementos arquitecturales TWS



También a nivel de regla se especifica el formato de salida de la información. Una de las tareas más tediosas a la hora de manejar certificados es la multitud de posibilidades a tener en cuenta en función del PSC manejado. Diferentes extensiones, políticas, formatos... hacen que una aplicación que desee manejar un nuevo tipo de certificados deba invertir mucho tiempo y esfuerzo en adaptarse. TrustedX solventa de una manera elegante este inconveniente mediante el uso de **plantillas de estilo** XSLT. Básicamente existen plantillas para formatear la información contenida en el certificado, CRL, respuestas OCSP y sellos de tiempo. Adicionalmente permite definir plantillas de información adicional que aglutinen toda la información necesaria. En el caso del Banco de España, se ha procedido a la creación de una plantilla para cada tipo de PSC, de forma que sea capaz de cumplimentar una ficha común de datos para las aplicaciones, tomando la información de diferentes atributos o extensiones según el PSC. De esta forma, una aplicación siempre manejará un XML idéntico de salida, independientemente del tipo de certificado.

Una vez definidas las reglas se ha procedido a su agrupación en diferentes políticas basándose en los criterios manifestados por el Banco de España.

Una vez definidos tanto los actores como las diferentes reglas, queda enlazarlas de forma que el resultado sea el deseado, esto es, que a una determinada aplicación, una vez **autenticada** se le **autorice**, en base principalmente a su pertenencia a grupos, a consumir determinados recursos, aplicándole la política adecuada. Es decir, se han definido una serie de reglas de autorización por medio de las cuales se autoriza a una determinada aplicación a que aplique una determinada política de validación o verificación.

La labor principal de Indra Sistemas ha consistido por tanto en el diseño de un adecuado mapa de políticas y reglas que permitan dar los servicios necesarios en la actualidad, y que permita el crecimiento y evolución de la plataforma según surjan nuevas necesidades, ya sea incorporando nuevos componentes de servicio (TWS-DS para funcionalidad de firma en servidor, TWS-DR para imple-

mentar el no repudio, etc.), ya sea incorporando nuevos PSC con nuevos requerimientos. La flexibilidad, escalabilidad, facilidad de integración y sencillez de la plataforma TrustedX® WS proporcionan la seguridad de disponer de los mimbres necesarios para un adecuado crecimiento de los servicios infraestructurales relacionados con PKI desplegados por el Banco de España.

Conclusiones

Mediante el despliegue e integración de los TrustedX® de Safelayer en la segunda fase del proyecto PKIBDE, el Banco de España ha cubierto las necesidades de firma electrónica y gestión de certificados más demandadas por sus aplicaciones corporativas, evitando recurrir a soluciones de corto plazo.

Se ha apostado por una arquitectura basada en Web Services, con capacidades de escalabilidad tanto de recursos como de servicios, de modo que añadir nuevas funcionalidades como, por ejemplo, firma longeva o cifrado centralizado, no sea traumático para la infraestructura desplegada. ●