2151

GOBIERNO DE MENDOZA

SECRETARÍA ADMINISTRATIVA LEGAL Y TÉCNICA

UNIDAD DE REFORMA DEL ESTADO

46 902

firma Digital

Informe Final

CONSEJO FEDERAL DE INVERSIONES

CONSULTOR: LIC. PABLO GUILLERMO LIOY

Fecha de impresión 28/02/2008 8:58

ÍNDICE

I. Resumen de Contenidos

Se presentan a continuación, a modo de Informe Final, las actividades y tareas desarrolladas en el marco de planificación del proyecto de Firma Digital Mendoza.

Los contenidos ya presentados en informes anteriores se incluyen resumidos y sintetizados por importancia, para obtener una versión más detallada de los temas por favor remitirse a los informes precedentes.

El resumen de las actividades realizadas es el siguiente:

1. **Participación en el proceso de Reglamentación de la Ley 7234:**
   - Se analizarán nuevas normativas nacionales e internacionales relacionadas.
   - Se emprenderán acciones en pos de concientizar a la conducción política sobre la importancia de la firma y publicación del decreto reglamentario, a fin de completar el marco legal de aplicación de la firma digital en el ámbito provincial.

2. **Identificación y diseño de experiencia A de firma o timbre digital**
   - Identificación de la necesidad: se recopila y analiza información sobre el problema, se entrevista a los posibles usuarios y se precisa la necesidad de aplicación de tecnología.
   - Análisis del sistema: se releva el circuito actual, y se define el alcance de la experiencia.
   - Diseño de la implementación: se elabora el diseño conceptual de la experiencia.

3. **Identificación y diseño de experiencia B de firma o timbre digital**

- Identificación de la necesidad: se recopila y analiza información sobre el problema, se entrevista a los posibles usuarios y se precisa la necesidad de aplicación de tecnología.
- Análisis del sistema: se releva los circuitos actuales de comunicaciones oficiales por email, y se define el alcance de la experiencia.
- Diseño de la implementación: se elabora el diseño conceptual de la experiencia.

4. **Implementación de experiencia A:**

- Desarrollo e implementación: se lleva a la práctica la experiencia piloto real. Se emiten los certificados de firma digital, se realizan las configuraciones, instalación de protocolos, ajustes y desarrollos necesarios en el equipamiento informático
- Puesta en Marcha de la implementación: el sistema existente se reemplaza por el nuevo mejorado y se capacita a los usuarios.
- Evaluación de la experiencia: se definen métricas de evaluación que a futuro permitirán evaluar el éxito de la implementación

5. **Implementación de experiencia B:**

- Desarrollo e implementación: se lleva a la práctica la experiencia piloto real. Se emiten los certificados de firma digital, se realizan las configuraciones en los servidores y clientes de correo electrónico, se realizan las adecuaciones necesarias en la plataforma tecnológica de los usuarios y se los asiste en la instalación y manipulación de sus Certificados Digitales.
- Puesta en Marcha de la implementación: se capacita a los usuarios en el uso de correo electrónico seguro y en los procedimientos a seguir para la emisión y verificación de e-mail seguro, se provee mate-

rial de consulta y se instrumentan mecanismos ágiles de asistencia técnica permanente.

- Evaluación de la experiencia: se definen métricas de evaluación que a futuro permitirán evaluar el éxito de la implementación

Los nuevos contenidos correspondientes a lo planificado para el informe final se refieren a la actividad 5 y se presentan a los 10 meses de iniciadas las tareas.

De esta manera se cumple con las actividades propuestas para el proyecto y con los objetivos planteados:

Objetivo estratégico

El principal objetivo de nuestro proyecto es difundir y promover el uso de la tecnología de firma digital.

Con ello, se espera facilitar el desarrollo de proyectos reales de teleadministración y de experiencias que agilicen y despapelicen multitud de tramitaciones internas de la Administración Pública de la Provincia.

Objetivos específicos:

- Fortalecer y expandir las aplicaciones de Firma Digital implementadas.
- Consolidar el uso de timbre digital en procesos de certificación.
- Introducir el uso de la firma digital en las comunicaciones internas
- Contribuir al fortalecimiento del marco normativo de Firma Digital en el contexto provincial.
- Realizar 2 nuevas implementaciones tecnológicas de Firma o Timbre Digital

II. Participación en el proceso de Reglamentación de la Ley 7234:

El objeto de este apartado es el de proveer a las dependencias legales de la Gobernación de la Provincia de las últimas normas en materia de Firma Digital a nivel Nacional e Internacional que afecten directa o indirectamente la Legislación Provincial y que deban tomarse al menos como referencia para la creación de normativa local.

En esta oportunidad presentamos y comentamos en una reunión con el equipo de la asesoría legal de la Secretaría Administrativa Legal y Técnica un proyecto de Ley que nos pareció muy interesante sobre la creación del servicio nacional de estampado de fecha y hora por Internet, a cargo del observatorio buenos aires del servicio de hidrografía naval.

Dicho Proyecto de ley ha sido ingresado a la Cámara de Diputados de la Nación Argentina con fecha 1 de septiembre del corriente año y fue elaborado por el Grupo Firma Digital Tucumán integrado: por las Universidades del Norte Santo Tomás de Aquino, Nacional de Tucumán y Tecnológica Nacional Facultad Regional Tucumán, por el Consejo Profesional de la Ingeniería, el Colegio de Graduados en Ciencias Económicas y la empresa proveedora de Internet Jet Net, todos de Tucumán; donde crea la "certificación de fecha y hora para los documentos enviados por Internet".

A continuación transcribimos la norma tomada de:

http://www.firmadigitaltucuman.com.ar/Leyes/Proyecto%20de%20Ley%20Time%20Stamping.pdf

PROYECTO DE LEY

Texto facilitado por los firmantes del proyecto. Debe tenerse en cuenta que solamente podrá ser tenido por auténtico el texto publicado en el respectivo Trámite Parlamentario, editado por la Imprenta del Congreso de la Nación.

Nº de Expediente 4991-D-2006

Trámite Parlamentario 122

Art. 1º.- Creación. Créase con carácter exclusivo el "Servicio Nacional de Estampado de fecha y hora por Internet" a cargo del Observatorio Buenos Aires del Servicio de Hidrografía Naval.

Art. 2º.- Modalidad de prestación del servicio. El Servicio Nacional de Estampado de fecha y hora por Internet se prestará con carácter gratuito y en general, a través de la emisión de la fecha y hora por medio de un sitio tecnológicamente seguro de acuerdo a los estándares más actualizados de la tecnología de seguridad.

Art. 3º.- Solicitud de particulares. Emisión de certificados. Los particulares que requieran el estampado de fecha y hora oficial en documentos electrónicos lo solicitarán por medios informáticos al Servicio Nacional de Estampado de fecha y hora por Internet, el que emitirá un certificado digital de acuerdo a las condiciones del Capítulo II de la Ley 25.506, sus Decretos Reglamentarios y disposiciones de la autoridad de aplicación.

Art. 4º.- Licencia como certificador. Para cumplir con las prestaciones del artículo anterior, el Servicio Nacional de Hidrografía Naval deberá obtener licenciamiento como certificador según lo dispuesto en el Capítulo III de la ley 25.506, sus Decretos

Reglamentarios y disposiciones de la autoridad de aplicación.

Art. 5º.- Otros servicios de seguridad. Prestación. El Servicio Nacional de Estampado de fecha y hora por Internet podrá prestar cualquier otro tipo servicios de seguridad a los documentos electrónicos, que sean permitidos por

la Ley 25.506, sus Decretos Reglamentarios y disposiciones de la autoridad de aplicación.

Art. 6º.- Medidas transitorias. Facúltase al Poder Ejecutivo Nacional para disponer medidas transitorias que garanticen la prestación de este servicio conforme a los artículos anteriores, hasta tanto del Servicio de Hidrografía Naval obtenga el licenciamiento de ley.

Art. 7º.- Comuníquese al Poder Ejecutivo.

III. Identificación y diseño de experiencia A de firma o timbre digital

A) Relevamiento del circuito actual e identificación de la necesidad

PROCEDIMIENTO DE SOLICITUD/ENTREGA DE CERTIFICADO DE VIGENCIA

IV.

Introducción:

El procedimiento de solicitud/entrega del certificado de vigencia debe entenderse como una de las principales constancias que otorga la Dirección de Personas Jurídicas.

El procedimiento se puede esquematizar en las siguientes etapas:

Secuencia Sintética del Proceso
(Forma arrow chart)

Etapas

Principal sector interviniente

Objetivo:

Existe un volumen alto de solicitudes de certificados de vigencia que requieren nuevos procedimientos que aseguren la correcta valuación y registración a través de herramientas informáticas de última generación, que garanticen la transparencia y seguridad de la información que se maneje. Por otro lado se persigue descongestionar los mostradores de la repartición logrando un procedimiento totalmente digitalizado que no requiera la presencia física del solicitante.

Alcance:

El procedimiento es operativo para la Dirección de Personas Jurídicas de la Provincia de Mendoza.

Referencias:

Para la correcta redacción y relevamiento del procedimiento se han desarrollado las siguientes actividades:

- Entrevistas con el Jefe de la Secretaría Administrativa Lic. Alberto Cruz.
- Entrevistas con el empleado de Atención al público el Sr Emiliano Gutierrez.
- Consulta de normativa legal vigente.

Procedimiento:

1. ***SOLICITANTE:*** presenta nota de solicitud firmada por duplicado (Registro A) acompañada del comprobante de la tasa retributiva de servicios correspondiente (Registro B) a Mesa de Entradas de la Dirección de Personas Jurídicas.

2. ***MESA DE ENTRADAS:*** recibe, numera y sella la nota de solicitud. Devuelve el duplicado al solicitante y el original lo remite a la Secretaría Administrativa.

3. ***SECRETARIA ADMINISTRATIVA:*** recibe el original de la nota de solicitud, procede a darle ingreso en el programa de registración interno, realiza las consultas necesarias y emite el certificado de vigencia (Anexo A).

4. ***DIRECCIÓN:*** recibe, firma, sella el certificado de vigencia y luego lo devuelve a Secretaría Administrativa.

5. ***SECRETARIA AMINISTRATIVA:*** controla y envía el certificado a mesa de entradas para ser retirado por el solicitante dentro de las 48 horas hábiles desde la recepción de la solicitud.

Registros:

A) Datos que debe contener la Nota de Solicitud:

- Nombre de la Entidad solicitante
- Domicilio
- Nombre y Apellido del firmante
- Cargo en la Entidad
- Detalle:
  - número de Personería
  - número de legajo Interno
  - balances presentados
  - nómina de autoridades

B) Tasa retributiva de servicios

- Código 476: Sociedades Anónimas $80
- Código 489: Asociaciones Civiles $15
- Código 497: Fundaciones $45

Adjuntos o anexos

A) MODELO DE CERTIFICADO DE VIGENCIA

CERTIFICOque la entidad "xxxxxxxxxxxxxxxxxxxxx", obtuvo su autorización para funcionar como persona jurídica por Resolución n° xxx del xx de xxxxxx del xxxx de ésta Dirección, encontrándose vigente a la fecha. Su legajo interno es el n° xxxxx. El último balance presentado es al 31 de diciembre del xxxx. El presente certificado se expide a solicitud de la interesada para ser presentado ante las autoridades que lo requieran, en Mendoza a los xx días des mes de xxxxxx del año xxxx.

Lic. Pablo Guillermo Lioy

"Firma Digital"

B) Análisis del Sistema

De acuerdo con la identificación de la necesidad y el relevamiento se han completado en esta etapa las tareas de especificación y documentación de diseño global y detallado, para la implantación del trámite de emisión on-line, del Certificado de Vigencia emitido por la Dirección Provincial de Personas Jurídicas para entidades que solicitan una certificación fehaciente del estado de su inscripción.

La documentación de diseño incluye una fase de diseño global, en la cuál se describen genéricamente las características funcionales que deberá proveer la aplicación, de forma de garantizar el cumplimiento de los requerimientos determinados en etapa de relevamiento y análisis. Complementariamente, el diseño detallado determina explícitamente los mecanismos mediante los cuáles deberán ser implementadas las aplicaciones del nuevo sistema, con detalle de la arquitectura y plataforma tecnológica que deberá soportar el desarrollo, el diseño de interfaces, el modelo de datos (entradas, procesos internos, salidas, mecanismos de control y verificación, otros) y las especificaciones detalladas en términos de obtención de Certificados de Firma Digital y generación del timbre.

Es importante mencionar que los criterios de diseño adoptados, parten de un conocimiento amplio de los enfoques que han tenido éxito en implementaciones previas de la tecnología de timbre digital, y firma digital en general.

Diseño Global

Descripción general de la solución propuesta

La solución debe comprender mecanismos que permitan el procesamiento de las solicitudes de Certificados de Vigencia cursadas por responsables acreditados de entidades registradas en la Dirección de Personas Jurídicas. Dichas solicitudes son remitidas a través de formularios html dispuestos en la Guía de Trámites de la Provincia, cuyos datos relevantes son almacenados de manera persistente en una base de datos dispuesta a tal fin.

El procesamiento de solicitudes incluye los siguientes pasos:

Consulta de solicitudes pendientes: como paso inicial del proceso, los responsables de la administración del procedimiento (personal asignado de la Dirección de Personas Jurídicas) deberán poder obtener de la aplicación, el reporte de solicitudes pendientes de atención. En dicha consulta, deberá constar para cada solicitud pendiente, el conjunto de datos que permita identificar unívocamente el pedido, la entidad involucrada, el responsable que cursa la solicitud y el detalle de datos a Certificar.

Decisión de Emisión/Rechazo: Para cada solicitud pendiente, los funcionarios responsables deberán ejecutar un proceso manual, basado en la información provista en la solicitud, más la que consta en los libros de inscripciones. Dicho proceso permitirá determinar la pertinencia o no de la emisión del Certificado de Vigencia, en función de lo cuál activarán en el sistema el proceso de Emisión o Rechazo respectivamente.

Emisión: En caso de que la decisión fuera positiva respecto de la solicitud, el sistema deberá emitir automáticamente el Certificado de Vigencia, timbrado digitalmente con detalle de los datos solicitados, tales como fecha de presentación del último balance o detalle de la constitución del Directorio.

Deberán proveerse los mecanismos para la comunicación y envío automático del Certificado al solicitante acreditado.

Rechazo: En caso de que la decisión fuera negativa respecto de la solicitud, el sistema deberá emitir automáticamente la comunicación de rechazo con detalle de los motivos que justifican la decisión.

Almacenamiento: El sistema deberá permitir el almacenamiento temporal de los Certificados de Vigencia emitidos, por un período de 90 días a partir de la fecha de emisión.

Especificaciones Generales de Diseño

Se documentan en esta sección, los criterios básicos de diseño que deben ser respetados tendientes a reducir la complejidad y la cantidad de excepciones del sistema.

1. Arquitectura Web: con la finalidad de mantener una interfaz abierta con la Guía de Trámites, reducir la complejidad de instalación y mantenimiento; y aprovechar las ventajas de esta arquitectura distribuida se deberá implementar la solución basada en arquitectura cliente-servidor para la web.

2. Interfaz Amigable - Usabilidad: deberán contemplarse de manera prioritaria todas aquellas condiciones que garanticen la facilidad de uso de la aplicación y la correcta comprensión de cada una de las funcionalidades de la misma, tanto por parte de los operadores capacitados como por parte de los usuarios finales. A tal fin, se requiere como mínimo: ayuda en línea sobre todos los aspectos del sistema, uso de simbología estándar, etiquetado de todas las entradas y salidas, secuenciación de pasos, alertas permanen-

tes sobre acciones relevantes, jerarquización de la información más relevante en las pantallas, separación de contenidos por grupos de contenidos relevantes, manejo uniforme de criterios de diseño y utilización de colores.

3. Control de Errores por Excepción: la lógica de control y procesamiento de errores deberá estar totalmente separada de la lógica de proceso de la aplicación, por lo cuál se sugiere la estructuración basada en excepciones.

4. Seguimiento y Verificabilidad: Todas las actividades realizadas en el sistema, en torno de una solicitud, deberán ser logeadas temporalmente por el Application Server de modo de poder obtener una traza completa de las actividades realizadas.

5. Portabilidad y Escalabilidad: Las decisiones de diseño detallado que se adopten, deberán contemplar de manera prioritaria la portabilidad y futura escalabilidad de la aplicación.

6. Ajuste a estándares: El diseño detallado deberá garantizar el ajuste a estándares en materia de firma digital y certificados digitales. Los estándares y algoritmos utilizados en la solución deberán estar debidamente consignados en las especificaciones de diseño.

7. Seguridad: Se deberán incluir todos los procedimientos que resulten necesarios para garantizar la seguridad en el acceso a las fuentes de datos, así como también a los Certificados de Firma Digital implicados en el proceso.

Entradas planeadas

El proceso de emisión de Certificados tendrá como fuentes de datos:

a. Consulta a Base de Datos de Solicitudes Pendientes: recordset con los resultados de una consulta sin filtro al modelo de datos del sistema.

La estructura genérica de esta consulta proveerá datos sobre: el total de solicitudes pendientes de atención, junto a los datos detallados que permitan individualizar cada solicitud para la toma de decisiones en los procesos de emisión o rechazo.

b. Detalle de datos ingresados manualmente: datos provistos en línea por los operadores, en el momento de emisión del Certificado.

Procesos Internos

Se describen a continuación los métodos y procedimientos de procesamiento de datos, que producirán las salidas deseadas para la solución, dadas ciertas entradas y archivos de datos.

a. Consulta de Solicitudes Pendientes:

Deberá estar diseñado sobre una interfaz web que permita la conexión dinámica a la base de solicitudes pendientes, y muestre el detalle de las mismas, a fin de que los funcionarios competentes puedan decidir sobre la pertinencia de emisión o rechazo del Certificado.

Los datos críticos a consignar sobre cada solicitud pendiente deberán ser como mínimo:

- Fecha del pedido
- Datos de identificación de la Entidad
- Datos de identificación del Solicitante
- Detalle de datos complementarios a Certificar (Balances, Nómina, Directorio, Presentación de Libros, etc.).

b. Proceso de Emisión de Certificado:

Para cada solicitud pendiente deberá darse la opción al operador de disparar el proceso automático de emisión del certificado o de manera contraria el proceso de rechazo del mismo.

La emisión de un Certificado implica la generación instantánea del Documento PDF timbrado digitalmente y su correspondiente envío por email al solicitante acreditado. Dicho proceso de emisión y envío, supone los siguientes subprocesos:

b.1. Subproceso de consignación de datos detallados: La emisión de un Certificado supone el ingreso de datos detallados que se obtienen de los libros presentados por las entidades. Una vez ordenada la emisión del Certificado por parte del operador, la aplicación deberá proveer una interfaz web para el ingreso y validación de dichos datos.

b.2. Subproceso de Firma Digital: Se firman digitalmente, por autoridad competente, los datos críticos a incluir en el Certificado. Dichos datos deberán permitir identificar unívocamente la transacción en el sistema, la entidad certificada y datos relevantes del solicitante responsable de la solicitud y recepción del Certificado.

b.3. Subproceso de Generación del Timbre: Este subproceso es el encargado de producir la nube de puntos PDF417 (timbre digital) con la in-

formación del texto firmado, su firma y la clave pública del firmante correctamente barcodeados.

b.4. Subproceso de Construcción del Documento en Formato PDF: El subproceso tomará como insumos la información a incluir en el Certificado, obtenida como parámetros de las fuentes de datos descriptas, y el timbre digital previamente generado sobre esta información. Con estos datos, deberá resolver la generación automática del documento .pdf que describe el Certificado de Vigencia con detalle de los datos pertinentes debidamente resaltados.

b.5. Subproceso de Notificación y Envío por e-mail del Certificado: El documento generado, deberá ser adjuntado al cuerpo de un mail de notificación y enviado instantáneamente a la cuenta de correo consignada por el solicitante, previamente verificada.

b.6. Subproceso de almacenamiento de Certificados: Deberá proveerse un mecanismo de almacenamiento del documento generado en el repositorio de Certificados por un período de 90 días.

c. Proceso de Rechazo de solicitudes:

En caso de no corresponder la emisión de un Certificado de Vigencia, el operador deberá contar con un procedimiento de comunicación del rechazo de la solicitud. El proceso de rechazo deberá contemplar el envío de un email a la cuenta de correo consignada en la solicitud, en cuyo cuerpo se informe sobre la improcedencia de la solicitud y los motivos que justifican el rechazo.

La confección y envío de dichas comunicaciones deberá ser resuelta automáticamente por parte de la aplicación, con parametrización del texto de justificaciones. Esto último además de agilizar los tiempos de respuesta, contribuye a evitar errores humanos en el envío de los correos.

d. Módulo de verificación de usuarios:

En todos los aspectos de su administración, la aplicación deberá proveer y monitorear un acceso restringido a usuarios. Esta implementación podrá estar solventada sobre una autenticación simple de login/password o sobre algún esquema de autenticación fuerte basado en Certificados Digitales, de acuerdo a como se considere más conveniente en etapa de diseño detallado.

Las funciones que podrán ser desarrolladas desde la interfaz de la aplicación no amerita en principio el diseño de un esquema de perfiles de acceso de usuarios con privilegios diferenciales.

Persistencia de datos

Se determinan en este punto de manera genérica, los repositorios de datos que será necesario mantener para garantizar la persistencia de la información relevante.

Base de Datos de Solicitudes Pendientes: estructura de información administrada concurrentemente por la aplicación de generación de solicitudes (implementada en la Guía de Trámites de la Provincia) y por la aplicación de Emisión de Certificados.

Repositorio de Certificados de Vigencia: los Certificados emitidos por la aplicación, debidamente timbrados, deberán ser mantenidos en este repositorio por un período de 90 días desde su fecha de emisión.

Logs de Transacciones: se deberán mantener archivos de seguimiento de las transacciones realizadas en el sistema, con detalle mensual.

Buzones de email: con fines de seguimiento y control deberán mantenerse los correos electrónicos enviados y recibidos por la aplicación por un período de 90 días.

Salidas Planeadas

Las salidas básicas que deberá proveer la aplicación contemplan:

- Certificados de Vigencia: documentos en formato .pdf con el cuerpo del certificado más el timbre digital correspondiente.
- Emails de notificación: de envío de certificado o rechazo del mismo
- Pantallas de notificación de secuencia: deberá informarse al operador sobre el estado de procesamiento de una transacción hasta el momento en que la misma se complete.
- Pantalla de notificación de errores: cualquier excepción producida en la aplicación que no pudiera ser resuelta por los manejadores de excepciones, deberá ser notificada al operador, con detalle de los motivos que la provocaron y referencia al soporte o ayuda al cuál deben contactarse para tomar las medidas correctivas pertinentes.

- Reportes de Certificados Emitidos: consulta al repositorio de Certificados Emitidos con detalle de los certificados emitidos en los últimos 90 días corridos y acceso a los documentos .pdf.

Diseño Detallado

Descripción General de Aplicaciones

El funcionamiento integral del sistema deberá soportarse sobre dos aplicaciones totalmente independientes, las cuáles operarán complementariamente en el circuito de emisión y verificación respectivamente.

a. Aplicación de emisión del Certificado de Vigencia: Aplicación dinámica para la web, basada en una arquitectura cliente-servidor que permite el procesamiento de las solicitudes de certificación y la emisión de los Certificados de Vigencia con aprobación de funcionarios competentes mediante timbre digital.

b. Aplicación de validación de Timbre Digital: aplicación standalone, que permite verificar la integridad y validez del timbre digital. El software toma la cadena de caracteres que ingresan desde el puerto de teclado conectado al scanner y reconstruye los caracteres de la firma, la clave pública y el texto en claro que se firmó. Hecho esto, provee estos datos junto al Certificado a un módulo de verificación de firma que valida la integridad de la firma en relación a los datos firmados, mostrando un mensaje final al funcionario sobre la validez o no del timbre incluido en el Certificado en cuestión.

Arquitectura y Plataforma Tecnológica

Para el desarrollo e implantación de las aplicaciones, se aprovechará la plataforma tecnológica utilizada en desarrollos previos de la tecnología de Timbre Digital. Esto, además de suponer un mayor aprovechamiento de la capacidad instalada, implica utilizar un conjunto de herramientas debidamente probadas en torno de implantaciones de Timbre Digital.

No obstante lo anterior, se proponen algunas actualizaciones sobre la plataforma Java y drivers JDBC a instalar del lado del servidor, de manera

de mantener actualizada la base tecnológica tanto de desarrollo como de producción.

Arquitectura de Servidor: del lado del servidor deberá instalarse una plataforma J2SDK 1.5 y un servidor de aplicaciones web JBOSS 4.0.1 o superior que permita la ejecución de servlets java.

Para la generación de los documentos .pdf y el codebar PDF417, se utilizará la API java iText ver. 1.5, instalada en el classpath de la aplicación. Alternativamente, para contemplar la posibilidad de generación de objetos de firma PKCS#7 deberá incorporarse al deploy del proyecto en el servidor el paquete BouncyCastle (http://www.bouncycastle.org).

Las aplicaciones deberán deployarse sobre el Application Server como un archivo empaquetado .ear, con su configuración expresada en documentos XML. Su configuración y parametrización debe permitir amplia portabilidad del software desarrollado sobre entornos Linux y/o Windows

Cabe recordar que tanto la plataforma java, como las librerías de clases y el application server requeridos en el servidor, son software de libre acceso.

Configuración del cliente: los clientes que se conecten a la aplicación, tanto desde la Intranet de Gobierno, como usuarios externos, sólo deberán necesitar un browser de Internet y Adobe Acrobat Reader 6.0 o superior.

Deberá excluirse del desarrollo la utilización de componentes activos que pudieran ser filtrados por configuraciones de seguridad de los browsers.

Selección del formato de los documentos Digitales

Debido a los buenos resultados obtenidos en experiencias previas y a los requerimientos especificados para este caso en particular, el desarrollo deberá generar los Certificados de Vigencia en formato PDF (Portable Document Format), dado que este formato constituye un estándar para la publicación de documentos en Internet, contribuye a la inalterabilidad de los do-

cumentos y además facilita la incorporación del código de barras PDF417 conteniendo el timbre digital.

Selección de los lenguajes de desarrollo

La programación deberá hacer uso de los siguientes lenguajes:

Servlets y Clases: Java (J2EE). El desarrollo deberá soportarse sobre servlets basados en J2EE. No se prevé en las especificaciones de diseño la utilización de tecnología de WebServices o JavaBeans.

Interface web: La interfase web del proyecto deberá sustentarse sobre código .jsp (Java Server Page) para la generación dinámica de código HTML/Javascript.

Librerías y paquetes de clases a utilizar

El lenguaje Java, nativamente orientado a objetos, explota al máximo la posibilidad de escalar su potencialidad con un sinnúmero de librerías de clases reutilizables, con propósitos específicos, proporcionadas gratuitamente por la comunidad de desarrolladores de java y en ocasiones por empresas u organismos que realizan desarrollos en esta línea. En particular el presente desarrollo con timbre digital deberá utilizar las siguientes librerías (APIs Java), cuyo propósito y características principales se describen a continuación:

API iText ver.1.5 o superior : iText es un proyecto Sourceforge mantenido por una comunidad abierta de desarrolladores de software libre. Es una librería de clases Java que permite la generación dinámica de documentos pdf totalmente compatibles con la PdfReference 1.6. Las clases provistas por iText son muy útiles para generar documentos de sólo lectura independientes de la plataforma que contentan texto, listas, tablas e imágenes. En nuestro caso particular, la utilizamos por las siguientes características:

- Describe objetos de alto nivel que permiten generar rápidamente los principales componentes de un documento pdf.

- Incorpora la posibilidad de manejar el contenido interno de documentos pdf a bajo nivel. Es decir manipular directamente el formato interno de los documentos generados.
- El código de los documentos pdf generados es altamente compatible con las especificaciones de la Adobe PdfReference 1.6. Esta especificación describe el formato interno de los documentos pdf.
- Incorpora una jerarquía de clases completamente dedicada a la generación de Codebar PDF417 con excelentes características de optimización de la imagen generada, posibilidades de customización muy amplias e incorporación del procedimiento MacroPdf417.
- Incorpora una jerarquía de clases completamente dedicada a la generación de firmas digitales sobre documentos pdf. Si bien esto no está estrictamente relacionado con la generación del timbre, es una característica fundamental a considerar en función del posible crecimiento de la aplicación.
- iText es especialmente útil en combinación con tecnología Java(TM) basada en Servlets, que como documentamos anteriormente es el esquema de servicio a implementar en el servidor elegido.
- Existe excelente documentación sobre la API y una comunidad de desarrollo muy activa con foros de consulta y documentación en permanentemente mantenimiento
- La librería cae dentro de la categoría de software libre y puede descargarse gratuitamente desde http://www.lowagie.com

- Paquete Java.Security: Dentro de la plataforma J2SDK 1.5.0 se incorpora el paquete de clases Java.Security. Este package describe clases que permiten manipular objetos de firmas digitales, Certificados, claves públicas y privadas, keystores, algoritmos de firma, etc. Es el conjunto nativo de clases que proporciona el lenguaje para la manipulación de firmas y certificados digitales. En particular, las especificaciones de diseño prevén la utilización de clases provistas en este paquete para generar, tomando un certificado X.509 v3, una firma SHA1withRSA representada en formato PKCS#1 (CodeBase64) que constituye la firma digital de los elementos de datos esenciales del Certificado. Esta firma deberá luego ser codificada en codebar PDF417 constituyendo así el timbre digital.
- Driver de Conexión JDBC: La conexión desde los módulos de la aplicación a la Base de Datos deberá resolverse mediante el Driver JDBC jdbcpostgresql 7.2 o superior. Dicho driver deberá manejar las cadenas de conexión a la base de datos con identificación de usuarios y claves de conexión. Así mismo, deberá parametrizarse la conexión para la selección de Charsets que permitan una interpretación correcta de cadenas alfabéticas con símbolos especiales del idioma español tales como ñ y letras acentuadas.

Determinación de niveles de Seguridad y Acceso al Sistema

El servlet de generación del Certificado deberá ser de acceso restringido a funcionarios autorizados de la Dirección Provincial de Personas Jurídicas. A tal efecto deberá proveerse en la interfase web un esquema de validación de login/password u otro mecanismo superior de identificación y otor-

gamiento de permisos. Complementariamente la aplicación deberá estar restringida en alcance a la Intranet de Gobierno.

La seguridad en la generación del Certificado deberá implementarse mediante la generación del timbre. El mismo garantizará la originalidad, integridad y autoría del documento.

El legítimo interés de los solicitantes en requerir un Certificado de Vigencia para la persona jurídica que representan será verificado mediante un circuito de verificación de email y el posterior envío automático, por parte de la aplicación del Certificado a la cuenta de correo debidamente registrada. Cualquier comunicación complementaria que el sistema desarrolle deberá ser remitida a la misma cuenta de correo electrónico.

La protección de los certificados está garantizada en el servidor de timbrado por los responsables de la Autoridad de Registro de la ONTI.

La aplicación de validación de timbres, instalada en las oficinas que así lo requieran, es de acceso exclusivo a usuarios con privilegios de administración u operación sobre el sistema, validados mediante esquemas de login-password.

Tolerancia a fallas y gestión de errores

Las fallas y errores que pueden producirse en tiempo de ejecución (por ej.: por problemas de conexión, caída del application server, ausencia de un reader, etc.) deberán gestionarse bajo el concepto de manejo de excepciones. Esto implica que el sistema genera una excepción ante un error o falla que es tratada por un manejador de excepciones especialmente diseñado para tratar este tipo de errores. De esta forma se separa el código de manejo de errores, del código que atiende a la lógica principal del desarrollo, facilitando su comprensión y mantenimiento posterior. Así mismo, un cuidadoso manejo de excepciones implica en nuestro desarrollo una mayor tole-

rancia a fallas, objetivo de diseño fundamental en un sistema que pretende estar on-line 24x7x365.

Fuentes de Datos

La base de datos de solicitudes pendientes deberá instalarse sobre el motor PostgreSql 7.3 o superior. Este motor se ejecuta en un equipo independiente del Application Server y es accedido concurrentemente por la aplicación de generación de solicitudes desarrollada en la Guía de Trámites de la Provincia.

La estructura de la base de datos deberá ajustarse al siguiente modelo:

Charset: windows-1252

Esquema: único

Vistas: ninguna

StoreProcedures y Triggers: ninguno

Funciones: ninguno

Usuario de conexión: consulta1

Lenguaje de Consulta: ajustarse a ANSI SQL

Condiciones de generación del timbre digital

Para que a partir de la lectura de los códigos generados se pueda reconstruir sin errores la firma digital de los datos timbrados, la generación del timbre digital cumple las siguientes condiciones técnicas:

Nivel de Corrección de Errores: para poder reconstruir la firma, aún cuando el código se haya deteriorado en parte es necesario mantener un determinado nivel de redundancia de datos. Dicho nivel debe ser optimizado, para que la redundancia introducida no degrade significativamente la capa-

cidad de almacenamiento de información del código. La clase BarcodePDF417 de la API iText, utilizada para generar el timbre posee un algoritmo que optimiza el nivel de corrección de errores aplicado, asignándolo dinámicamente entre 0 y 5 como lo prescribe el estándar, de acuerdo la longitud de los CodeWords. En particular el nivel se fija de acuerdo a la siguiente lógica:

```
if (lenCodewords < 41)
errorLevel = 2;
else if (lenCodewords < 161)
errorLevel = 3;
else if (lenCodewords < 321)
errorLevel = 4;
else
      errorLevel = 5;
```

Modo de Compactación: PDF417 soporta tres modos de compactación: alfanumérico, numérico y binario. Cada uno de estos modos es más eficiente que el resto en ciertos juegos de caracteres. La clase Barcode PDF417 utiliza un sistema de optimización que elige el modo de compactación más óptimo para el conjunto de caracteres que se está codificando.

Capacidad de codificación y representación de la firma: Un código de barras 2D PDF417 puede almacenar hasta 1.100 bytes en binario o 1.800 caracteres ASCII, por lo que la representación del timbre debe ser inferior a ese tamaño. Atendiendo esto, la el desarrollo debe contemplar las siguientes condiciones:

Excluir la posibilidad de representar la firma como un objeto PKCS#7[PKC93] debido a que el conjunto de bytes generados supera la densidad de información soportada por el timbre (3 Kbytes aprox.).

La firma digital, está avalada por una cadena de certificación. Los certificados digitales se emiten para los algoritmos asimétricos RSA[RSA78] y

DSS[Nat99] (con una clara preferencia por RSA). En función de lo anterior, la firma digital deberá ser representada por un identificador en ASCII (SHA1withRSA), el separador ASCII "-" y el valor de la firma RSA usando el estándar PKCS#1[KS98]. Esto último, por ser las formas más comunes de representar los valores por las aplicaciones y bibliotecas criptográficas.

La clave pública, contenida en la firma deberá representarse por un identificador del algoritmo en un código ASCII, seguido de los parámetros del algoritmo en un orden predefinido separados por el carácter ASCII "-".

El resto de datos incluidos en el timbre, se representarán en formato de texto en claro mediante código ASCII de una manera legible al ser humano.

De acuerdo a las consideraciones anteriores la representación interna de la información codificada en el timbre deberá ajustarse al siguiente formato:

<<Cadena de Datos firmados>> + <<inscripción obtenida como parámetro>> + "-" + <<fecha pedido obtenido como parámetro>> + "-" + <<transacción obtenido como parámetro>> + "-" + <<apellido y nombre del solicitante obtenido como parámetro>> + "-" + <<Nro. Documento del solicitante obtenido como parámetro>> + <<Cadena de firma codificada en CodeBase64 (PKCS#1)>> + <<Clave pública>>

La imagen del timbre generado deberá cumplir con las siguientes condiciones:

aspect ratio: 1:3 (relación de aspecto)

quiet zone: 1 cmt. (perímetro blanco)

c) Diseño de Implementación

Descripción general de la solución propuesta

La solución debe comprender mecanismos que permitan el procesamiento de las solicitudes de Certificados de Vigencia cursadas por responsables acreditados de entidades registradas en la Dirección de Personas Jurídicas. Dichas solicitudes son remitidas a través de formularios html dispuestos en la Guía de Trámites de la Provincia, cuyos datos relevantes son almacenados de manera persistente en una base de datos dispuesta a tal fin.

PROCEDIMIENTO DE SOLICITUD/ENTREGA DE CERTIFICADO DE VIGENCIA POR INTERNET

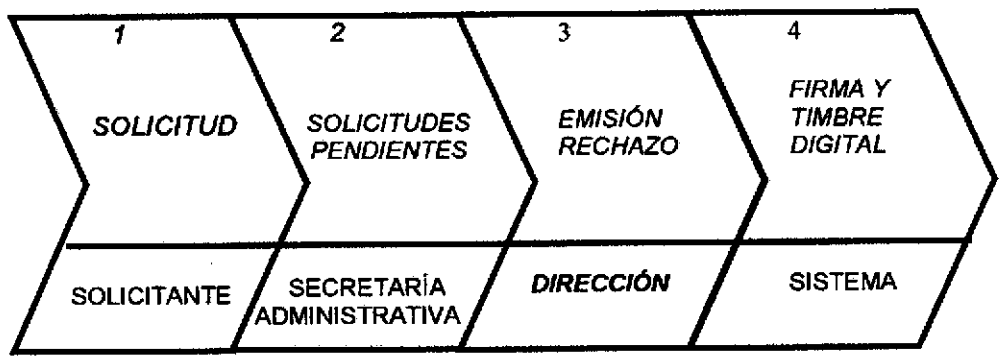
Introducción:

El procedimiento de solicitud/entrega del certificado de vigencia por Internet debe entenderse como una de las principales constancias que otorga la Dirección de Personas Jurídicas.

El procedimiento se puede esquematizar en las siguientes etapas:

Secuencia Sintética del Proceso
(Forma arrow chart)

Etapas



Principal sector interviniente

Objetivo:

Existe un volumen alto de solicitudes de certificados de vigencia que requieren nuevos procedimientos que aseguren la correcta valuación y registración a través de herramientas informáticas de última generación, que garanticen la transparencia y seguridad de la información que se maneje. Por otro lado se persigue descongestionar los mostradores de la repartición logrando un procedimiento totalmente digitalizado que no requiera la presencia física del solicitante.

Alcance:

El procedimiento por Internet se establece así operativo para la Dirección de Personas Jurídicas de la Provincia de Mendoza.

Referencias:

Para la correcta redacción del procedimiento se han desarrollado las siguientes actividades:

- Entrevistas con el Jefe de la Secretaría Administrativa Lic. Alberto Cruz.
- Entrevistas con el empleado de Atención al público el Sr Emiliano Gutierrez.
- Consulta de normativa legal vigente.

Procedimiento:

1. ***SOLICITANTE:*** ingresa a la Guía de Trámites y llena la solicitud (Registro A) indicando el número del comprobante de la tasa retributiva de servicios correspondiente (Registro B).

2. ***SECRETARIA ADMINISTRATIVA:*** consulta de solicitudes pendientes en el sistema de la aplicación y procede a darle ingreso en el programa de registración interno. En dicha consulta, deberá constar para cada solicitud pendiente, el conjunto de datos que permita identificar unívocamente el pedido, la entidad involucrada, el responsable que cursa la solicitud y el detalle de datos a Certificar.

3. ***DIRECCIÓN:*** los funcionarios responsables ejecutan un proceso manual, basado en la información provista en la solicitud, más la que consta en los libros de inscripciones. Dicho proceso permite determinar la pertinencia o no de la emisión del Certificado de Vigencia, en función de lo cuál activarán en el sistema el proceso de Emisión o Rechazo respectivamente.

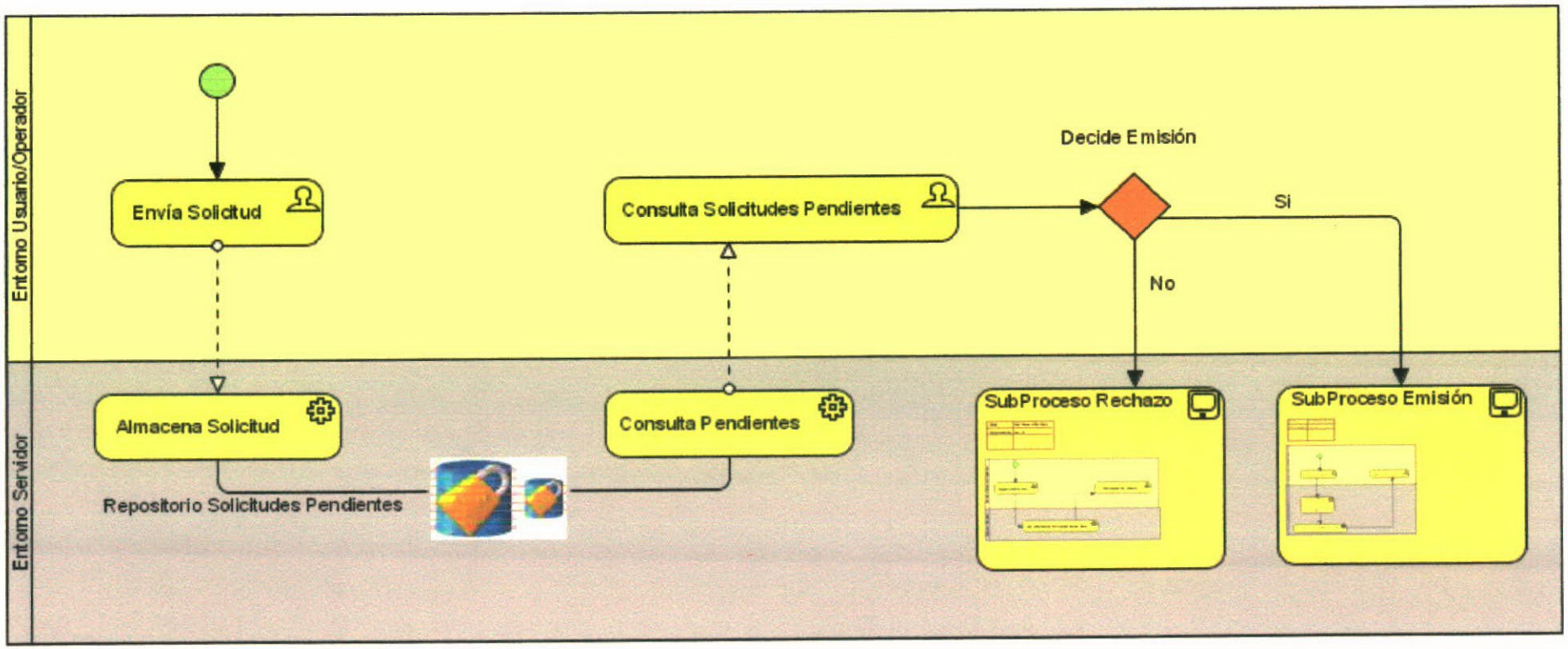
4. ***SECRETARIA AMINISTRATIVA:*** en caso de que la decisión fuera positiva respecto de la solicitud, emite automáticamente por sistema el Certificado de Vigencia, timbrado digitalmente con detalle de los datos solicitados, emite la comunicación y envía automáticamente el Certificado al so-

licitante acreditado. Luego almacena temporalmente en el sistema los Certificados de Vigencia emitidos, por un período de 90 días a partir de la fecha de emisión.

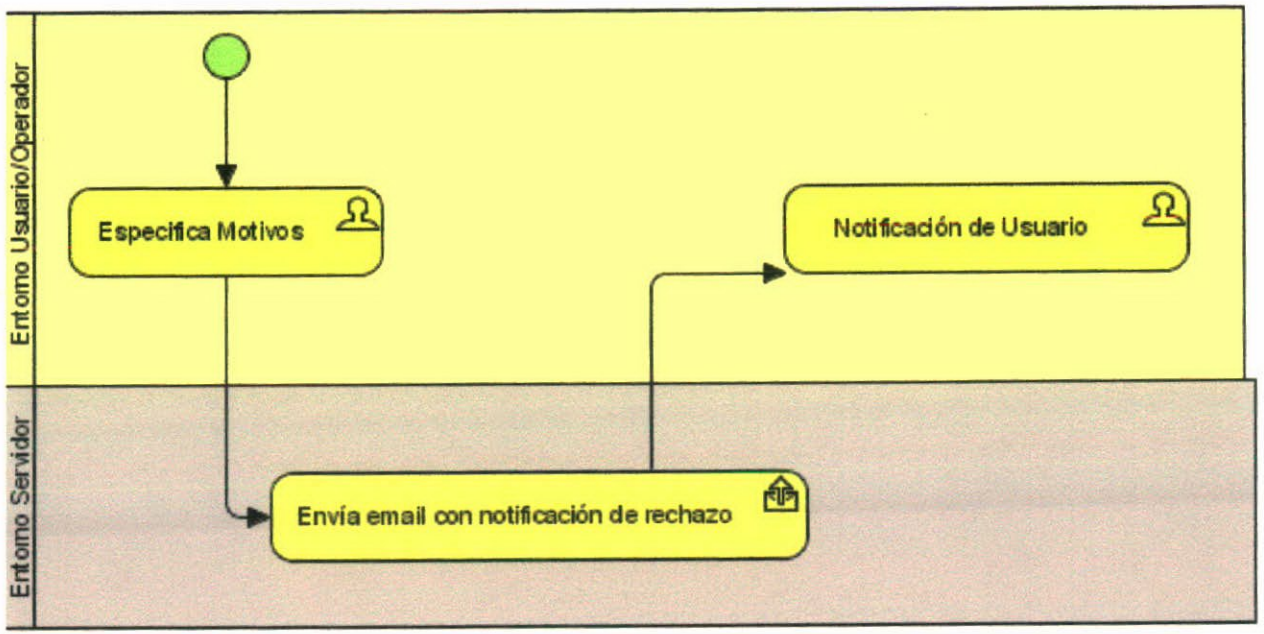
En caso de que la decisión fuera negativa respecto de la solicitud, emite automáticamente por sistema la comunicación de rechazo con detalle de los motivos que justifican la decisión.

Diagramas

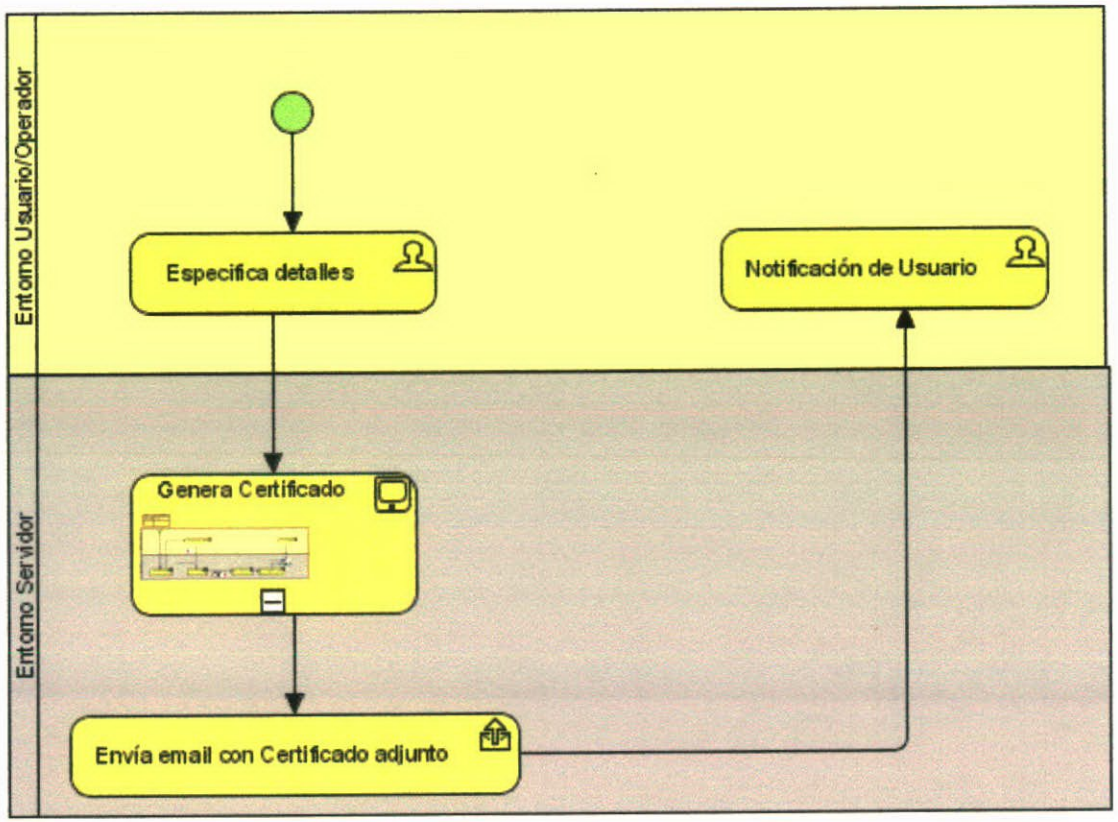
Proceso Emisión



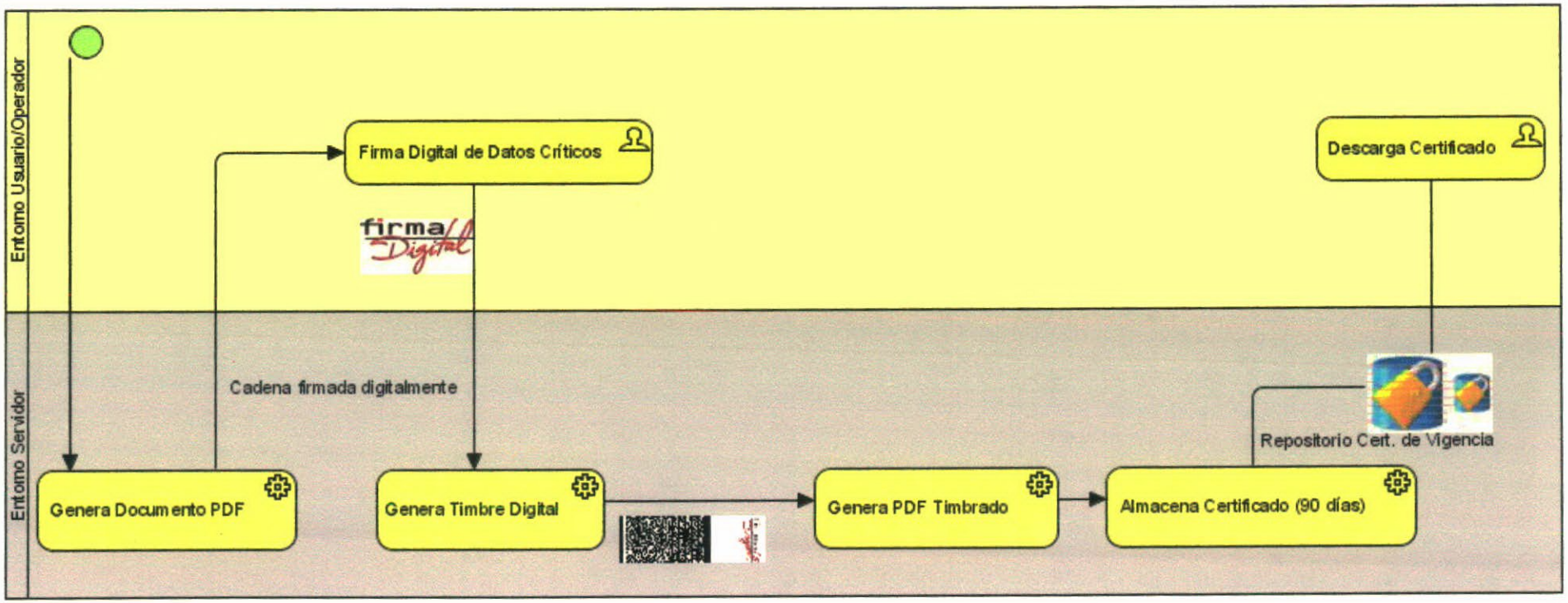
Subproceso Rechazo



Subproceso Emisión



Generación del Certificado de Vigencia



Detalle de Procesos

Consulta de solicitudes pendientes: como paso inicial del proceso, los responsables de la administración del procedimiento (personal asignado de la Dirección de Personas Jurídicas) deberán poder obtener de la aplicación, el reporte de solicitudes pendientes de atención. En dicha consulta, deberá constar para cada solicitud pendiente, el conjunto de datos que permita identificar unívocamente el pedido, la entidad involucrada, el responsable que cursa la solicitud y el detalle de datos a Certificar.

Decisión de Emisión/Rechazo: Para cada solicitud pendiente, los funcionarios responsables deberán ejecutar un proceso manual, basado en la información provista en la solicitud, más la que consta en los libros de inscripciones. Dicho proceso permitirá determinar la pertinencia o no de la emisión del Certificado de Vigencia, en función de lo cuál activarán en el sistema el proceso de Emisión o Rechazo respectivamente.

Emisión: En caso de que la decisión fuera positiva respecto de la solicitud, el sistema deberá emitir automáticamente el Certificado de Vigencia, timbrado digitalmente con detalle de los datos solicitados, tales como fecha de presentación del último balance o detalle de la constitución del Directorio. Deberán proveerse los mecanismos para la comunicación y envío automático del Certificado al solicitante acreditado.

Rechazo: En caso de que la decisión fuera negativa respecto de la solicitud, el sistema deberá emitir automáticamente la comunicación de rechazo con detalle de los motivos que justifican la decisión.

Almacenamiento: El sistema deberá permitir el almacenamiento temporal de los Certificados de Vigencia emitidos, por un período de 90 días a partir de la fecha de emisión.

Registros:

A) Datos que debe contener la Nota de Solicitud:

- Nombre de la Entidad solicitante
- Domicilio
- Nombre y Apellido del firmante
- Cargo en la Entidad
- Detalle:
    - número de Personería
    - número de legajo Interno
    - balances presentados
    - nómina de autoridades

B) Tasa retributiva de servicios

- Código 476: Sociedades Anónimas $80
- Código 489: Asociaciones Civiles $15
- Código 497: Fundaciones $45

Especificaciones Generales de Diseño

Se documentan en esta sección, los criterios básicos de diseño que deben ser respetados para el procedimiento tendientes a reducir la complejidad y la cantidad de excepciones del sistema.

1. Arquitectura Web: con la finalidad de mantener una interfaz abierta con la Guía de Trámites, reducir la complejidad de instalación y mantenimiento; y aprovechar las ventajas de esta arquitectura distribuida se deberá implementar la solución basada en arquitectura cliente-servidor para la Web.

2. Interfaz Amigable - Usabilidad: deberán contemplarse de manera prioritaria todas aquellas condiciones que garanticen la facilidad de uso de la aplicación y la correcta comprensión de cada una de las funcionalidades de la misma, tanto por parte de los operadores capacitados como por parte de los usuarios finales. A tal fin, se requiere como mínimo: ayuda en línea sobre todos los aspectos del sistema, uso de simbología estándar, etiquetado de todas las entradas y salidas, secuenciación de pasos, alertas permanentes sobre acciones relevantes, jerarquización de la información más relevante en las pantallas, separación de contenidos por grupos de contenidos relevantes, manejo uniforme de criterios de diseño y utilización de colores.

3. Control de Errores por Excepción: la lógica de control y procesamiento de errores deberá estar totalmente separada de la lógica de proceso de la aplicación, por lo cuál se sugiere la estructuración basada en excepciones.

4. Seguimiento y Verificabilidad: Todas las actividades realizadas en el sistema, en torno de una solicitud, deberán ser logeadas temporalmente por el Application Server de modo de poder obtener una traza completa de las actividades realizadas.

5. Portabilidad y Escalabilidad: Las decisiones de diseño detallado que se adopten, deberán contemplar de manera prioritaria la portabilidad y futura escalabilidad de la aplicación.

6. Ajuste a estándares: El diseño detallado deberá garantizar el ajuste a estándares en materia de firma digital y certificados digitales. Los estánda-

res y algoritmos utilizados en la solución deberán estar debidamente consignados en las especificaciones de diseño.

7. Seguridad: Se deberán incluir todos los procedimientos que resulten necesarios para garantizar la seguridad en el acceso a las fuentes de datos, así como también a los Certificados de Firma Digital implicados en el proceso.

Entradas planeadas

El proceso de emisión de Certificados tendrá como fuentes de datos:

a. Consulta a Base de Datos de Solicitudes Pendientes: recordset con los resultados de una consulta sin filtro al modelo de datos del sistema.

La estructura genérica de esta consulta proveerá datos sobre: el total de solicitudes pendientes de atención, junto a los datos detallados que permitan individualizar cada solicitud para la toma de decisiones en los procesos de emisión o rechazo.

b. Detalle de datos ingresados manualmente: datos provistos en línea por los operadores, en el momento de emisión del Certificado.

Procesos Internos

Se describen a continuación los métodos y procedimientos de procesamiento de datos, que producirán las salidas deseadas para la solución, dadas ciertas entradas y archivos de datos.

a. Consulta de Solicitudes Pendientes:

Deberá estar diseñado sobre una interfaz Web que permita la conexión dinámica a la base de solicitudes pendientes, y muestre el detalle de las mismas, a fin de que los funcionarios competentes puedan decidir sobre la pertinencia de emisión o rechazo del Certificado.

Los datos críticos a consignar sobre cada solicitud pendiente deberán ser como mínimo:

- Fecha del pedido
- Datos de identificación de la Entidad
- Datos de identificación del Solicitante
- Detalle de datos complementarios a Certificar (Balances, Nómina, Directorio, Presentación de Libros, etc.).

b. Proceso de Emisión de Certificado:

Para cada solicitud pendiente deberá darse la opción al operador de disparar el proceso automático de emisión del certificado o de manera contraria el proceso de rechazo del mismo.

La emisión de un Certificado implica la generación instantánea del Documento PDF timbrado digitalmente y su correspondiente envío por email al solicitante acreditado. Dicho proceso de emisión y envío, supone los siguientes subprocesos:

b.1. Subproceso de consignación de datos detallados: La emisión de un Certificado supone el ingreso de datos detallados que se obtienen de los libros presentados por las entidades. Una vez ordenada la emisión del Certificado por parte del operador, la aplicación deberá proveer una interfaz Web para el ingreso y validación de dichos datos.

b.2. Subproceso de Firma Digital: Se firman digitalmente, por autoridad competente, los datos críticos a incluir en el Certificado. Dichos datos deberán permitir identificar unívocamente la transacción en el sistema, la entidad

certificada y datos relevantes del solicitante responsable de la solicitud y recepción del Certificado.

b.3. Subproceso de Generación del Timbre: Este subproceso es el encargado de producir la nube de puntos PDF417 (timbre digital) con la información del texto firmado, su firma y la clave pública del firmante correctamente barcodeados.

b.4. Subproceso de Construcción del Documento en Formato PDF: El subproceso tomará como insumos la información a incluir en el Certificado, obtenida como parámetros de las fuentes de datos descriptas, y el timbre digital previamente generado sobre esta información. Con estos datos, deberá resolver la generación automática del documento .pdf que describe el Certificado de Vigencia con detalle de los datos pertinentes debidamente resaltados.

b.5. Subproceso de Notificación y Envío por e-mail del Certificado: El documento generado, deberá ser adjuntado al cuerpo de un mail de notificación y enviado instantáneamente a la cuenta de correo consignada por el solicitante, previamente verificada.

b.6. Subproceso de almacenamiento de Certificados: Deberá proveerse un mecanismo de almacenamiento del documento generado en el repositorio de Certificados por un período de 90 días.

c. Proceso de Rechazo de solicitudes:

En caso de no corresponder la emisión de un Certificado de Vigencia, el operador deberá contar con un procedimiento de comunicación del rechazo de la solicitud. El proceso de rechazo deberá contemplar el envío de un email a la cuenta de correo consignada en la solicitud, en cuyo cuerpo se informe sobre la improcedencia de la solicitud y los motivos que justifican el rechazo.

La confección y envío de dichas comunicaciones deberá ser resuelta automáticamente por parte de la aplicación, con parametrización del texto de

justificaciones. Esto último además de agilizar los tiempos de respuesta, contribuye a evitar errores humanos en el envío de los correos.

d. Módulo de verificación de usuarios:

En todos los aspectos de su administración, la aplicación deberá proveer y monitorear un acceso restringido a usuarios. Esta implementación podrá estar solventada sobre una autenticación simple de login/password o sobre algún esquema de autenticación fuerte basado en Certificados Digitales, de acuerdo a como se considere más conveniente en etapa de diseño detallado.

Las funciones que podrán ser desarrolladas desde la interfaz de la aplicación no amerita en principio el diseño de un esquema de perfiles de acceso de usuarios con privilegios diferenciales.

Persistencia de datos

Se determinan en este punto de manera genérica, los repositorios de datos que será necesario mantener para garantizar la persistencia de la información relevante.

Base de Datos de Solicitudes Pendientes: estructura de información administrada concurrentemente por la aplicación de generación de solicitudes (implementada en la Guía de Trámites de la Provincia) y por la aplicación de Emisión de Certificados.

Repositorio de Certificados de Vigencia: los Certificados emitidos por la aplicación, debidamente timbrados, deberán ser mantenidos en este repositorio por un período de 90 días desde su fecha de emisión.

Logs de Transacciones: se deberán mantener archivos de seguimiento de las transacciones realizadas en el sistema, con detalle mensual.

Buzones de email: con fines de seguimiento y control deberán mantenerse los correos electrónicos enviados y recibidos por la aplicación por un período de 90 días.

Salidas Planeadas

Las salidas básicas que deberá proveer la aplicación contemplan:

- Certificados de Vigencia: documentos en formato .pdf con el cuerpo del certificado más el timbre digital correspondiente.
- Emails de notificación: de envío de certificado o rechazo del mismo
- Pantallas de notificación de secuencia: deberá informarse al operador sobre el estado de procesamiento de una transacción hasta el momento en que la misma se complete.
- Pantalla de notificación de errores: cualquier excepción producida en la aplicación que no pudiera ser resuelta por los manejadores de excepciones, deberá ser notificada al operador, con detalle de los motivos que la provocaron y referencia al soporte o ayuda al cuál deben contactarse para tomar las medidas correctivas pertinentes.

- Reportes de Certificados Emitidos: consulta al repositorio de Certificados Emitidos con detalle de los certificados emitidos en los últimos 90 días corridos y acceso a los documentos .pdf.

Descripción General de Aplicaciones

El funcionamiento integral del sistema deberá soportarse sobre dos aplicaciones totalmente independientes, las cuáles operarán complementariamente en el circuito de emisión y verificación respectivamente.

a. Aplicación de emisión del Certificado de Vigencia: Aplicación dinámica para la Web, basada en una arquitectura cliente-servidor que permite el procesamiento de las solicitudes de certificación y la emisión de los Certificados de Vigencia con aprobación de funcionarios competentes mediante timbre digital.

b. Aplicación de validación de Timbre Digital: aplicación standalone, que permite verificar la integridad y validez del timbre digital. El software toma la cadena de caracteres que ingresan desde el puerto de teclado conectado al scanner y reconstruye los caracteres de la firma, la clave pública y el texto en claro que se firmó. Hecho esto, provee estos datos junto al Certificado a un módulo de verificación de firma que valida la integridad de la firma en relación a los datos firmados, mostrando un mensaje final al funcionario sobre la validez o no del timbre incluido en el Certificado en cuestión.

Arquitectura y Plataforma Tecnológica

Para el desarrollo e implantación de las aplicaciones, se aprovechará la plataforma tecnológica utilizada en desarrollos previos de la tecnología de Timbre Digital. Esto, además de suponer un mayor aprovechamiento de la capacidad instalada, implica utilizar un conjunto de herramientas debidamente probadas en torno de implantaciones de Timbre Digital.

No obstante lo anterior, se proponen algunas actualizaciones sobre la plataforma Java y drivers JDBC a instalar del lado del servidor, de manera de mantener actualizada la base tecnológica tanto de desarrollo como de producción.

Arquitectura de Servidor: del lado del servidor deberá instalarse una plataforma J2SDK 1.5 y un servidor de aplicaciones web JBOSS 4.0.1 o superior que permita la ejecución de servlets java.

Para la generación de los documentos .pdf y el codebar PDF417, se utilizará la API java iText ver. 1.5, instalada en el classpath de la aplicación. Alternativamente, para contemplar la posibilidad de generación de objetos de firma PKCS#7 deberá incorporarse al deploy del proyecto en el servidor el paquete BouncyCastle (http://www.bouncycastle.org).

Las aplicaciones deberán deployarse sobre el Application Server como un archivo empaquetado .ear, con su configuración expresada en documentos XML. Su configuración y parametrización debe permitir amplia portabilidad del software desarrollado sobre entornos Linux y/o Windows

Cabe recordar que tanto la plataforma java, como las librerías de clases y el application server requeridos en el servidor, son software de libre acceso.

Configuración del cliente: los clientes que se conecten a la aplicación, tanto desde la Intranet de Gobierno, como usuarios externos, sólo deberán necesitar un browser de Internet y Adobe Acrobat Reader 6.0 o superior.

Deberá excluirse del desarrollo la utilización de componentes activos que pudieran ser filtrados por configuraciones de seguridad de los browsers.

Selección del formato de los documentos Digitales

Debido a los buenos resultados obtenidos en experiencias previas y a los requerimientos especificados para este caso en particular, el desarrollo deberá generar los Certificados de Vigencia en formato PDF (Portable Document Format), dado que este formato constituye un estándar para la publicación de documentos en Internet, contribuye a la inalterabilidad de los documentos y además facilita la incorporación del código de barras PDF417 conteniendo el timbre digital.

Selección de los lenguajes de desarrollo

La programación deberá hacer uso de los siguientes lenguajes:

Servlets y Clases: Java (J2EE). El desarrollo deberá soportarse sobre servlets basados en J2EE. No se prevé en las especificaciones de diseño la utilización de tecnología de WebServices o JavaBeans.

Interface web: La interfase web del proyecto deberá sustentarse sobre código .jsp (Java Server Page) para la generación dinámica de código HTML/Javascript.

Librerías y paquetes de clases a utilizar

El lenguaje Java, nativamente orientado a objetos, explota al máximo la posibilidad de escalar su potencialidad con un sinnúmero de librerías de clases reutilizables, con propósitos específicos, proporcionadas gratuitamente por la comunidad de desarrolladores de java y en ocasiones por empresas u organismos que realizan desarrollos en esta línea. En particular el presente desarrollo con timbre digital deberá utilizar las siguientes librerías (APIs Java), cuyo propósito y características principales se describen a continuación:

API iText ver.1.5 o superior : iText es un proyecto Sourceforge mantenido por una comunidad abierta de desarrolladores de software libre. Es una librería de clases Java que permite la generación dinámica de documentos pdf totalmente compatibles con la PdfReference 1.6. Las clases provistas por iText son muy útiles para generar documentos de sólo lectura independientes de la plataforma que contentan texto, listas, tablas e imágenes. En nuestro caso particular, la utilizamos por las siguientes características:

- Describe objetos de alto nivel que permiten generar rápidamente los principales componentes de un documento pdf.
- Incorpora la posibilidad de manejar el contenido interno de documentos pdf a bajo nivel. Es decir manipular directamente el formato interno de los documentos generados.

- El código de los documentos pdf generados es altamente compatible con las especificaciones de la Adobe PdfReference 1.6. Esta especificación describe el formato interno de los documentos pdf.
- Incorpora una jerarquía de clases completamente dedicada a la generación de Codebar PDF417 con excelentes características de optimización de la imagen generada, posibilidades de customización muy amplias e incorporación del procedimiento MacroPdf417.
- Incorpora una jerarquía de clases completamente dedicada a la generación de firmas digitales sobre documentos pdf. Si bien esto no está estrictamente relacionado con la generación del timbre, es una característica fundamental a considerar en función del posible crecimiento de la aplicación.
- iText es especialmente útil en combinación con tecnología Java(TM) basada en Servlets, que como documentamos anteriormente es el esquema de servicio a implementar en el servidor elegido.
- Existe excelente documentación sobre la API y una comunidad de desarrollo muy activa con foros de consulta y documentación en permanentemente mantenimiento
- La librería cae dentro de la categoría de software libre y puede descargarse gratuitamente desde http://www.lowagie.com

- Paquete Java.Security: Dentro de la plataforma J2SDK 1.5.0 se incorpora el paquete de clases Java.Security. Este package describe clases que permiten manipular objetos de firmas digitales, Certificados, claves públicas y privadas, keystores, algoritmos de firma, etc. Es el conjunto nativo de clases que propor-

ciona el lenguaje para la manipulación de firmas y certificados digitales. En particular, las especificaciones de diseño prevén la utilización de clases provistas en este paquete para generar, tomando un certificado X.509 v3, una firma SHA1withRSA representada en formato PKCS#1 (CodeBase64) que constituye la firma digital de los elementos de datos esenciales del Certificado. Esta firma deberá luego ser codificada en codebar PDF417 constituyendo así el timbre digital.

- Driver de Conexión JDBC: La conexión desde los módulos de la aplicación a la Base de Datos deberá resolverse mediante el Driver JDBC jdbcpostgresql 7.2 o superior. Dicho driver deberá manejar las cadenas de conexión a la base de datos con identificación de usuarios y claves de conexión. Así mismo, deberá parametrizarse la conexión para la selección de Charsets que permitan una interpretación correcta de cadenas alfabéticas con símbolos especiales del idioma español tales como ñ y letras acentuadas.

Determinación de niveles de Seguridad y Acceso al Sistema

El servlet de generación del Certificado deberá ser de acceso restringido a funcionarios autorizados de la Dirección Provincial de Personas Jurídicas. A tal efecto deberá proveerse en la interfase web un esquema de validación de login/password u otro mecanismo superior de identificación y otorgamiento de permisos. Complementariamente la aplicación deberá estar restringida en alcance a la Intranet de Gobierno.

La seguridad en la generación del Certificado deberá implementarse mediante la generación del timbre. El mismo garantizará la originalidad, integridad y autoría del documento.

El legítimo interés de los solicitantes en requerir un Certificado de Vigencia para la persona jurídica que representan será verificado mediante un

circuito de verificación de email y el posterior envío automático, por parte de la aplicación del Certificado a la cuenta de correo debidamente registrada. Cualquier comunicación complementaria que el sistema desarrolle deberá ser remitida a la misma cuenta de correo electrónico.

La protección de los certificados está garantizada en el servidor de timbrado por los responsables de la Autoridad de Registro de la ONTI.

La aplicación de validación de timbres, instalada en las oficinas que así lo requieran, es de acceso exclusivo a usuarios con privilegios de administración u operación sobre el sistema, validados mediante esquemas de login-password.

Tolerancia a fallas y gestión de errores

Las fallas y errores que pueden producirse en tiempo de ejecución (por ej.: por problemas de conexión, caída del application server, ausencia de un reader, etc.) deberán gestionarse bajo el concepto de manejo de excepciones. Esto implica que el sistema genera una excepción ante un error o falla que es tratada por un manejador de excepciones especialmente diseñado para tratar este tipo de errores. De esta forma se separa el código de manejo de errores, del código que atiende a la lógica principal del desarrollo, facilitando su comprensión y mantenimiento posterior. Así mismo, un cuidadoso manejo de excepciones implica en nuestro desarrollo una mayor tolerancia a fallas, objetivo de diseño fundamental en un sistema que pretende estar on-line 24x7x365.

Fuentes de Datos

La base de datos de solicitudes pendientes deberá instalarse sobre el motor PostgreSql 7.3 o superior. Este motor se ejecuta en un equipo independiente del Application Server y es accedido concurrentemente por la apli-

cación de generación de solicitudes desarrollada en la Guía de Trámites de la Provincia.

La estructura de la base de datos deberá ajustarse al siguiente modelo:

Charset: windows-1252

Esquema: único

Vistas: ninguna

StoreProcedures y Triggers: ninguno

Funciones: ninguno

Usuario de conexión: consulta1

Lenguaje de Consulta: ajustarse a ANSI SQL

Tabla de Solicitudes Pendientes:

Campo	***Tipo***	***Descripción***
id_internopj	VARCHAR 11	Nº Interno de identificación de la entidad en el Registro Provincial de Personas Jurídicas. Este código alfanumérico permite identificar unívocamente a la entidad.
id_transc	VARCHAR 6	Nº único de transacción. Este número permite identificar unívocamente la solicitud. Deberá generarse correlativamente a partir de 000001
entidad	VARCHAR 80	Nombre o identificación de la entidad, reservado en el Registro Provincial de Personas Jurídicas
domicilio	VARCHAR 60	Domicilio registrado de la entidad.

fechapedido	DATE	Fecha de generación de la solicitud de Certificado.
apellidosolicita	VARCHAR 30	Apellido del responsable acreditado de la entidad, que emite la solicitud o pedido de certificación.
nombresolicita	VARCHAR 30	Nombre de pila del responsable acreditado de la entidad, que emite la solicitud o pedido de certificación.
Email	VARCHAR 60	Dirección de correo registrada por el solicitante. A este email deberán ser remitidos las notificaciones de emisión o rechazo de Certificados. Así como también cualquier notificación intermedia que se remita.
dnisolicita	VARCHAR 8	Documento Nacional de Identidad del solicitante.
Cargo	VARCHAR 60	Descripción del cargo del solicitante en la entidad.
itempersoneria	BOOLEAN	Bandera que activa o no la certificación de personería jurídica.
itemlegajo	BOOLEAN	Bandera que activa o no la certificación de legajo.
itembalances	BOOLEAN	Bandera que activa o no la certificación

		de último balance presentado.
itemnomina	BOOLEAN	Bandera que activa o no la certificación de nómina.
itemdirectorio	BOOLEAN	Bandera que activa o no la certificación de constitución de directorio.
itemconcursos	BOOLEAN	Bandera que activa o no la certificación de antecedentes en concursos preventivos de la entidad.
itemsedesocial	BOOLEAN	Bandera que activa o no la certificación de constitución de sede social de la entidad.
itemotros	BOOLEAN	Bandera que activa o no la certificación de otros ítems no previstos en la parametrización descripta previamente.
observación	VARCHAR 120	Campo alfanumérico para indicar el cuerpo de texto a agregar en el certificado en caso de que se active la bandera itemotros.
Estado	ENUM {1,2}	Enumeración con valores 0 ó 1. Puesta a 0, indica que el estado de la solicitud es: *"pendiente de atención"*. Puesta a 1, indica que el estado de la solicitud es *"procesada"*.

Condiciones de Generación del Certificado de Vigencia

Se describe en este apartado, el contenido del documento PDF (Portable Document Format) que constituye el Certificado de Vigencia, su disposición y formato:

Componente	Formato	Texto Parámetros Dinámicos
Encabezado	Imagen gif transparente encabezado.gif	N/A
Título	Fuente: Helvética Tamaño: 16 Estilo: Negrita, cursiva	"CERTIFICADO DE VIGENCIA"
Cuerpo	Fuente: Helvética Tamaño: 14 Estilo: Normal, con parámetros resaltados en negrita.	"CERTIFICO que la entidad " + entidad + personeria + legajo + balances + "\n " + nomina + directorio + concursos + sedesocial
Pie de Cuerpo	Fuente: Helvética Tamaño: 14 Estilo: Normal.	"El presente certificado se expide a solicitud del interesado para ser presentado ante las autoridades que lo requieran, en Mendoza a los " + fechaemision + ".-"
Timbre Digital	Imagen PDF417	N/A
Marca Firma	Imagen gif transparente	N/A

	"marcafirma.gif"	

El formato de diseño del Certificado debe jerarquizar la información más relevante del mismo. En particular, deberá resaltarse con letra negrita y en tamaño de fuente superior:

Condiciones de generación del timbre digital

Para que a partir de la lectura de los códigos generados se pueda reconstruir sin errores la firma digital de los datos timbrados, la generación del timbre digital cumple las siguientes condiciones técnicas:

Nivel de Corrección de Errores: para poder reconstruir la firma, aún cuando el código se haya deteriorado en parte es necesario mantener un determinado nivel de redundancia de datos. Dicho nivel debe ser optimizado, para que la redundancia introducida no degrade significativamente la capacidad de almacenamiento de información del código. La clase BarcodePDF417 de la API iText, utilizada para generar el timbre posee un algoritmo que optimiza el nivel de corrección de errores aplicado, asignándolo dinámicamente entre 0 y 5 como lo prescribe el estándar, de acuerdo la longitud de los CodeWords. En particular el nivel se fija de acuerdo a la siguiente lógica:

```
if (lenCodewords < 41)
errorLevel = 2;
else if (lenCodewords < 161)
errorLevel = 3;
else if (lenCodewords < 321)
errorLevel = 4;
else
      errorLevel = 5;
```

Modo de Compactación: PDF417 soporta tres modos de compactación: alfanumérico, numérico y binario. Cada uno de estos modos es más eficiente que el resto en ciertos juegos de caracteres. La clase Barcode PDF417 utiliza un sistema de optimización que elige el modo de compactación más óptimo para el conjunto de caracteres que se está codificando.

Capacidad de codificación y representación de la firma: Un código de barras 2D PDF417 puede almacenar hasta 1.100 bytes en binario o 1.800 caracteres ASCII, por lo que la representación del timbre debe ser inferior a ese tamaño. Atendiendo esto, la el desarrollo debe contemplar las siguientes condiciones:

Excluir la posibilidad de representar la firma como un objeto PKCS#7[PKC93] debido a que el conjunto de bytes generados supera la densidad de información soportada por el timbre (3 Kbytes aprox.).

La firma digital, está avalada por una cadena de certificación. Los certificados digitales se emiten para los algoritmos asimétricos RSA[RSA78] y DSS[Nat99] (con una clara preferencia por RSA). En función de lo anterior, la firma digital deberá ser representada por un identificador en ASCII (SHA1withRSA), el separador ASCII "-" y el valor de la firma RSA usando el estándar PKCS#1[KS98]. Esto último, por ser las formas más comunes de representar los valores por las aplicaciones y bibliotecas criptográficas.

La clave pública, contenida en la firma deberá representarse por un identificador del algoritmo en un código ASCII, seguido de los parámetros del algoritmo en un orden predefinido separados por el carácter ASCII "-".

El resto de datos incluidos en el timbre, se representarán en formato de texto en claro mediante código ASCII de una manera legible al ser humano.

De acuerdo a las consideraciones anteriores la representación interna de la información codificada en el timbre deberá ajustarse al siguiente formato:

<<Cadena de Datos firmados>> + <<inscripción obtenida como parámetro>> + "-" + <<fecha pedido obtenido como parámetro>> + "-" + <<transacción obtenido como parámetro>> + "-" + <<apellido y nombre del solicitante obtenido como parámetro>> + "-" + <<Nro. Documento del solicitante obtenido como parámetro>> + <<Cadena de firma codificada en CodeBase64 (PKCS#1)>> + <<Clave pública>>

La imagen del timbre generado deberá cumplir con las siguientes condiciones:

aspect ratio: 1:3 (relación de aspecto)

quiet zone: 1 cmt. (perímetro blanco)

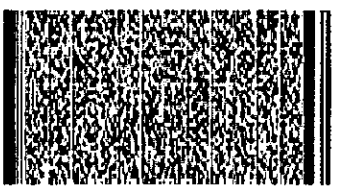
Adjuntos o anexos

CERTIFICADO DE VIGENCIA

CERTIFICAMOS que la entidad ***Organización de Prueba*** obtuvo su autorización para funcionar como persona jurídica por Resolución Nº 12.345/2-06 de ésta Dirección, encontrándose vigente a la fecha.

El último balance presentado es al 31/05/2007.

El presente certificado se expide a solicitud del interesado para ser presentado ante las autoridades que lo requieran, en Mendoza a los 24 días del mes de agosto del año dos mil siete.-



V. Identificación y diseño de experiencia B de firma o timbre digital

A) Identificación de la necesidad y análisis del sistema actual

Nuestra segunda experiencia de firma/timbre digital se orienta a la solución de una necesidad puntual. Dicha necesidad surge del trabajo que viene realizando la Unidad de Reforma del Estado en materia de difusión de Gobierno electrónico y de generación de espacios vitales para su desarrollo fomentando la interacción con expertos y puesta en común de soluciones exitosas. Nos referimos a la organización de eventos internacionales, provinciales, regionales y locales que cuentan con la asistencia de numerosas personas interesadas en la gestión eficiente y la modernización del Estado a través de las herramientas que brinda el e-gov. Nuestro trabajo en este sentido tiende a optimizar una de las partes vitales del desarrollo operativo de este tipo de eventos con un inédito procedimiento de emisión/entrega on-line, de "Certificados de Asistencia digitales con firma digital" emitidos por el Gobierno de Mendoza y sus organizadores asociados a participantes acreditados.
Los fundamentos de la aplicación de la tecnología de firma y timbre digital a este procedimiento tienen que ver con los problemas que se suscitan en el proceso tradicional de emisión de certificados en papel y con los beneficios asociados a estas tecnologías.

Procedimiento Tradicional

1. ***Inscripción:*** aquellos individuos interesados en participar del evento, deberán concretar su inscripción en tiempo y forma, mediante un formulario ***en soporte papel*** que permita registrar la información relevante para el proceso de confección y emisión de certificados.

2. ***Acreditación:*** en instancia de realización del evento, los inscriptos asistentes deberán cumplir con el proceso de acreditación, registrándose así en una planilla soporte papel su efectiva asistencia y participación al evento.

3. ***Confección de Certificados:*** cumplidos los plazos pertinentes para la acreditación de participantes y en coincidencia con el cierre del evento, se realiza un proceso de confección e impresión de una plantilla de Certificados de Asistencia a los participantes acreditados, con espacios en blanco para su nombre, número de documento y detalle de su rol en el evento (asistente, expositor, organizador o patrocinador).

4. ***Llenado de datos:*** se procede a llenar los datos con la planilla de los asisitentes acreditados en los espacios en blanco y de forma manual

5. ***Firma de Certificados:*** una vez confeccionados todos los certificados se pasan para se firmados y sellados por la autoridad competente.

6. ***Envío de Certificados:*** se procede a comunicar a los asistentes que su certificado se encuentra disponible para retiro o se envían por correo tradicional.

Como ya sabemos, casi cualquier tipo de transacciones electrónicas puede requerir los niveles de seguridad que provee la implementación de las tecnologías de firma y timbre digital, sin embargo es importante hacer una adecuada elección del alcance y los ámbitos de aplicación de los servicios de criptografía asimétrica para lograr ahorros y no incurrir en sobrecostos de implementación. A continuación analizaremos más profundamente dichos fundamentos.

Beneficios y fundamentos:

- A través del nuevo procedimiento aumenta eficiencia interna de la organización del evento, se evitan sobrecostos y se generan ahorros en papel y en tiempos administrativos de procesamiento confección y entrega

- La firma digital provee garantías de autoría y el timbre digital de autenticidad al certificado digital de asistencia

- Aquellos participantes acreditados que viven muy alejados del lugar de realización del evento no necesitan volver a buscar su certificado de asistencia, ni distraer tiempo en conseguir el certificado durante el evento.

- Las características particulares de la tecnología de timbre digital, permiten, de ser necesaria, la impresión en soporte papel del certificado digital de asistencia asegurando la autenticidad y verificabilidad del mismo.

- De forma consistente con las afirmaciones anteriores, la aplicación de la tecnología genera un gran beneficio para el asistente

acreditado quién ya cuenta con su certificado digital en su casilla de correo a la finalización del evento.

B) Documentación de diseño del "Procedimiento de emisión/entrega de certificados de asistencia digitales con firma digital"

Se han completado en esta etapa las tareas de especificación de diseño, del procedimiento de emisión on-line, de "Certificados de Asistencia digitales con firma digital" emitidos por el Gobierno de Mendoza y sus organizadores asociados a participantes acreditados en los seminarios y foros que en la provincia regularmente se realizan.

La documentación de diseño incluye una fase de ***diseño global***, en la cuál se describen genéricamente las características funcionales que deberá proveer la aplicación, de forma de garantizar el cumplimiento de los requerimientos y objetivos determinados.

Complementariamente, el ***diseño detallado*** determina explícitamente los recursos tecnológicos que soportarán el proceso de desarrollo, con detalle de la arquitectura y plataforma tecnológica que deberá considerarse en etapa de implementación, el diseño de interfaces, el modelo de datos (entradas, procesos internos, salidas, mecanismos de control y verificación) y las especificaciones detalladas en términos de obtención de Certificados de Firma Digital y generación del procedimiento de timbrado digital; así como también la publicación y envío de certificados.

Es importante mencionar que los criterios de diseño adoptados, parten de un conocimiento amplio de los enfoques que han tenido éxito en implementaciones previas de la tecnología de timbre digital, y firma digital en general.

1) Diseño Global

Descripción general de la solución propuesta

La solución debe comprender mecanismos que permitan registrar la asistencia de individuos a un evento particular y emitir de manera ágil y segura, al cierre del mismo, su constancia de asistencia, en formato digital, firmada por autoridad competente. Deben contemplarse también procedimientos de distribución de Certificados que permitan a los asistentes contar con una constancia válida sin necesidad de acudir personalmente a retirarlos desde alguna oficina de gobierno.

En particular, el procedimiento debe incluir las siguientes características funcionales, secuenciadas en formas de pasos:

1. ***Inscripción:*** como paso inicial, aquellos individuos interesados en participar del evento, deberán concretar su inscripción en tiempo y forma, mediante un formulario ***en línea*** que permita registrar la información relevante para el proceso de emisión y envío de certificados.

2. ***Acreditación:*** en instancia de realización del evento, los inscriptos asistentes deberán cumplir con el proceso de acreditación, registrándose así en el sistema su efectiva asistencia y participación al evento.

3. ***Emisión de Certificados:*** cumplidos los plazos pertinentes para la acreditación de participantes y en coincidencia con el cierre del evento, se deberá contar con un proceso de emisión automática de Certificados de Asistencia a los participantes acreditados, con detalle de su rol en el evento (asistente, expositor, organizador o patrocinador).

4. ***Timbrado de Certificados:*** los certificados emitidos deberán ser timbrados digitalmente a fin de posibilitar la persistencia de las garantías de la firma digital cuando el documento es impreso. Dicho timbre digital, deberá incluir detalle de datos críticos incluidos en el Certificado, tales como nombre y DNI del participante; y datos relevantes del evento que se certifica.

5. ***Firma digital de Certificados:*** los Certificados de asistencia emitidos deberán ser firmados por parte de la/las autoridades competentes, en un proceso ágil de firmado por lotes, cumpliendo las restricciones y medidas de seguridad requeridas en materia de firma digital.

6. ***Envío de Certificados:*** la aplicación deberá disponer de una función de envío automático de los certificados de asistencia con firma digital, mediante correo electrónico, a los participantes acreditados.

7. ***Publicación de Certificados:*** de forma complementaria al envío de certificados, los mismos deberán ser publicados en el sitio del evento o, en su defecto, en el portal de la Unidad de Reforma y Modernización del Estado, para que los mismos puedan ser descargados desde allí por parte del usuario interesado. Esta medida atiende a brindar un mecanismo alternativo de acceso a las certificaciones, en caso existir inconvenientes con la entrega de algún correo en particular. Deberá cumplirse un período de almacenamiento de los Certificados emitidos, por un período no inferior a 90 días a partir de la fecha de emisión.

8. ***Almacenamiento:*** Cumplido el plazo de publicación on-line de Certificados, los mismos deberán almacenarse en CDs o DVDs., debidamente documentados y entregarse a los responsables de la organización del evento.

Especificaciones Generales de Diseño

Se documentan en esta sección, los criterios básicos de diseño que deben ser respetados tendientes a reducir la complejidad y la cantidad de excepciones del sistema.

1. Arquitectura Web: con la finalidad de disponer de mecanismos de acceso on-line al sistema y posibilitar su integración dinámica con los sitios de difusión de eventos en Internet; así como también, reducir la complejidad de instalación y mantenimiento de software y plataforma tecnológica; se deberá implementar la solución basada en arquitectura cliente-servidor para la web.

2. Interfaz Amigable - Usabilidad: deberán contemplarse de manera prioritaria todas aquellas condiciones que garanticen la facilidad de uso de la aplicación y la correcta comprensión de cada una de las funcionalidades de la misma, tanto por parte de los usuarios finales, los operadores habilitados para su parametrización, los agentes de carga de acreditación y las autoridades firmantes. A tal fin, se requiere como mínimo: ayuda en línea sobre todos los aspectos del sistema, uso de simbología estándar, etiquetado de todas las entradas y salidas, secuenciación de pasos, alertas permanentes sobre acciones relevantes, jerarquización de la información más relevante en las pantallas, separación de contenidos por grupos de contenidos relevantes, manejo uniforme de criterios de diseño y utilización de colores.

3. Control de Errores por Excepción: la lógica de control y procesamiento de errores deberá estar totalmente separada de la lógica de proceso de

la aplicación, por lo cuál se sugiere la estructuración basada en excepciones propia de un diseño orientado a objetos.

4. Seguimiento y Verificabilidad: Todas las actividades realizadas en el sistema, deberán ser logueadas temporalmente por el Application Server y el motor de base de datos, de modo de poder obtener una traza completa de los procesos realizados. Así mismo, deben preverse mecanismos de comunicación gráfica a los operadores sobre el éxito en los procesos de emisión, timbrado, firmado, envío y publicación de cada Certificado procesado.

5. Portabilidad y Escalabilidad: Las decisiones de diseño detallado que se adopten, deberán contemplar de manera prioritaria la portabilidad y futura escalabilidad de la aplicación.

6. Ajuste a estándares: El diseño detallado deberá garantizar el ajuste a estándares en materia de firma digital y certificados digitales. Los estándares y algoritmos utilizados en la solución deberán estar debidamente consignados en las especificaciones de diseño.

7. Seguridad: Se deberán incluir todos los procedimientos que resulten necesarios para garantizar la seguridad en el acceso a las fuentes de datos, así como también a los Certificados de Firma Digital implicados en el proceso.

Entradas planeadas

El proceso de emisión de Certificados tendrá como fuentes de datos:

a. Formulario de Inscripción on-line de participantes: las personas interesadas en participar del evento, deberán completar el formulario de ins-

cripción en línea al evento. Dicho formulario debe recabar datos suficientes para individualizar unívocamente a una persona, determinar su rol en el evento; y poder contactarla luego.
El formulario de inscripción debe disponerse en tiempo y forma, en el sitio web de difusión del evento (foro, jornada, seminario, curso, otros). En caso de que no exista tal sitio, el servicio podrá implementarse en el portal de la Unidad de Reforma del Estado y/o en las páginas institucionales de las entidades organizadoras.

b. Acreditación de asistentes: los agentes de acreditación, deberán registrar en el sistema la efectiva asistencia de los inscriptos al evento, a fin de disponer de un mecanismo de control que permita seleccionar que personas deben ser debidamente certificadas y quienes no. Para tal actividad, deberá proveerse de una interface web que permita acceder y modificar dinámicamente los registros de inscripción.
Se requiere aquí un desarrollo web de acceso al repositorio de datos, para permitir que la tarea de acreditación sea realizada desde el lugar de realización del evento sin instalaciones o configuraciones previas de software en las máquinas dispuestas a tal fin.

Como sugerencia de implementación, es recomendable concientizar a los agentes de acreditación sobre la importancia de cumplimentar adecuadamente esta tarea y la necesidad de que verifiquen en esta instancia la corrección de los datos consignados por los participantes en su formulario de inscripción.

La corrección y completitud de los datos ingresados al sistema son fundamentales para garantizar el correcto funcionamiento de sus procesos internos y el logro de los resultados esperados.
Es por ello mandatario instrumentar todos los mecanismos de verificación y control posible que contribuyan a garantizar la pertinencia de las entradas al sistema.

En particular, y sin perjuicio de otra información relevante que pudiera ser considerada en etapa de diseño detallado, se consideran datos críticos de entrada:

- √ *Nombre y apellido del inscripto*
- √ *Documento Nacional de Identidad, Pasaporte u otro medio de identificación legal*
- √ *Calidad de participante: asistente, expositor, organizador, patrocinador, otras.*
- √ *Dirección de correo electrónico particular*

Procesos Internos

Se describen a continuación los métodos y procedimientos de procesamiento de datos, que producirán las salidas deseadas para la solución, dadas ciertas entradas y archivos de datos.

Dichos procesos deben secuenciarse por pasos, en el orden que a continuación se exponen, de modo de conducir al usuario en una línea de trabajo que lo lleve a completar toda la tarea de generación, firma y envío de certificados para un evento en particular.

Paso 1: Consulta de inscriptos acreditados:

Deberá estar diseñado sobre una interfaz web que permita la conexión dinámica a la base de datos de inscripciones y acreditaciones, y muestre el reporte de individuos acreditados a un evento particular, a fin de que el sistema determine los Certificados a emitir.

Los datos críticos a consignar sobre cada inscripto acreditado deberán ser como mínimo:

- *Nombre y apellido del inscripto*
- *Documento Nacional de Identidad, Pasaporte u otro medio de identificación legal*
- *Calidad de participante: asistente, expositor, organizador, patrocinador, otras.*

Paso 2: Proceso de Emisión de Certificados Firmados:

Una vez determinados los individuos acreditados a un evento particular que deben ser certificados, el operador deberá contar con la opción de disparar el proceso automático de ***emisión*** de certificados.

Los certificados deberán ser emitidos en un proceso de ***lote único*** para el evento, automático y ágil, que contemple las medidas de seguridad, control y verificación de errores necesarias para garantizar la corrección en tan relevante tarea.

La emisión de cada Certificado implica la generación instantánea del Documento PDF (Portable Document Format) timbrado y firmado digitalmente. Dicho proceso de emisión, timbrado y firma, supone los siguientes subprocesos:

2.1. Subproceso de Generación del Timbre: La construcción del timbre implica la firma digital, por autoridad competente, de aquellos datos individualizados como críticos a incluir en el Certificado. Dichos datos deberán permitir identificar unívocamente la transacción en el sistema, el individuo certificado y la jornada, foro o curso implicado. Una vez obtenida la firma digital de estos datos, el subproceso deberá producir la nube de puntos PDF417 (timbre digital) con la información del texto firmado, su firma y la clave pública del firmante correctamente barcodeados.

2.2. Subproceso de construcción preliminar del documento PDF: En función de los datos obtenidos del recordset de inscriptos acreditados y el timbre digital previamente generado sobre esta información, este subproceso será el encargado de construir dinámicamente un archivo ajustado a la especificación PDF 1.6 o superior con detalle de la siguiente información:

- √ Logos o marcas institucionales de la/las entidades organizadoras y patrocinantes de la jornada, seminario, curso, etc.
- √ Título del evento que se certifica.
- √ Nombre y Apellido de la persona certificada.
- √ Documento de la persona certificada.
- √ Fecha de realización del evento.
- √ Timbre Digital (Nube de puntos PDF417)

Este documento PDF constituye el certificado digital preliminar sobre el cuál se aplicará el proceso de firma digital.

2.3. Subproceso de Firma Digital del Certificado emitido: Una vez construido el documento PDF preliminar, el mismo deberá ser firmado digitalmente por la/las autoridades competentes, obteniendo así el documento PDF final, timbrado y firmado digitalmente. Es importante recalcar en este punto que si bien estas especificaciones de diseño prevén el timbrado y firma de certificados en un proceso batch, no deben por esto obviarse las recomendaciones restrictivas a considerar en la aplicación de firma digital. En particular:

- √ Deberán instrumentarse los mecanismos necesarios para que el proceso de firma, tanto en instancia de generación del timbre como en instancia de firma final del documento PDF, se realice íntegramente en el desktop del firmante.

- √ La aplicación debe integrar con dispositivos criptográficos de almacenamiento de firmas y certificados, compatibles con las disposiciones técnicas emanadas en este sentido de la legislación nacional y provincial.
- √ Bajo ninguna circunstancia deben considerarse soluciones de implementación que impliquen la transferencia de la clave privada del firmante fuera del dominio de dispositivo criptográfico aplicado.

Paso 3: Proceso de Notificación y Envío por e-mail de Certificados;

Cada certificado generado, deberá ser adjuntado al cuerpo de un mail de notificación y enviado automáticamente a la cuenta de correo consignada por el participante en instancia de inscripción. El cuerpo del correo electrónico debe incluir como tema clara referencia al evento implicado y en su cuerpo la notificación de envío, un vínculo a la dirección web desde donde se puede descargar una copia del Certificado y direcciones o teléfonos de contacto para consultas o reclamos.
Si bien el Certificado en formato PDF, debe adjuntarse al correo electrónico, la previsión de incluir un vínculo al sitio de descarga atiende a brindar un medio alternativo de obtención del documento, para aquellos casos en que los servidores de correo filtren o impidan la descarga de archivos adjuntos.

Paso 4: Proceso de Publicación de Certificados:

Cada certificado emitido, firmado y timbrado, debe ser publicado en el sitio web del evento, y mantenido allí por un plazo no inferior a 90 días. En caso de que el evento no cuente con una página propia de difusión, el servicio podrá ser provisto desde el portal de la Unidad de Reforma y Modernización del Estado del Gobierno de Mendoza y/o desde las páginas institucionales de las entidades organizadoras.

Como mecanismo de acceso, se deberá diseñar una página de consulta por documento (DNI, pasaporte, Cédula de Identidad, otros) que permita acceder directamente al documento correspondiente.

Paso 5: Proceso de almacenamiento de Certificados:

El paso final a realizar, luego de emitidos, enviados y publicados los Certificados de asistencia con timbre y firma digital, para un evento particular, será la generación de una copia del repositorio de Certificados, en un dispositivo de almacenamiento secundario como CD o DVD.

Dicha copia deberá ser etiquetada y entregada a los responsables de la organización del evento para su archivo histórico.

Persistencia de datos

Se determinan en este punto de manera genérica, los repositorios de datos que se deberán mantener para garantizar la persistencia de la información relevante.

a. Base de datos de Inscripciones y acreditaciones: para cada evento deberá mantenerse una tabla con detalle de los inscriptos al evento y su efectiva acreditación posterior. La estructura genérica de esta tabla deber permitir individualizar a las personas inscriptas, individualizar a las personas acreditadas, jerarquizar la participación de un individuo de acuerdo a su rol en el evento (asistente, expositor, organizador, patrocinador, etc.).

b. Repositorio on-line de Certificados emitidos: los Certificados emitidos por la aplicación, debidamente timbrados y firmados, deberán ser mantenidos en este repositorio por un período no inferior a los 90 días desde su fecha de emisión. Dicho repositorio deberá permanecer en un servidor web a fin de que los mismos puedan ser accedidos desde Internet.

c. Repositorio permanente de Certificados emitidos: los Certificados emitidos por la aplicación para un evento particular, debidamente timbrados y firmados, deberán almacenarse en un dispositivo de soporte secundario, tal como CD o DVD, debidamente etiquetado, que será oportunamente entregado a los responsables de la organización del mismo.

d. Logs de Transacciones: se deberán mantener archivos de seguimiento de las transacciones realizadas en el sistema.

e. Buzones de email: con fines de seguimiento y control deberán mantenerse los correos electrónicos enviados y recibidos por la aplicación por un período de 90 días.

Salidas Planeadas

Las salidas básicas que deberá proveer la aplicación contemplan:

a. Certificados de Asistencia: documentos en formato .pdf (Portable Document Format) con el cuerpo del certificado más el timbre digital correspondiente y la firma digital de la/las autoridades competentes.

b. Emails de notificación: mensajes de correo con la notificación del envío de Certificado y el correspondiente documento adjunto. Por las características descriptas en el proceso de notificación y envío *(Ver paso 4)*, es mandatario que el cuerpo de estos correos electrónicos se diseñe dinámicamente en formato HTML

c. Pantallas de notificación de secuencia: deberá informarse al operador sobre el estado de procesamiento de una transacción hasta el momento en que la misma se complete.

d. Pantalla de notificación de errores: cualquier excepción producida en la aplicación que no pudiera ser resuelta por los manejadores de excepciones, deberá ser notificada al operador, con detalle de los motivos que la provocaron y referencia al soporte o ayuda al cuál deben contactarse para tomar las medidas correctivas pertinentes.

e. Reportes de Certificados Emitidos: detalle de los certificados emitidos para un evento en particular, con acceso a los documentos .pdf.

f. Reportes de Certificados Enviados: detalle de los certificados enviados por email en relación a un evento en particular.

2) Diseño Detallado

Descripción General de Aplicaciones

Tal como ha sucedido en experiencias previas que implican el uso de timbre y firma digital, el funcionamiento integral de la solución deberá soportarse sobre tres aplicaciones totalmente independientes, las cuáles operarán complementariamente en el circuito de emisión y verificación respectivamente.

a. Aplicación de emisión de los Certificados de Asistencia: Aplicación dinámica para la web, basada en una arquitectura cliente-servidor que permite la generación, timbrado, firma y envío de Certificados de Asistencia para cada uno de los inscriptos efectivamente acreditados en un evento particular. Las características funcionales de esta aplicación, deben ajustarse en etapa de desarrollo a la especificación de requerimientos descripta en la documentación de diseño global.

b. Aplicación de validación de Firma Digital: el proceso de validación on-line de firmas digitales y su cadena de Certificados de firma X.509, aplicados sobre los documentos PDF emitidos, se resuelve de manera adecuada y completa mediante el software Acrobat Reader V.6 o superior. Dado que esta aplicación puede descargarse libremente desde la red, e integra automáticamente con los navegadores de Internet, consideramos que es la solución ideal para que los usuarios finales puedan verificar de manera distribuida la validez y garantías de sus Certificados de Asistencia. Por lo expuesto, no se requiere desarrollo alguno en este sentido.

c. Aplicación de validación de Timbre Digital: en caso de que los Certificados de Asistencia deban ser validados en forma impresa, se deberá contar con una aplicación standalone, que permita verificar la integridad y validez del timbre digital. El software toma la cadena de caracteres que ingresan desde el puerto de teclado conectado al scanner y reconstruye los caracteres de la firma, la clave pública y el texto en claro que se firmó. Hecho esto, provee estos datos junto al Certificado a un módulo de verificación de firma que valida la integridad de la firma en relación a los datos firmados, mostrando un mensaje final al funcionario, sobre la validez o no del timbre incluido en el Certificado en cuestión. Esta aplicación ha sido previamente desarrollada por el Equipo de Firma Digital, y por sus características flexibles y portables, entendemos se adapta perfectamente en esta oportunidad a la experiencia.

Arquitectura y Plataforma Tecnológica

Para el desarrollo e implantación de las aplicaciones, se aprovechará la plataforma tecnológica utilizada en desarrollos previos de Firma y Timbre Digital. Esto, además de suponer un mayor aprovechamiento de la capacidad instalada y los conocimientos adquiridos, implica utilizar un conjunto de herramientas debidamente probadas en torno de implantaciones vinculadas a tecnologías PKI.

Se describe a continuación detalladamente el software de base, IDEs y librerías de software, formatos y estándares a los cuáles deberá ajustarse el desarrollo de la aplicación.

Arquitectura de Servidor: del lado del servidor deberá instalarse una plataforma J2SDK 1.6 y un servidor de aplicaciones web *JBOSS 4.0.1 o superior* que permita la ejecución de servlets java.

Para la generación de los documentos .pdf y el codebar PDF417, se utilizará la API java iText ver. 1.5, instalada en el classpath de la aplicación. Alternativamente, para contemplar la posibilidad de generación de objetos de firma PKCS#7 deberá incorporarse al deploy del proyecto en el servidor el paquete BouncyCastle (http://www.bouncycastle.org).

Las aplicaciones deberán deployarse sobre el Application Server como un archivo empaquetado .ear, con su configuración expresada en documentos XML. Su configuración y parametrización debe permitir amplia portabilidad del software desarrollado sobre entornos Linux y/o Windows

Cabe recordar que tanto la plataforma java, como las librerías de clases y el application server requeridos en el servidor, son software de libre acceso.

Configuración del cliente: los clientes que se conecten a la aplicación, tanto desde la Intranet de Gobierno, como usuarios externos, sólo deberán necesitar un browser de Internet y Adobe Acrobat Reader 6.0 o superior. Deberá excluirse del desarrollo la utilización de componentes activos que pudieran ser filtrados por configuraciones de seguridad de los browsers.

Selección del formato de los documentos Digitales

Debido a los buenos resultados obtenidos en experiencias previas y a los requerimientos especificados para este caso en particular, el desarrollo deberá generar los Certificados de Asistencia en formato PDF (Portable Document Format), dado que este formato constituye un estándar para la publicación de documentos en Internet, contribuye a la inalterabilidad de los documentos y además facilita la incorporación del código de barras PDF417 conteniendo el timbre digital. Otro punto en favor del uso de documentos .pdf, tiene que ver con las posibilidades que el estándar aporta al diseño gráfico de los documentos. Aspecto que consideramos relevante en el marco de la presente experiencia.

Selección de los lenguajes de desarrollo

La programación deberá hacer uso de los siguientes lenguajes:

- Servlets y Clases: *Java (J2EE).* El desarrollo deberá soportarse sobre servlets basados en J2EE. No se prevé en las especificaciones de diseño la utilización de tecnología de WebServices o JavaBeans.
- Interface web: La interfase web del proyecto deberá sustentarse sobre código .jsp (Java Server Page) para la generación dinámica de código HTML/*Javascript.*

Librerías y paquetes de clases a utilizar

El lenguaje Java, nativamente orientado a objetos, explota superlativamente la posibilidad de escalar su potencialidad con un sinnúmero de librerías de clases reutilizables, con propósitos específicos, proporcionadas gratuitamente por la comunidad de desarrolladores de java y en ocasiones por empresas u organismos que realizan desarrollos en esta línea. En particular el presente desarrollo con timbre digital deberá utilizar las siguientes librerías (APIs Java), cuyo propósito y características principales se describen a continuación:

API iText ver.1.5 o superior: iText es un proyecto Sourceforge mantenido por una comunidad abierta de desarrolladores de software libre. Es una librería de clases Java que permite la generación dinámica de documentos pdf totalmente compatibles con la PdfReference 1.6. Las clases provistas por iText son muy útiles para generar documentos de sólo lectura independientes de la plataforma que contentan texto, listas, tablas e imágenes. En nuestro caso particular, la utilizamos por las siguientes características:

- Describe objetos de alto nivel que permiten generar rápidamente los principales componentes de un documento pdf.
- Incorpora la posibilidad de manejar el contenido interno de documentos pdf a bajo nivel. Es decir manipular directamente el formato interno de los documentos generados.
- El código de los documentos pdf generados es altamente compatible con las especificaciones de la Adobe PdfReference 1.6. Esta especificación describe el formato interno de los documentos pdf.
- Incorpora una jerarquía de clases completamente dedicada a la generación de Codebar PDF417 con excelentes características de optimización de la imagen generada, posibilidades de customización muy amplias e incorporación del procedimiento MacroPdf417.
- Incorpora una jerarquía de clases completamente dedicada a la generación de firmas digitales sobre documentos pdf. que integra completamente con el paquete BouncyCastle para la generación y verificación de objetos de firma PKCS#7 y la API java.security utilizada en el proceso de firma e integración con los midlware de dispositivos criptográficos (tokens de firma).
- iText es especialmente útil en combinación con tecnología Java(TM) basada en Servlets, que como documentamos anteriormente es el esquema de servicio a implementar en el servidor elegido.

- Existe excelente documentación sobre la API y una comunidad de desarrollo muy activa con foros de consulta y documentación en permanentemente mantenimiento
- La librería cae dentro de la categoría de software libre y puede descargarse gratuitamente desde http://www.lowagie.com

Paquete BouncyCastle: librería java de libre acceso que provee clases para manipular objetos de firmas digitales, Certificados, claves públicas y privadas, keystores y algoritmos de firma. Este paquete permite el empaquetamiento de firmas y certificados digitales en una envoltura PKCS#7, requerida para la concreción de firmas digitales en documentos PDF (Portable Document Format) bajo la especificación PDF Reference 1.6; y su posterior verificación.

Paquete Java.Security: Dentro de la plataforma J2SDK 1.5.0 se incorpora el paquete de clases Java.Security. Este package describe clases que permiten manipular objetos de firmas digitales, Certificados, claves públicas y privadas, keystores, algoritmos de firma, etc. Es el conjunto nativo de clases que proporciona el lenguaje para la manipulación de firmas y certificados digitales. En particular, las especificaciones de diseño prevén la utilización de clases provistas en este paquete para generar, tomando un certificado X.509 v3, una firma SHA1withRSA representada en formato PKCS#1 (CodeBase64) que constituye la firma digital de los elementos de datos esenciales del Certificado. Esta firma deberá luego ser codificada en codebar PDF417 constituyendo así el timbre digital.

Driver de Conexión JDBC: La conexión desde los módulos de la aplicación a la Base de Datos deberá resolverse mediante el Driver JDBC jdbcpostgresql 7.2 o superior. Dicho driver deberá manejar las cadenas de conexión a la base de datos con identificación de usuarios y claves de conexión. Así mismo, deberá parametrizarse la conexión para la selección de Charsets que permitan una interpretación correcta de cadenas alfabéticas con símbolos especiales del idioma español tales como ñ y letras acentuadas.

Determinación de niveles de Seguridad y Acceso al Sistema

El servlet de generación, timbrado, firmado y envío de Certificados deberá ser de acceso restringido a usuarios operadores habilitados para un evento particular.

La seguridad en la generación del Certificado deberá implementarse mediante la generación la firma digital y el timbre digital sobre el mismo. Dichas firmas, basadas en tecnología PKI, garantizarán la originalidad, integridad y autoría del documento.

El legítimo interés de los solicitantes en requerir un Certificado de Asistencia será verificado mediante la comprobación de su dirección de email particular, a la cual le será remitido el Certificado; y mediante el requerimiento de su DNI, pasaporte u otro documento que acredite identidad, ante la posibilidad de descarga del Certificado vía web.

La protección de los certificados de firma digital estará garantizada por el uso de dispositivos criptográficos usb.

La aplicación de validación de timbres, instalada en las oficinas que así lo requieran, es de acceso exclusivo a usuarios con privilegios de administración u operación sobre el sistema, validados mediante esquemas de login-password.

Tolerancia a fallas y gestión de errores

Las fallas y errores que pueden producirse en tiempo de ejecución *(por ej.: por problemas de conexión, caída del application server, errores en el formato de los documentos pdf, ,ausencia de un reader, etc.)* deberán gestionarse bajo el concepto de ***manejo de excepciones***.

Lo anterior implica que el sistema genera una excepción ante un error o falla que es tratada por un manejador de excepciones especialmente diseñado para tratar particularmente el suceso acontecido.
De esta forma se separa el código de manejo de errores, del código que atiende a la lógica principal del desarrollo, facilitando su comprensión y mantenimiento posterior. Así mismo, un cuidadoso manejo de excepciones implica en nuestro desarrollo una mayor tolerancia a fallas, lo que se traduce en bajo riesgo de caídas del sistema.
Es mandatario que cualquier excepción que se produzca en la ejecución de los procesos internos descriptos en la documentación de diseño global, sea mostrada al usuario operador mediante ***íconos gráficos*** que le permitan identificar claramente los Certificados que por esta causa no fueron debidamente generados, o firmados, o timbrados, o enviados, con detalle de la instancia que no pudo ser debidamente completada. Esto permitirá tomar las medidas correctivas necesarias para cada caso particular que se presente.

Fuentes de Datos

La base de datos de Inscripciones y Acreditaciones, deberá instalarse sobre el motor PostgreSql 7.3 o superior. Este motor se ejecuta en un equipo independiente del Application Server y será accedido concurrentemente por los procesos de inscripción, acreditación y emisión de Certificados.

La estructura de la base de datos deberá ajustarse genéricamente al siguiente ***modelo***:
Charset: windows-1252 o ANSI1
Esquema: único
Vistas: ninguna
StoreProcedures y Triggers: ninguno
Funciones: ninguno
Usuario de conexión: inscripcion1, consulta1
Lenguaje de Consulta: ajustarse a ANSI SQL

VI. Implementación de experiencia A

Se han completado en esta etapa las tareas de desarrollo, implementación y planificación de evaluación del trámite de emisión on-line, del Certificado de Vigencia emitido por la Dirección Provincial de Personas Jurídicas según las especificaciones de diseño global y detallado previsto. La documentación del proceso de implementación involucra: el desarrollo de aplicaciones de acuerdo al diseño propuesto, su implantación en la plataforma de producción, el ajuste de protocolos y configuraciones y la generación de certificados digitales.

A) Desarrollo e implementación:

Se lleva a la práctica la experiencia piloto real. Se emiten los certificados de firma digital, se realizan las configuraciones, instalación de protocolos, ajustes y desarrollos necesarios en el equipamiento informático

De acuerdo a las especificaciones generales de diseño documentadas en el informe previo, la aplicación de solicitud, aprobación y generación de Certificados de vigencia, fue codificada como una solución basada en arquitectura cliente-servidor para la web cumpliendo con las siguientes características técnicas:

Portabilidad y escalabilidad:

El desarrollo se ajusta a un modelo de tres-capas e implementa una arquitectura Cliente-Servidor. Del lado del servidor se requiere el motor de base de datos PostgreSQL 8.1 al cual se accede a través de un conector JDBC incorporado como librería externa en la aplicación, la plataforma J2EE y cualquier servidor de aplicaciones web que interprete código JSP (*Java Server Pages*) y Servlets Java. En particular se ha utilizado para el desarrollo el *Application Server* JBoss 4.0.1 – GA con Tomcat 5.0 embebido, pero cualquier otro

que cumpla los requisitos es aceptable. Del lado del cliente, sólo se necesita un browser de Internet y algún pluggin de firma digital de documentos PDF.

Se debe destacar que el desarrollo sobre plataforma J2EE garantiza la portabilidad del software a entornos Linux o Windows; y que además tanto la plataforma java, como el motor de base de datos y el application server requeridos en el servidor, son software de libre acceso.

Arquitectura web:

Todo el front-end del sistema está basado en *interfase web* con el usuario. Esto posibilita:

- Libre acceso a la aplicación y sus servicios desde cualquier puesto de trabajo conectado a la Intranet de Gobierno sin necesidad de instalación previa de aplicaciones cliente.
- Carga de la complejidad del lado del servidor, con la ventaja de que los usuarios pueden consultar o gestionar solicitudes de certificación desde un cliente delgado. Costo cero en inversión en Hardware.
- Mayores posibilidades de escalabilidad.
- Costo cero en licencias de software cliente.
- Mantenimiento y resolución de problemas centralizado.
- Menor esfuerzo de capacitación y aprendizaje intuitivo de los usuarios.

Seguridad y Acceso:

El módulo de consulta y gestión de solicitudes de certificación pendientes es de acceso exclusivo a usuarios con privilegios de administración u operación sobre la aplicación. La seguridad en el acceso a las aplicaciones y transacciones sobre la base de datos se implementa a través de:

- Control de privilegios de usuarios en la conexión a la base de datos.
- Sitio seguro con validación de certificado de cliente en el Application Server.

Son usuarios autorizados, el personal de la Dirección de Personas Jurídicas que posea Certificado Digital X509.v3 emitido por la AC-URME (Autoridad Certificante Prototipo de la Unidad de Reforma del Estado) para registrar su acceso al sistema.

Código Fuente

La programación hace uso de los siguientes lenguajes:

- Consultas y transacciones sobre el motor de base de datos: *ANSI-SQL*
- Procedimientos almacenados en la base de datos: *PL/SQL*
- Servlets y Clases: *Java (J2EE)*
- Interface web: *JSP, Javascript, HTML*

Formato de los documentos Digitales

Los Certificados de Vigencia son construidos dinámicamente una vez aprobada la solicitud, según la especificación PDF 1.6. Este formato es soportado por Acrobat Reader 6 o superior y ha sido testeado en múltiples readers pdf alternativos, sin identificar inconvenientes.

Firma Digital

Con el objetivo de garantizar interoperabilidad con los principales manejadores de firma, la aplicación utiliza los algoritmos estándar de hash y firma digital SHA-1/RSA. Se aplican claves RSA de 1024 bits.

El subproceso de firma está implementado en un applet java que opera localmente en la máquina del firmante. Es una condición sumamente importan-

te que todo el proceso de firma se concrete de forma stand-alone y bajo completo control del firmante.

Timbre Digital

El Timbre Digital (Nube de puntos PDF417) es generado por el Servidor de Timbrado en función de los datos firmados y agregado dinámicamente al Certificado correspondiente.

- **Nivel de Corrección de Errores:** errorLevel 5
- **Modo de Compactación:** modo de optimización.
- **Capacidad de codificación y representación de la firma:** ASCII - Binario codificado en Base64.
- **Estructura de la información codificada:**

  <<Cadena de Datos firmados>> + *<<inscripción obtenida como parámetro>>* + "-" + *<<fecha pedido obtenido como parámetro>>* + "-" + *<<transacción obtenido como parámetro>>* + "-" + *<<apellido y nombre del solicitante obtenido como parámetro>>* + "-" + *<<Nro. Documento del solicitante obtenido como parámetro>>* + ***<<Cadena de firma codificada en CodeBase64 (PKCS#1)>>*** + ***<<Clave pública>>***
- **Condiciones de dimensión y ubicación:**
  - aspect ratio: 1:3 (relación de aspecto)
  - quiet zone: 1 cmt. (perímetro blanco)

Desarrollo

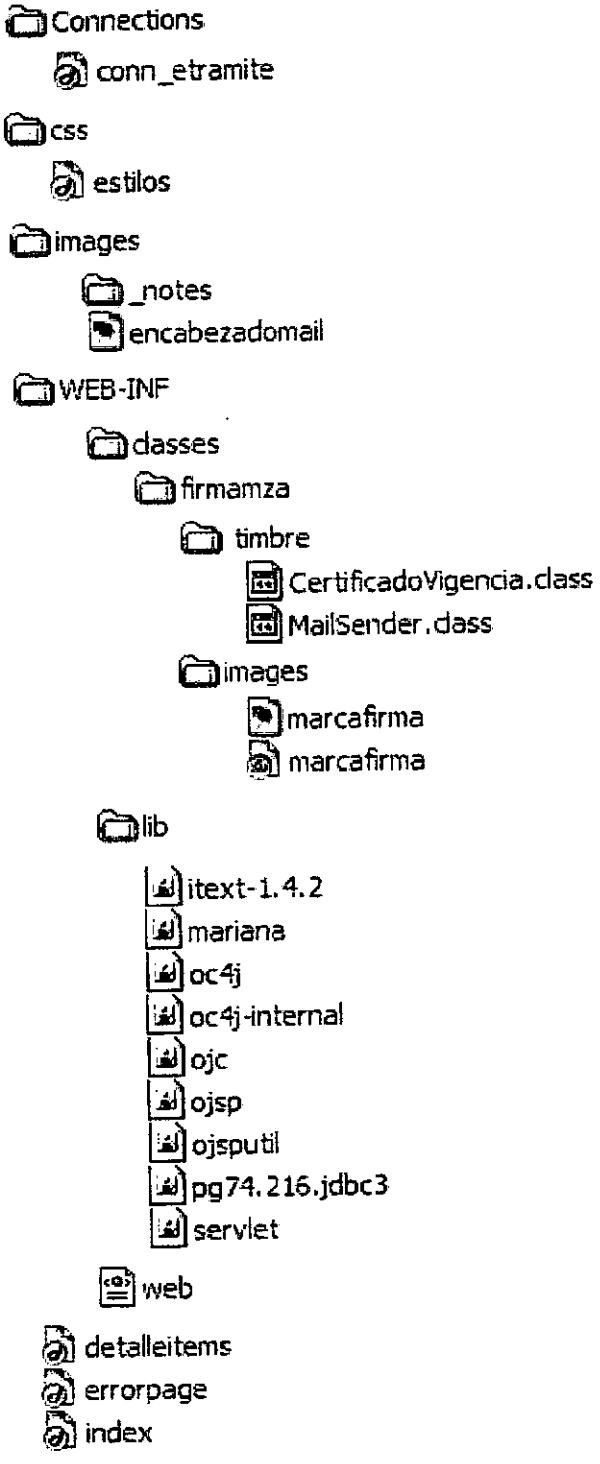
En las tareas de desarrollo se utilizó el IDE JDeveloper 10g por cuanto esta herramienta ha demostrado integrar muy bien con JBoss permitiendo el deploy directo sin configuraciones adicionales; y satisface las necesidades de programación determinadas en términos de herramientas visuales, de edición de código, de depuración y ayudas.

El front-end de la aplicación, que permite a los funcionarios de la Dirección de Personas Jurídicas administrar la lista de solicitudes pendientes fue codificado en lenguaje JSP (Java Server Pages).

La lógica de proceso fue implementada mediante un Servlet Java encargado de gestionar la conexión a Bases de Datos, generar dinámicamente el Certificado de Vigencia (en caso de que la solicitud fuera aprobada), y emitir automáticamente los correos electrónicos de remisión o rechazo del Certificado solicitado.

La base de datos asociada a la aplicación, se desarrolló sobre un motor de base de datos Postgress independiente.

Como se explicó previamente, el conjunto completo de código que compone la aplicación ha sido desarrollado utilizando tecnologías Java 2 Enterprise Edition, manteniendo de esta forma compatibilidad tecnológica con el resto de los desarrollos realizados en el marco del Proyecto de Firma Digital e integración directa con la plataforma Linux + J2EE Application Server. Todos los componentes de la aplicación fueron empaquetados el contenedor ***certificado-vigencia.ear***, cuya estructura se describe a continuación y deployados sobre JBoss 4.0.1 – GA con Tomcat 5.0 embebido.


Connections
conn_etramite
css
estilos
images
_notes
encabezadomail
WEB-INF
classes
firmamza
timbre
CertificadoVigencia.class
MailSender.class
images
marcafirma
marcafirma
lib
itext-1.4.2
mariana
oc4j
oc4j-internal
ojc
ojsp
ojsputil
pg74.216.jdbc3
servlet
web
detalleitems
errorpage
index

Paquete completo de módulos y librerías que componen la aplicación

La página ***index.jsp,*** implementa la consulta de solicitudes de certificación pendientes. Este código hace uso del modulo de ***conn_etramite.jsp*** en donde se definen las cadenas de conexión a la base de datos.

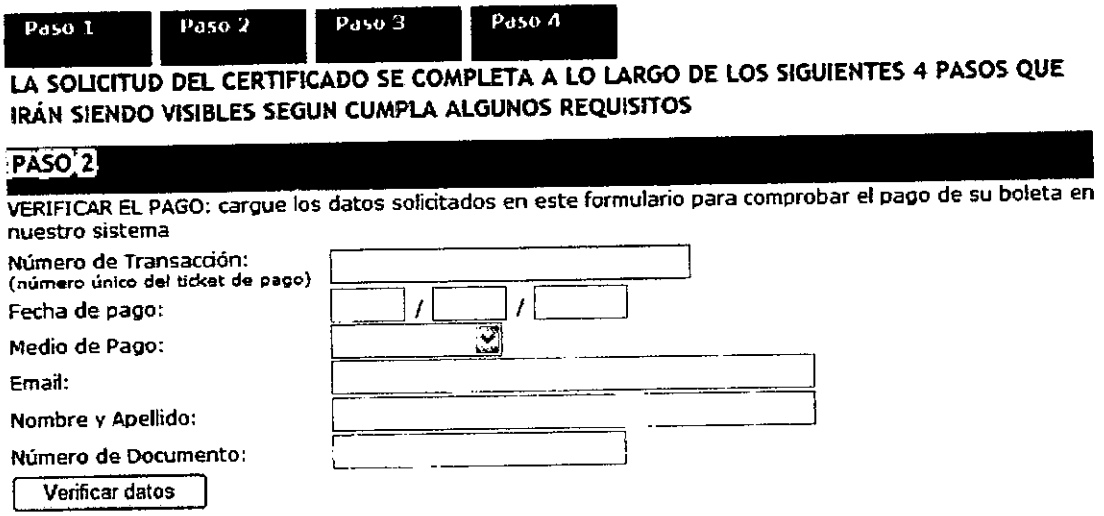
El módulo central está constituido por la clase ***CertificadoVigencia.class*** que implementa el servlet de generación del Certificado de Vigencia y dispara las notificaciones por mail de envío o rechazo del mismo. Este servlet y sus clases subsidiarias, tales como ***MailSender.class*** que implementa la salida de correo, han sido implementados según especificaciones de diseño previamente documentadas.

La aplicación completa fue deployada sobre JBoss 4.01 – GA con Tomcat 5.0 embebido. Complementariamente, se desarrollaron pruebas de deploy de la aplicación sobre el servidor de aplicaciones Tomcat 5.0 y sobre el Oracle Application Server corriendo tanto sobre Linux como sobre Windows XP. Se comprobó así la portabilidad directa del servicio a otras plataformas tecnológicas.

La solución desarrollada e implementada comprende, según especificaciones de diseño, los siguientes subprocesos:

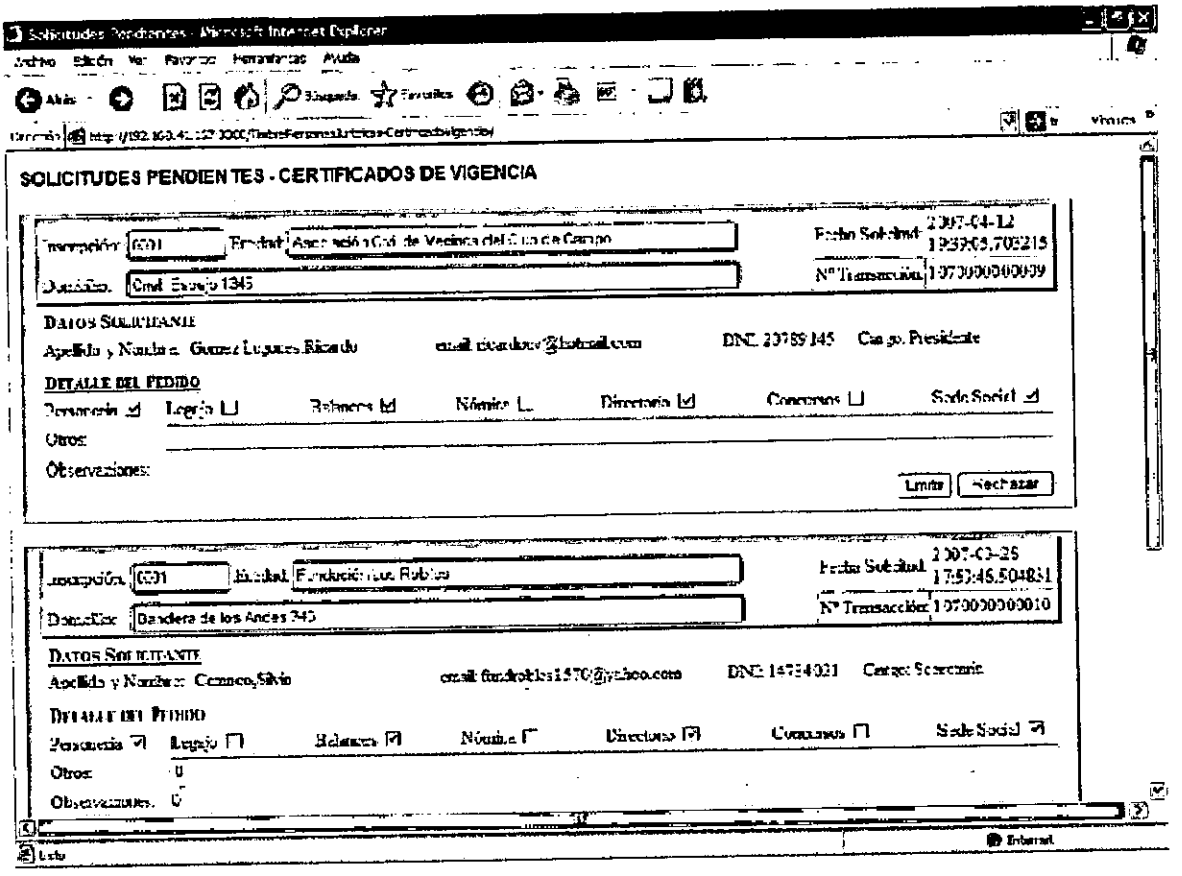
1. ***Formulario de solicitud*** de Certificados de Vigencia cursadas por responsables acreditados de entidades registradas en la Dirección de Personas Jurídicas. Las solicitudes son remitidas mediante formularios HTML disponibles en la Guía de Trámites, cuyos datos relevantes son almacenados de manera persistente en la base de datos dispuesta a tal fin.

CERTIFICADO DE VIGENCIA - FUNDACIONES



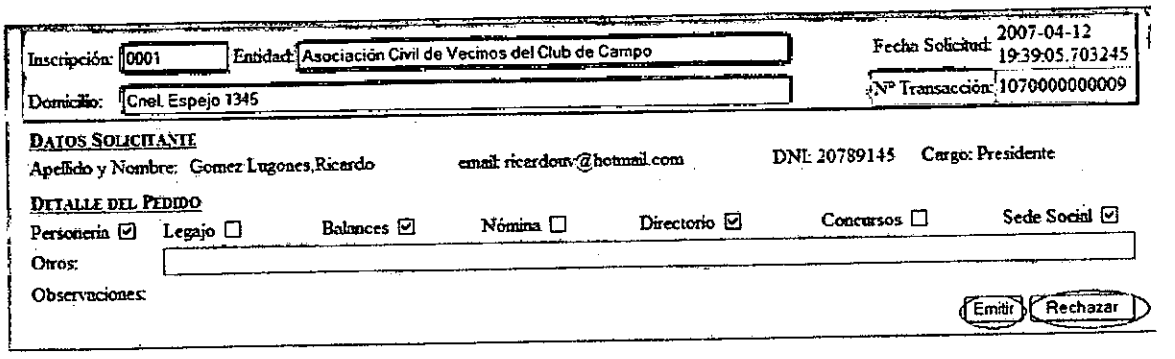
Importante: Estos formularios HTML han sido implementado sólo para entidades exentas de pago, por el trámite de solicitud de Certificado de Vigencia.

2. ***Consulta de solicitudes pendientes:*** consulta web disponible en la Intranet de Gobierno, que permite a los responsables de la administración del procedimiento (personal asignado de la Dirección de Personas Jurídicas) obtener de la aplicación, el reporte de solicitudes pendientes de atención. En dicha consulta, consta para cada solicitud pendiente, el conjunto de datos que permita identificar unívocamente el pedido, la entidad involucrada, el responsable que cursa la solicitud y el detalle de datos a Certificar.



Para cada solicitud pendiente, se otorga la posibilidad al funcionario de modificar los datos que corresponde Certificar y agregar otros datos que se considere pertinente incluir en el Certificado.

3.Decisión de Emisión/Rechazo: Para cada solicitud pendiente, los funcionarios responsables deberán ejecutar un proceso manual, basado en la información provista en la solicitud, más la que consta en los libros de inscripciones. Dicho proceso permitirá determinar la pertinencia o no de la emisión del Certificado de Vigencia, en función de lo cuál activarán en el sistema el proceso de Emisión o Rechazo respectivamente.



Emisión: Subproceso encargado de emitir el Certificado de Vigencia, timbrado digitalmente con detalle de los datos solicitados, tales como fecha de presentación del último balance o detalle de la constitución del Directorio. Dicho proceso genera en línea el Certificado y lo adjunta a un email de notificación, el cuál es enviado automáticamente a la dirección de correo consignada en la solicitud.

Gobierno de Mendoza

firma Digital

Sr./a. Gomez Lugones,Ricardo

Adjunto al presente correo encontrará el Certificado de Vigencia solicitado para Asociación Civil de Vecinos del Club de Campo remitida a esta Dirección con fecha 2007-04-12 19:39:05.703245, a través del sitio web www.trámite.mendoza.gov.ar

Sin otro particular, saluda a Ud. Atentamente.

Dra. María Elena Sotano
Directora

Ante cualquier duda comunicarse con: Dirección de Personas Jurídicas - 4492189

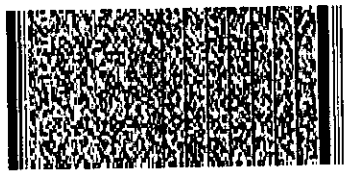
Ficheros adjuntos:

certificado.pdf 11 k [application/octet-stream] Descargar

Gobierno de Mendoza

Dirección de Personas Jurídicas

CERTIFICO que la entidad **"ASOCIACION CIVL DE VECINOS DEL CLUB DE CAMPO"**, obtuvo su autorización para funcionar por Resolución 1942 del 18 de Octubre del 2006,la que se encuentra vigente. Su legajo interno es el N° 5576. La entidad tiene su último balance presentado al 30/04/2007. El presente certificado se expide a solicitud de la interesada, para ser presentado ante las autoridades que lo requieran en la ciudad de Mendoza a los veintidós días del mes de Noviembre del año dos mil siete.----------



Rechazo: En caso de que la decisión fuera negativa respecto de la solicitud, el sistema emite y envía automáticamente mail de rechazo con detalle de los motivos que justifican la decisión.

Gobierno de Mendoza

firma Digital

Sr./a. Gomez Lugones,Ricardo

Cumplimos en informar que la Solicitud de Certificado de Vigencia de Asociación Civil de Vecinos del Club de Campo remitida a esta Dirección con fecha 2007-04-12 19:39:05.703245, a través del sitio web www.trámite.mendoza.gov.ar ha sido rechazada por: no registrarse presentación de último Balance en tiempo y forma

Por tal motivo, no podemos expedir el Certificado de Vigencia solicitado.

Asi mismo, informamos a usted que podrá reutilizar por única vez, el ticket de pago electrónico abonado para realizar nuevamente esta solicitud una vez cumplimentado los requerimientos.

Sin otro particular, saluda a Ud. Atentamente.

Dra. María Elena Sotano
Directora

Ante cualquier duda comunicarse con: Dirección de Personas Jurídicas - 4492189

Plataforma de Producción

La plataforma de producción donde se montó la aplicación está compuesta del application Server, encargado de distribuir los servicios de la aplicación a sus usuarios y el Motor de Base de datos, en donde se implementa la persistencia de datos administrados por el desarrollo.

Servidor de Aplicaciones

Una vez concluido el desarrollo se instaló el paquete ***certificadovigencia.ear*** en el Application Server de producción. Estas actividades implicaron tareas de configuración y ajuste de las aplicaciones en el lado del servidor.

Se describe a continuación la plataforma tecnológica operativa en el servidor y las configuraciones realizadas.

Application Server: Entorno de producción en Intranet.
Servidor Linux Red Hat
Servidor de Aplicaciones JBoss 4.0.4.GA
WebServer Tomcat 1.5
Plataforma J2EE – jdk1.5.0_08
Librerías criptográficas JCE – BouncyCasttle (Open Source)
Librerías PDF417 – iText (Open Source)

A nivel de configuraciones, se definió el contexto de activación de la plataforma web y un virtual host para el mismo en el archivo de configuración del servidor de aplicaciones. Se securizó el acceso lógico a la aplicación ***.ear*** que contiene la aplicación compilada y se definieron usuarios autorizados para su administración.

Para favorecer la portabilidad futura de la aplicación, las librerías de clases Java necesarias para su correcto funcionamiento fueron empaquetadas junto al resto del código en el módulo .ear. Entre ellas, la API iText 1.5.jar y la API firmadigital.jar con clases subsidiarias programadas internamente por el Equipo de Desarrollo de este proyecto.

Motor de Base de Datos

Se migró la estructura de la Base de Datos de desarrollo al motor de base de datos en producción, Postgres 8.01 corriendo sobre servidor Linux RedHat en un equipo independiente, sin interconexión a la red pública.

La estructura de la base de datos de la aplicación se ajusta al siguiente modelo:
Charset: windows-1252
Esquema: único

Vistas: ninguna

StoreProcedures y Triggers: ninguno

Funciones: ninguno

Usuario de conexión: consulta1

Lenguaje de Consulta: ajustarse a ANSI SQL

Tabla de Solicitudes Pendientes:

Campo	*Tipo*	*Descripción*
id_internopj	VARCHAR 11	Nº Interno de identificación de la entidad en el Registro Provincial de Personas Jurídicas. Este código alfanumérico permite identificar unívocamente a la entidad.
id_transc	VARCHAR 6	Nº único de transacción. Este número permite identificar unívocamente la solicitud. Deberá generarse correlativamente a partir de 000001
Entidad	VARCHAR 80	Nombre o identificación de la entidad, reservado en el Registro Provincial de Personas Jurídicas
domicilio	VARCHAR 60	Domicilio registrado de la entidad.
fechapedido	DATE	Fecha de generación de la solicitud de Certificado.
apellidosolicita	VARCHAR 30	Apellido del responsable acreditado de la entidad, que emite la solicitud o pedido de certificación.

nombresolicita	VARCHAR 30	Nombre de pila del responsable acreditado de la entidad, que emite la solicitud o pedido de certificación.
Email	VARCHAR 60	Dirección de correo registrada por el solicitante. A este email deberán ser remitidos las notificaciones de emisión o rechazo de Certificados. Así como también cualquier notificación intermedia que se remita.
dnisolicita	VARCHAR 8	Documento Nacional de Identidad del solicitante.
Cargo	VARCHAR 60	Descripción del cargo del solicitante en la entidad.
itempersoneria	BOOLEAN	Bandera que activa o no la certificación de personería jurídica.
itemlegajo	BOOLEAN	Bandera que activa o no la certificación de legajo.
itembalances	BOOLEAN	Bandera que activa o no la certificación de último balance presentado.
itemnomina	BOOLEAN	Bandera que activa o no la certificación de nómina.
itemdirectorio	BOOLEAN	Bandera que activa o no la certificación de constitución de directorio.

itemconcursos	BOOLEAN	Bandera que activa o no la certificación de antecedentes en concursos preventivos de la entidad.
itemsedesocial	BOOLEAN	Bandera que activa o no la certificación de constitución de sede social de la entidad.
itemotros	BOOLEAN	Bandera que activa o no la certificación de otros ítems no previstos en la parametrización descripta previamente.
observación	VARCHAR 120	Campo alfanumérico para indicar el cuerpo de texto a agregar en el certificado en caso de que se active la bandera itemotros.
Estado	ENUM {1,2}	Enumeración con valores 0 ó 1. Puesta a 0, indica que el estado de la solicitud es: *"pendiente de atención"*. Puesta a 1, indica que el estado de la solicitud es *"procesada"*.

La conexión desde los módulos de la aplicación a la Base de Datos se resolvió mediante el Driver de conexión JDBC jdbcpostgresql 7.3, el cual fue empaquetado como librería java en el módulo certificadovigencia.ear. Dicho driver recibe y gestiona las cadenas de conexión a la base de datos con identificación de usuarios y claves de conexión.

Emisión de Certificados

En etapa de desarrollo se trabajó con un Certificado de Prueba a nombre de ***usuario de prueba 1***, emitido por la AC-URME (Autoridad Certificante prototipo de la Unidad de Reforma y Modernización del Estado), con un período de validez de un año.

Una vez concluido el desarrollo y comprobado el correcto funcionamiento de todo el circuito de generación, firma y timbrado digital de los Certificados de Vigencia y el correcto funcionamiento de la aplicación en la plataforma de producción, se procedió a solicitar y emitir el Certificado a nombre de la Dirección de Personas Jurídicas de la Provincia, y los Certificados AC-URME de acceso al sitio seguro SSL. Dichos certificados digitales constituyen el instrumento de certificación utilizado en la experiencia. Fueron emitidos por la ONTI y la AC-URME (Autoridad Certificante prototipo de la Unidad de Reforma y Modernización del Estado) respectivamente, con un período de validez de un año y respetando los procedimientos establecidos en la política de certificación.

B) Puesta en Marcha de la implementación:

Puesta en marcha

Concluida la etapa de desarrollo e implementación se llevó a cabo la Puesta en Marcha de la implementación y se capacitó a usuarios.

Con la aplicación en producción se inició la fase de capacitación a usuarios cuyas acciones describimos a continuación.

Capacitación a Usuarios

Se identificaron para la experiencia dos tipos de usuarios a capacitar: el personal de la Dirección de Personas Jurídicas que gestiona el trámite y los responsables de entidades solicitantes, usuarios finales de la aplicación.

Se describen a continuación las acciones de capacitación y difusión emprendidas para cada uno de estos perfiles.

Personal de la Dirección de Personas Jurídicas: son los empleados públicos encargados de la gestión de información en el sistema y su administración. Estos funcionarios son quienes deciden, en base a comprobaciones manuales sobre los libros y presentaciones de cada entidad, si corresponde o no emitir el Certificado de Vigencia y determinar que ítems corresponde certificar. Si bien para estos usuarios, la introducción de Timbre Digital a los comprobantes de Retención de Ingresos Brutos es totalmente transparente y no genera ninguna modificación en su operatoria normal; son ellos, quienes interactúan con los responsables de las entidades solicitantes, atienden sus dudas y los orientan en su vínculo con los servicios de la aplicación. Por ello, resulta importante capacitarlos en la comprensión del concepto de Timbre Digital, las garantías que provee, sus alcances y los beneficios que genera tanto para la administración central como para los usuarios finales. Es importante lograr la adhesión de estos operadores a la experiencia por cuanto serán ellos multiplicadores de sus efectos hacia el público en general y las personas jurídicas en particular. En este sentido, se realizó con el grupo de operadores un entrenamiento intensivo tanto en los aspectos operativos del sistema, como en la toma de conciencia sobre la mejora de procesos y principios básicos introducidos por el timbrado digital. La capacitación se realizó en oficinas de la Dirección de Personas Jurídicas de la Provincia durante una jornada de 4hs.

Se trabajó sobre la aplicación puesta en producción y se mostró además la operación de la aplicación de validación del timbre. Por la simplicidad operativa de la aplicación de verificación, no se utilizó documentación específica, distinta de la ayuda incluida en la aplicación.

Usuarios finales del sistema: se incluye en este grupo a todos los responsables de personas jurídicas inscriptas, que estuvieran exentas de pago por el trámite de solicitud de Certificado de Vigencia. Con este grupo, se realizó una campaña de difusión on-line que explicó los alcances del nuevo servicio y la validez otorgada al Certificado por el timbre digital. Se fortaleció la idea de que esta nueva modalidad, los exime en adelante de asistir personalmente a los mostradores de la Dirección de Personas Jurídicas para requerir el Certificado y su posterior visita para retirarlo.

Se debe tener claro que la experiencia no propone como único canal, la solicitud web del Certificado, quedando operativos los mecanismos habituales de solicitud personal del Certificado, para aquellas entidades que por diversas razones así lo prefieran.

No obstante esto, se focalizó la difusión en los beneficios que la experiencia genera, por cuanto es un factor de éxito significativo, tener en cuenta que la apropiación por parte de los ciudadanos usuarios de cualquier trámite por Internet con timbre digital depende directamente de la utilidad que este le brinde. En particular, se expusieron como mejoras sustanciales: el ahorro de tiempos, la disminución de colas y las posibilidades de reducir problemas ante la distribución geográfica.

Soporte continuo y retroalimentación al sistema

Las etapas de capacitación y puesta en marcha, constituyen en toda implementación oportunidades de prueba funcional del sistema. De estas etapas, se obtiene en general retroalimentación para los diseñadores y desarrolladores, en función de la experiencia que aportan los actores involucrados en su operación y uso.

En nuestro caso particular, se han dejado previstos vínculos permanentes entre los expertos del proyecto de firma digital y los responsables afectados por la Dirección de Personas Jurídicas, a fin de identificar necesarios ajustes sobre el desarrollo de la herramienta informática o el circuito operativo que pudieran presentarse en el futuro; y emprender las acciones de mantenimiento

correctivo pertinentes. Así mismo, se espera que este vínculo, así como también el establecido con las autoridades de la Dirección, sean de utilidad en un futuro próximo, para extender la experiencia de timbrado a la emisión de otros comprobantes y certificaciones.

C) Evaluación de la experiencia:

Se definen métricas de evaluación que a futuro permitirán evaluar el éxito de la implementación

Describimos a continuación el sistema de evaluación de resultados que se aplicará. El modelo reúne un conjunto de indicadores y aspectos observables que permitirán identificar las ventajas comparativas del circuito y obtener conclusiones válidas sobre la experiencia.

Dicho diseño respeta el enfoque particular a los procesos específicos de la presente aplicación.

Este modelo se basa en métricas con las que, razonablemente, se puedan cuantificar las dimensiones que son de nuestro interés.

La siguiente tabla define los indicadores generales utilizados para medir el rendimiento de la aplicación.

EXPERIENCIA DE SOLICITUD/ENTREGA DE CERTIFICADO DE VIGENCIA CON TIMBRE DIGITAL Instrumento de Evaluación	
Indicadores Cualitativos	Métricas y Resultados

Satisfacción de los usuarios:

- Temática de reclamos
  Resistencia al cambio
  Grado de aceptación de funcionarios – Nivel de confianza
- Grado de aceptación del personal de Personas Jurídicas – Nivel de Confianza
- Solicitudes de transferencia tecnológica

Beneficios diferenciales:

- Reducción de gastos en formularios preimpresos
- Disponibilidad
- Seguridad
- Integridad de la Información
- Ahorros de tiempo

Marco legal:

- Impacto en normativa interna

Alcance:

- Participación de los sectores relacionados
- Difusión pública
- Difusión internacional

Indicadores Cuantitativos	Métricas y Resultados

Eficiencia:

- % de timbres emitidos correctamente
- Nro. de cert. emitidas válidas / Total de cert. emitidas mensuales
- Nro. de cert. emitidas rechazadas / Total de cert. emitidas mensuales
- % de fallas de sistema
- % de interrupciones del servicio
- Tiempos comparados
- Ahorros generados

Asistencia:

- Número de visitas de soporte mensuales

- Nivel de reclamos atendidos mensuales

Uso del Sistema:

- Cant. de consultas mensuales
- Cant. de mensajes negativos mensuales (a través de la Guía de Trámite)
- Cant. de mensajes positivos mensuales (a través de la Guía de Trámite)
- Cant. de cert. emitidas mensuales
- Cant. de verificaciones de certificación mensuales
- % de utilización de servicios (sobre el total de actores involucrados)

Calificación de la experiencia ponderada final

.....

VII. Implementación de experiencia B

Se han completado en esta etapa las tareas de desarrollo e implementación de la aplicación de emisión automática, de ***"Certificados de Asistencia digitales con firma digital"*** emitidos por el Gobierno de Mendoza y sus organizadores asociados, a participantes acreditados en los seminarios y foros que en la provincia regularmente se realizan.

La documentación del proceso de implementación involucra: el desarrollo de aplicaciones de acuerdo al diseño propuesto, su implantación en la plataforma de producción, y el ajuste de protocolos y configuraciones.

A) Desarrollo e implementación

Informar el desarrollo e implantación preliminar de la experiencia implica documentar las tareas de codificación de la aplicación de emisión, timbrado, firma, envío, publicación y almacenamiento de Certificados. De forma complementaria, se documenta también el desarrollo de la aplicación de inscripción on-line y el sistema de efectiva acreditación de asistentes a eventos.

Este conjunto de aplicaciones, cuyo diseño es genérico para cualquier tipo de evento, debe ser luego customizado y adaptado a cada experiencia en particular, previo a su ejecución en la plataforma de producción.

Consideraciones Generales

De acuerdo a las especificaciones generales de diseño documentadas en el segundo informe parcial del proyecto corriente, la aplicación de emisión de certificados de asistencia con firma y timbre digital, fue codificada como una solución basada en arquitectura cliente-servidor para la web cumpliendo con las siguientes características técnicas:

Portabilidad y escalabilidad:

El desarrollo se ajusta a un modelo de tres-capas e implementa una arquitectura Cliente-Servidor.

Del lado del servidor se requiere el motor de base de datos PostgreSQL 8.1 al cual se accede a través de un conector JDBC incorporado como librería externa en la aplicación, la plataforma J2EE y cualquier servidor de aplicaciones web que interprete código JSP (*Java Server Pages*) y Servlets Java. En particular se ha utilizado para el desarrollo el *Application Server* JBoss 4.0.1 – GA con Tomcat 5.0 embebido, pero cualquier otro que cumpla los requisitos es aceptable. Del lado del cliente, sólo se necesita un browser de Internet y algún pluggin de firma digital de documentos PDF.

Se debe destacar que el desarrollo sobre plataforma J2EE garantiza la portabilidad del software a entornos Linux o Windows; y que además tanto la plataforma java, como el motor de base de datos y el application server requeridos en el servidor, son software de libre acceso.

Arquitectura web:

Todo el front-end del sistema está basado en *interfase web* con el usuario. Esto posibilita:

- Libre acceso a la aplicación y sus servicios desde cualquier puesto de trabajo conectado a la Intranet de Gobierno sin necesidad de instalación previa de aplicaciones cliente.
- Eventualmente, puede habilitarse la aplicación en Internet, bajo un sitio seguro con validación de certificados digitales del lado del cliente. Esto permite el acceso al mismo desde los distintos sitios de realización de congresos o seminarios.
- Carga de la complejidad del lado del servidor, con la ventaja de que los usuarios pueden consultar o gestionar solicitudes de certificación desde un cliente delgado. Costo cero en inversión en Hardware.
- Mayores posibilidades de escalabilidad.

- Costo cero en licencias de software cliente.
- Mantenimiento y resolución de problemas centralizado.
- Menor esfuerzo de capacitación y aprendizaje intuitivo de los usuarios.

Seguridad y Acceso:

El ***formulario de inscripción*** on-line es de acceso público en Internet, con cupo máximo parametrizable. El sistema puede eventualmente ser customizado para permitir la inscripción a un evento mediante el uso de una ***clave de matriculación***. De este modo se contempla el caso de eventos con participación restringida a invitados especiales.

El ***módulo de acreditación***, tanto como los procesos de generación, envío y publicación de certificados de asistencia, es de acceso exclusivo a usuarios con privilegios de administración u operación sobre la aplicación. La seguridad en el acceso a las aplicaciones y transacciones sobre la base de datos de inscripciones se implementa a través de:

- Control de privilegios de usuarios en la conexión a la base de datos.
- Sitio seguro con validación de certificado de cliente en el Application Server.

Serán usuarios autorizados, para una experiencia de certificación particular, el personal afectado a la tarea de acreditaciones y certificación de un evento en particular.

Los *procesos de timbrado y firma digital* de los certificados de asistencia que el sistema emite, son competencia absoluta de la autoridad responsable para un evento en particular; y se resuelven mediante la colocación de dispositivo criptográfico con Certificado de Firma Digital X509.v3 con clave privada.

El legítimo interés de los solicitantes en requerir un Certificado de Asistencia se verifica, tal como se prescribió en las especificaciones de diseño, me-

diante la comprobación de la dirección de email particular, a la cual le será remitido el Certificado; y mediante el requerimiento de su DNI, pasaporte u otro documento que acredite identidad, ante la posibilidad de descarga del Certificado vía web.

Código Fuente

La programación hace uso de los siguientes lenguajes:

- Consultas y transacciones sobre el motor de base de datos: *ANSI-SQL*
- Procedimientos almacenados en la base de datos: *PL/SQL*
- Servlets y Clases: *Java (J2EE)*
- Interface web: *JSP, Javascript, HTML*

Formato de los documentos Digitales

Los Certificados de Asistencia son construidos dinámicamente en un proceso por lote que considera todos los inscriptos efectivamente acreditados a un evento. Los documentos son construidos según la especificación PDF 1.6. Este formato es soportado por Acrobat Reader 6 o superior y ha sido testeado en múltiples readers pdf alternativos, sin identificar inconvenientes.

Firma Digital

Con el objetivo de garantizar interoperabilidad con los principales manejadores de firma, la aplicación utiliza los algoritmos estándar de hash y firma digital SHA-1/RSA. Se aplican claves RSA de 1024 bits.

En cuanto al envelope de la firma digital y certificados se ha cumplido con las especificaciones de diseño prescritas: la firma y el digesto firmado (hash md5 o sha-1) se encapsulan junto al Certificado X.509 del firmante y el certificado de Autoridad Certificante de la ONTI en un objeto PKCS#7, codificado en Base64, de forma que la misma pueda ser verificada por cualquier brow-

ser de archivos PDF, y alternativamente por otras herramientas específicas de validación de firma digital.

Timbre Digital

El Timbre Digital (Nube de puntos PDF417) es generado por el Servidor de Timbrado en función de los datos firmados y agregado dinámicamente al Certificado correspondiente.

- **Nivel de Corrección de Errores:** errorLevel 5
- **Modo de Compactación:** modo de optimización.
- **Capacidad de codificación y representación de la firma:** ASCII - Binario codificado en Base64.
- **Estructura de la Información codificada:**

  <<Cadena de Datos firmados>> + *<<inscripción obtenida como parámetro>>* + *"-"* + *<<nombre obtenido como parámetro>>* + *"-"* + *<<N° documento obtenido como parámetro>>* + *"-"* + *<<Título del evento>>* + *"-"* + *<<fecha del evento>>* + ***<<Cadena de firma codificada en CodeBase64 (PKCS#1)>>*** + ***<<Clave pública>>***
- **Condiciones de dimensión y ubicación:**
  - aspect ratio: 1:3 (relación de aspecto)
  - quiet zone: 1 cmt. (perímetro blanco)

Desarrollo

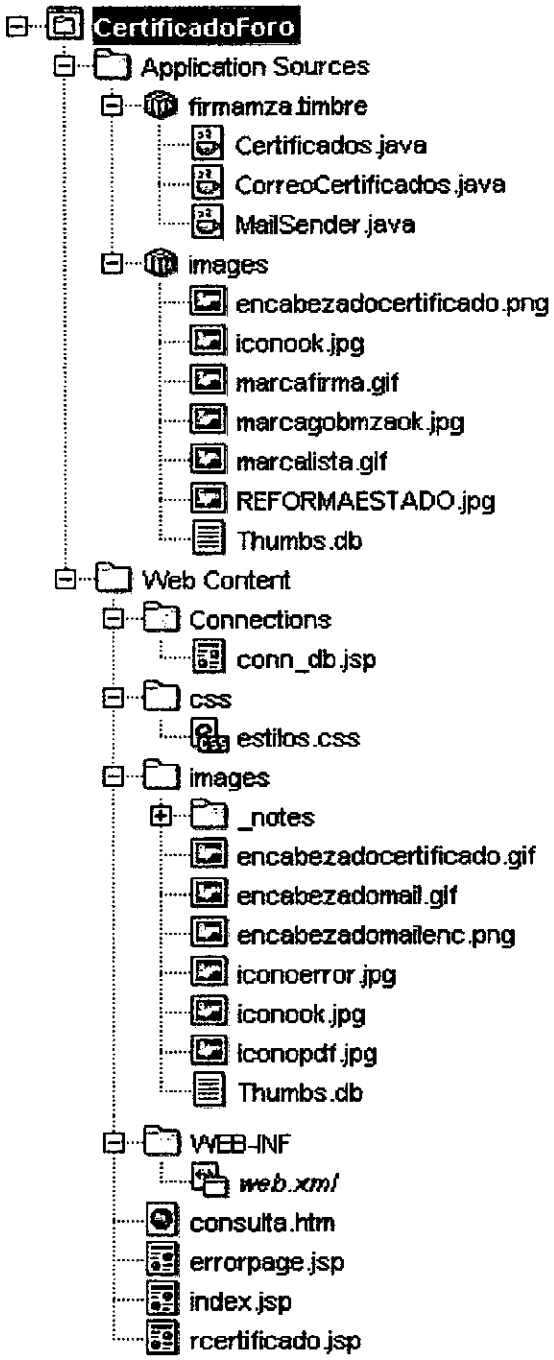
En las tareas de desarrollo se utilizó el IDE JDeveloper 10g por cuanto esta herramienta ha demostrado integrar muy bien con JBoss permitiendo el deploy directo sin configuraciones adicionales; y satisface las necesidades de programación determinadas en términos de herramientas visuales, de edición de código, de depuración y ayudas.

El front-end de la aplicación, que incluye el formulario de inscripción de acceso público y las interfaces de parametrización del sistema y administración de acreditaciones, restringidas a los operadores del sistema, fue codificado en lenguaje JSP (Java Server Pages).

La lógica de los procesos de emisión y envío de certificados fue implementada mediante un Servlet Java encargado de gestionar la conexión a Bases de Datos, generar dinámicamente los Certificados de Asistencia y emitir automáticamente los correos electrónicos de remisión de certificados.

La base de datos asociada a la aplicación, se desarrolló sobre un motor de base de datos Postgress independiente.

Como se explicó previamente, el conjunto completo de código que compone la aplicación ha sido desarrollado utilizando tecnologías Java 2 Enterprise Edition, manteniendo de esta forma compatibilidad tecnológica con el resto de los desarrollos realizados en el marco del Proyecto de Firma Digital e integración directa con la plataforma Linux + J2EE Application Server. Todos los componentes de la aplicación fueron empaquetados el contenedor ***certificadosasistencia.ear***, cuya estructura se describe a continuación y deployados sobre JBoss 4.0.1 – GA con Tomcat 5.0 embebido.



Paquete completo de módulos y librerías que componen la aplicación

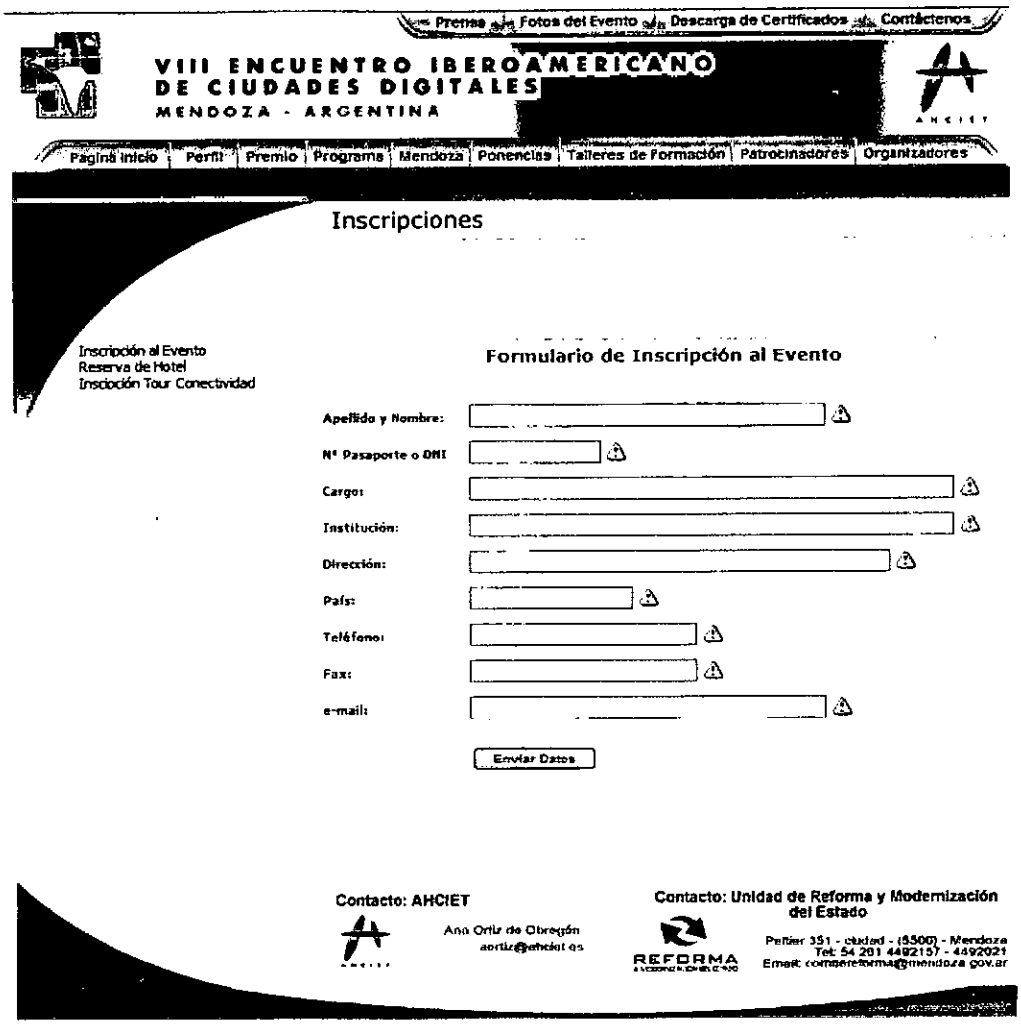
La página ***index.jsp,*** implementa la consulta de inscriptos efectivamente acreditados cuyos certificados de asistencia deben ser emitidos. Este código hace uso del modulo de ***conn_db.jsp*** en donde se definen las cadenas de conexión a la base de datos de inscripciones y acreditaciones.

El módulo central está constituido por la clase ***Certificados.class*** que implementa el servlet de emisión, timbrado, firma, envío y publicación de certificados. Este servlet y sus clases subsidiarias, tales como ***CorreoCertificados.class*** o ***MailSender.class*** que implementan la generación y envío de correo respectivamente, han sido implementados según las especificaciones de diseño previamente documentadas.

La aplicación completa fue deployada sobre JBoss 4.01 – GA con Tomcat 5.0 embebido. Complementariamente, se desarrollaron pruebas de deploy de la aplicación sobre el servidor de aplicaciones Tomcat 5.0 y sobre el Oracle Application Server corriendo tanto sobre Linux como sobre Windows XP. Se comprobó así la portabilidad directa del servicio a otras plataformas tecnológicas.

La solución desarrollada e implementada comprende, según especificaciones de diseño, los siguientes subprocesos:

7. ***Inscripción:*** Formulario HTML que permite a los individuos interesados en participar de un evento particular, concretar en línea su inscripción en tiempo y forma. Los datos relevantes consignados en el formulario de inscripción son almacenados de manera persistente en la base de datos de inscripciones.



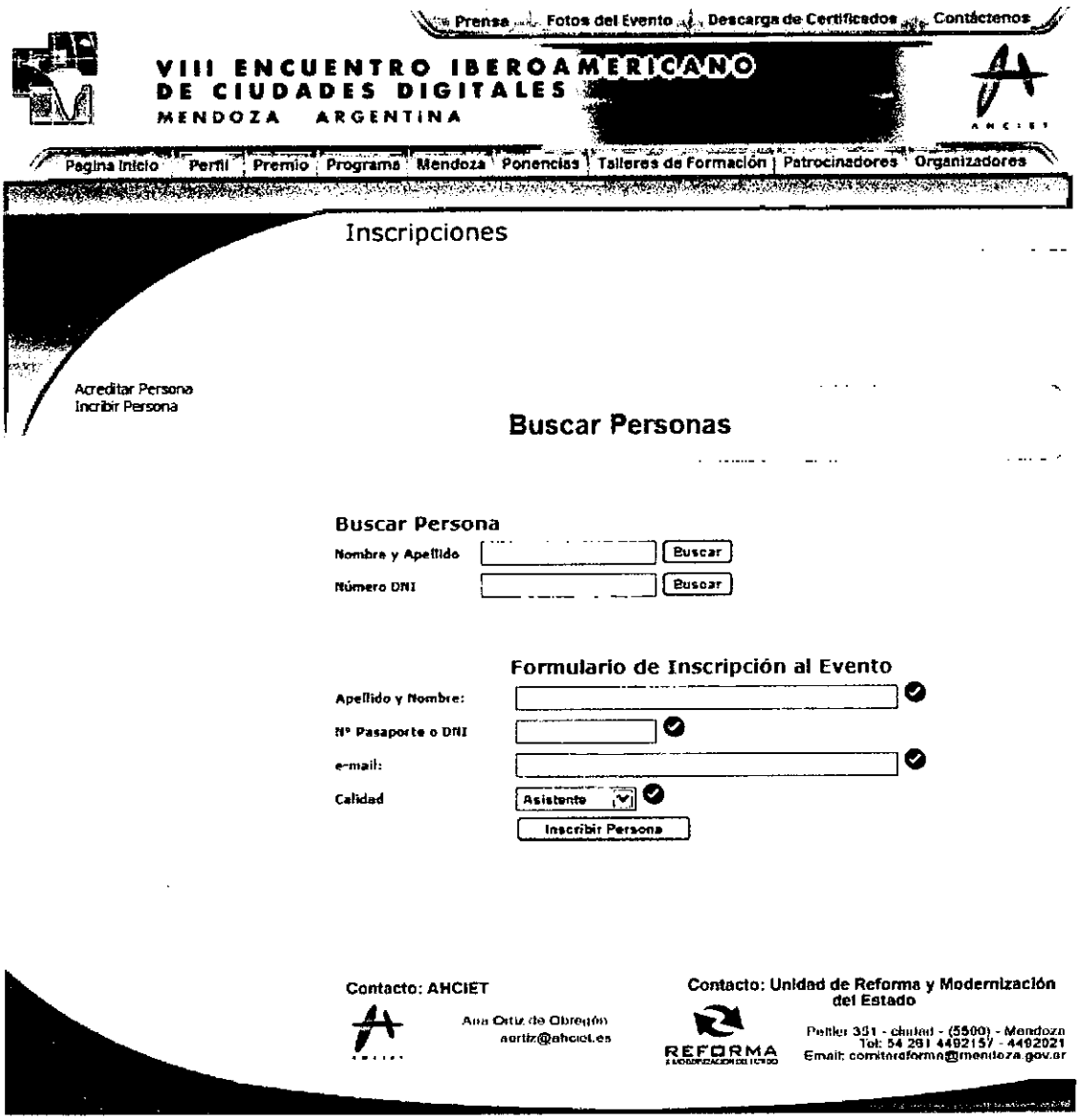
Formulario de Inscripción on-line de participantes al evento

Nota: Se utiliza en gráficos e ilustraciones los que surgen de la primera experiencia de Certificación Digital de Asistencia en instancia de realización del VIII Encuentro de Ciudades Digitales, realizado en Mendoza en Junio de 2007.-

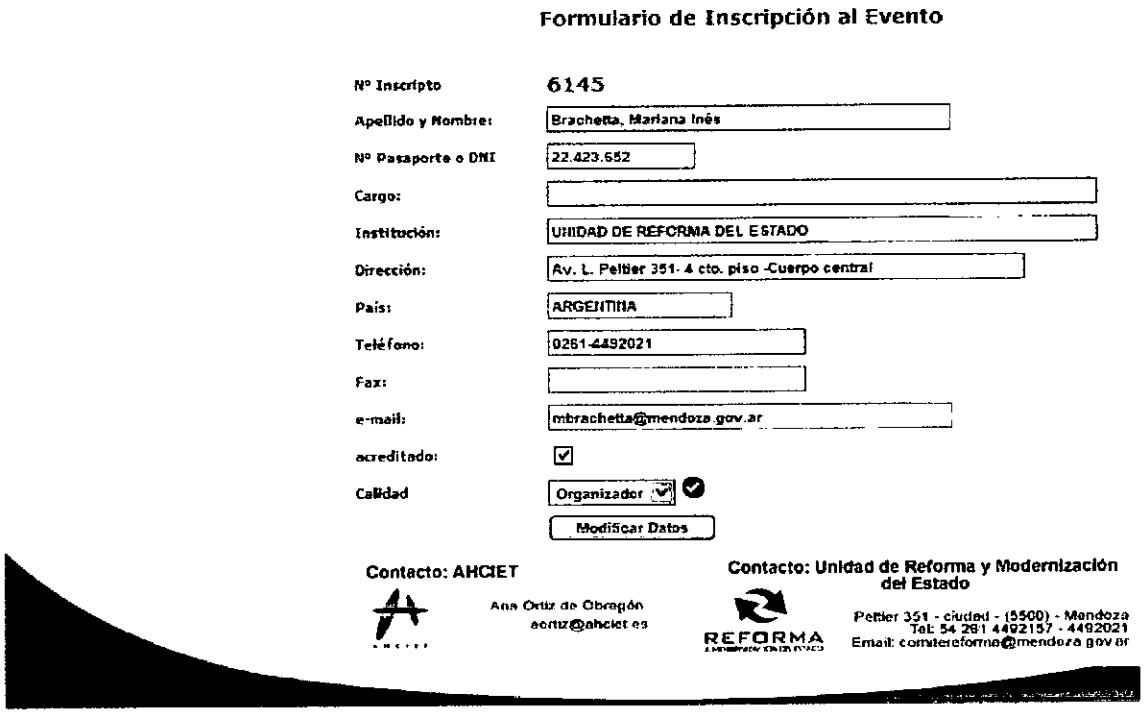
Importante: Los campos incluidos en el formulario de inscripción, se ajustan a la estructura de la tabla de Inscripciones – Acreditaciones, descripta en la sección 3.8 de las especificaciones de diseño detallado. Su diseño

debe personalizarse con los logos, gráfica e información de referencia propia de cada evento.

Acreditación: en instancia de realización del evento, los inscriptos asistentes deberán cumplir con el proceso de acreditación, registrándose así en el sistema su efectiva asistencia y participación al evento. El módulo de acreditaciones desarrollado, ofrece una interfaz web para que los operadores del sistema (agentes de acreditación), busquen un inscripto por ***id_inscripto***, ***nombre*** o ***documento***, y consignen su efectiva acreditación, tildando una casilla de verificación. Al acreditar un inscripto, se otorga la posibilidad al operador de modificar los datos que corresponde Certificar.



Formulario para buscar un inscripto en el evento en instancia de Acreditación



Interfaz de Acreditación de inscriptos

8. ***Procesos Internos:*** Se describe a continuación el desarrollo de métodos y procedimientos de procesamiento de datos, que producirán las salidas especificadas para la solución, dadas ciertas entradas y archivos de datos.

   Según prescripciones de diseño, los procesos internos se secuencian en pasos, en el orden que a continuación se exponen, de modo de conducir al operador en una línea de trabajo que lo lleve a completar toda la tarea de generación, firma y envío de certificados para un evento en particular.

   Paso 1: Consulta de inscriptos acreditados: interfaz web que muestra el recordset de inscriptos acreditados cuyos certificados van a ser emitidos. Este paso da lugar a los operadores y firmantes a verificar los certificados que van a generarse antes de lanzar el

proceso de emisión y corregir cualquier error que se detectase en la lista de inscriptos efectivamente acreditados.

LISTADO DE INSCRIPTOS ACREDITADOS
VIII ENCUENTRO IBEROAMERICANO DE CIUDADES DIGITALES

N° Inscripción	Nombre	Documento	Email
6508	Oscar A. León	11.264.921	oleon@frm.utn.edu.ar
6244	Jorge Ceña	0C0000C04	acatapanc@mendoza.gov.ar
6102	Iván Paredes Valenzuela	1C01057379	acatapanc@mendoza.gov.ar
6103	Patricio Peñaliel Acosta	1600129272	acatapanc@mendoza.gov.ar
6220	Jaime Herrera	102800501	jherreras@ice.go.cr
6525	Achiary, Carlos	1C.964.495	cachiary@sgp.gov.ar
6263	Mauricio Brunetti Labrin	0C0000019	acatapanc@mendoza.gov.ar
6297	Gutierrez, Héctor María	1C.240.552	privada@pergamino.gov.ar
6188	Szterealicat, Edmundo Gabriel	1C.400.495	edmundo@cfired.org.ar
6509	Francisco, Bravo	8.324.543	francisco.bravo@dipros.com.ar
6202	Irigo, Andrés	22.519.280	andres@wh.com.ar
6148	Andrea Rotella	21.740.289	andrea.rotella@osep.mendoza.gov.ar
6452	Garcia Diego	23.086.945	dgarcia@bgh.com.ar
6151	Caponucco, Amira	20.429.132	amira.caponucco@osep.mendoza.gov.ar
6453	Sandra Gómez	17.640.986	sgomez@mendoza.gov.ar
6274	Daron, Mónica C.	20.942.170	informatica@municipioderawson.gov.ar
6277	Camporro, Yanina V.	24.464.271	informatica@municipioderawson.gov.ar
6276	Flores, Oscar H.	20.942.327	informatica@municipioderawson.gov.ar
6014	De Marco, Gerardo	13.700.625	gdemarco@guaymallen.gov.ar
6346	Badui, María Teresa	24.878.671	mbadui@mendoza.gov.ar
6499	Felipe De Jesús Díaz Sevilla	07140131904	fjdiaz@guadalajara.gob.mx
6136	Marovel Tascón, Luis	10043452-L	luis.marovel@tres-cantos.org
6503	Miguel Ángel Marovel Tascon	9704293	mamarovel@gmail.com
6101	Beatriz Agudelo Henao	24432225	baguhi@hotmail.com
6104	Francisco Javier Álvarez	16749036	falvarez@cali.gov.co
6069	Martinez, Christian Jorge	4.647.902	christian.martinez@ericsson.com
6504	Ronildo Assis De Oliveira	0000000001	governo@saojoaodelrei.mg.gov.br
6505	Assis De Oliveira Ronildo	111111111	governo@joaodelrei.mg.gov.br
5972	Hendi, Kim	15.111.247	hendi.kim@ic.gc.ca
6253	Matias Rodriguez Perdomo	1541544-8	mrodriguez@antel.com.uy
6189	Porrua, Miguel A.	OEA 30614	mporrua@oas.org
6506	Hugo Marias	7.935.728	hmarias@nec.com.ar
6507	Petri, Luis	25.387.111	lpetri@hcdmza.gov.ar

TOTAL DE CERTIFICADOS A EMITIR 354

Emitir y Firmar Certificados

Listado de inscriptos acreditados

Paso 2: Proceso de Emisión de Certificados Firmados: sobre la consulta de inscriptos acreditados se implementó el botón ***"Emitir***

Certificados" que dispara el proceso automático de ***emisión*** de certificados con timbre y firma digital.

Los certificados son emitidos en un proceso de ***lote único*** para cada evento particular. Como resultado de la ejecución de este proceso el operador obtiene el lote de documentos .pdf que representan los certificados de asistencia, con timbre y firma digital. Así mismo, se obtiene como salida un reporte de Certificados generados que documenta el éxito o fracaso en el proceso de generación de generación de cada certificado particular.

La emisión de cada Certificado implica la generación instantánea del Documento PDF (Portable Document Format) timbrado y firmado digitalmente. Dicho proceso de emisión, timbrado y firma, supone los siguientes subprocesos:

2.1. Subproceso de Generación del Timbre: La construcción del timbre implica la firma digital, por autoridad competente, de aquellos datos individualizados como críticos a incluir en el Certificado. Dichos datos permiten identificar unívocamente la transacción en el sistema, el individuo certificado y la jornada, foro o curso implicado. Una vez obtenida la firma digital de estos datos, el subproceso produce la nube de puntos PDF417 (timbre digital) con la información del texto firmado, su firma y la clave pública del firmante correctamente barcodeados.

2.2. Subproceso de construcción preliminar del documento PDF: En función de los datos obtenidos del recordset de inscriptos acreditados y el timbre digital previamente generado sobre esta información, este subproceso construye dinámicamente un archivo ajustado a la especificación PDF 1.6 o superior con detalle de la siguiente información:

- √ Logos o marcas institucionales de la/las entidades organizadoras y patrocinantes de la jornada, seminario, curso, etc.
- √ Título del evento que se certifica.
- √ Nombre y Apellido de la persona certificada.
- √ Documento de la persona certificada.
- √ Fecha de realización del evento.
- √ Timbre Digital (Nube de puntos PDF417)

Este documento PDF constituye el certificado digital preliminar sobre el cuál se aplicará el proceso de firma digital.
Los documentos PDF preliminares son almacenados en un directorio temporal dispuesto a tal fin.

2.3. Subproceso de Firma Digital del Certificado emitido: Una vez construido el documento PDF preliminar, el mismo deberá se firma digitalmente por autoridad competente, obteniendo así el documento PDF final, timbrado y firmado digitalmente.

Todo el proceso de generación, timbrado y firma de documentos .pdf se realiza en un lote único (proceso batch) para cada evento. Este proceso por lote se realiza cumpliendo las especificaciones de diseño prescritas. En particular:

- √ Se han instrumentado los mecanismos necesarios para que el proceso de firma, tanto en instancia de generación del timbre como en instancia de firma final del documento PDF, se realice íntegramente en el desktop del firmante.
- √ La aplicación integra con dispositivos criptográficos de almacenamiento de firmas y certificados, compatibles con las disposiciones técnicas emanadas en este sentido de la legislación nacional y provincial.

EMISIÓN DE CERTIFICADOS FIRMADOS
VIII ENCUENTRO IBEROAMERICANO DE CIUDADES DIGITALES
Reporte de Emisión de Certificados

☑ 6508 Oscar A. León 11.264.921

☑ 6244 Jorge Cella 000000004

☑ 6102 Iván Paredes Valenzuela 1001057379

☑ 6103 Patricio Peñafiel Acosta 1600129272

☑ 6220 Jaime Herrera 102800501

☑ 6525 Achiary, Carlos 10.964.495

☑ 6263 Mauricio Brunetti Labrin 000000019

☑ 6297 Gutierrez, Héctor Maria 10.240.952

☑ 6188 Szterenlicht, Edmundo Gabriel 10.400.495

☑ 6509 Francisco, Bravo S.324.543

- -

☑ 6253 Matias Rodriguez Perdomo 1541844-8

☑ 6189 Porrua, Miguel A. OEA 30614

☑ 6506 Hugo Marias 7.985.728

☑ 6507 Petri, Luis 25.887.111

TOTAL CERTIFICADOS PROCESADOS: 354
TOTAL CERTIFICADOS EMITIDOS: 0

Enviar e-mails

Reporte de Certificados emitidos

REFORMA y MODERNIZACIÓN DEL ESTADO — GOBIERNO DE Mendoza — AMCIET

Certificado

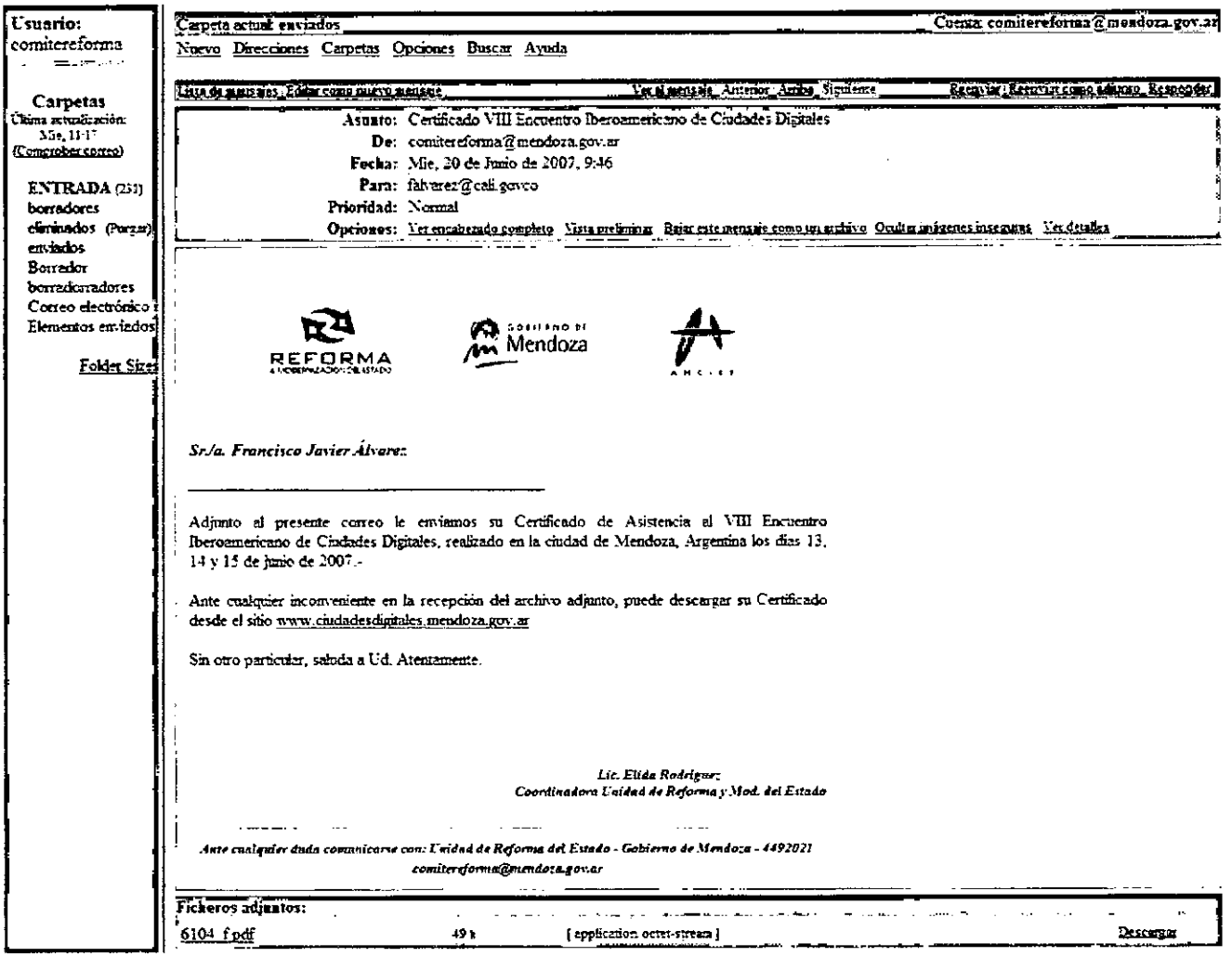
CERTIFICAMOS que el Sr./Sra. ***Dimarco, Jorge*** con Documento Nº ***18.336.366*** ha participado en calidad de ***ASISTENTE*** en el VIII Encuentro Iberoamericano de Ciudades Digitales, realizado en la ciudad de Mendoza - Argentina, los días 13, 14 y 15 de junio de 2007.-

firma digital
Elida Rodriguez
Coordinadora Unidad de Modernización del Estado
Gobierno de Mendoza
Secretaría Administrativa Legal y Técnica
Fecha de firma:20/06/2007

Modelo de certificado generado

Paso 3: Proceso de Notificación y Envío por e-mail de Certificados

Se ha agregado al reporte de certificados emitidos, un botón que permite al operador del sistema disparar el proceso de notificación y envío por email de certificados de asistencia. Este proceso, que también trabaja por lote, toma cada uno de los Certificados de Asistencia emitidos y lo adjunta al cuerpo de un email de notificación, que envía automáticamente a la cuenta de correo consignada por el participante en instancia de inscripción. El cuerpo del correo electrónico incluye como subject el título *"Certificado de Asistencia - " más el nombre del evento implicado* y en su cuerpo la notificación de envío junto a un vínculo a la dirección web desde donde se puede descargar una copia del Certificado y direcciones o teléfonos de contacto para consultas o reclamos.



Usuario: comitereforma

Carpetas
Última actualización: Xie, 11:17 (Comprobar correo)

ENTRADA (251)
borradores
eliminados (Purgar)
enviados
Borrador
borradoradores
Correo electrónico
Elementos enviados

Folder Sizes

Carpeta actual: enviados — Cuenta: comitereforma@mendoza.gov.ar

Nuevo Direcciones Carpetas Opciones Buscar Ayuda

Lista de mensajes Editar como nuevo mensaje Ver el mensaje Anterior Arriba Siguiente Responder Responder a todos Reenviar Reenviar como adjunto Responder

Asunto: Certificado VIII Encuentro Iberoamericano de Ciudades Digitales
De: comitereforma@mendoza.gov.ar
Fecha: Mie, 20 de Junio de 2007, 9:46
Para: falvarez@cali.gov.co
Prioridad: Normal
Opciones: Ver encabezado completo Vista preliminar Bajar este mensaje como un archivo Ocultar imágenes inseguras Ver detalles

REFORMA
GOBIERNO DE Mendoza
AMCIUDAD

Sr./a. Francisco Javier Álvarez

Adjunto al presente correo le enviamos su Certificado de Asistencia al VIII Encuentro Iberoamericano de Ciudades Digitales, realizado en la ciudad de Mendoza, Argentina los días 13, 14 y 15 de junio de 2007.-

Ante cualquier inconveniente en la recepción del archivo adjunto, puede descargar su Certificado desde el sitio www.ciudadesdigitales.mendoza.gov.ar

Sin otro particular, saluda a Ud. Atentamente.

Lic. Elida Rodriguez
Coordinadora Unidad de Reforma y Mod. del Estado

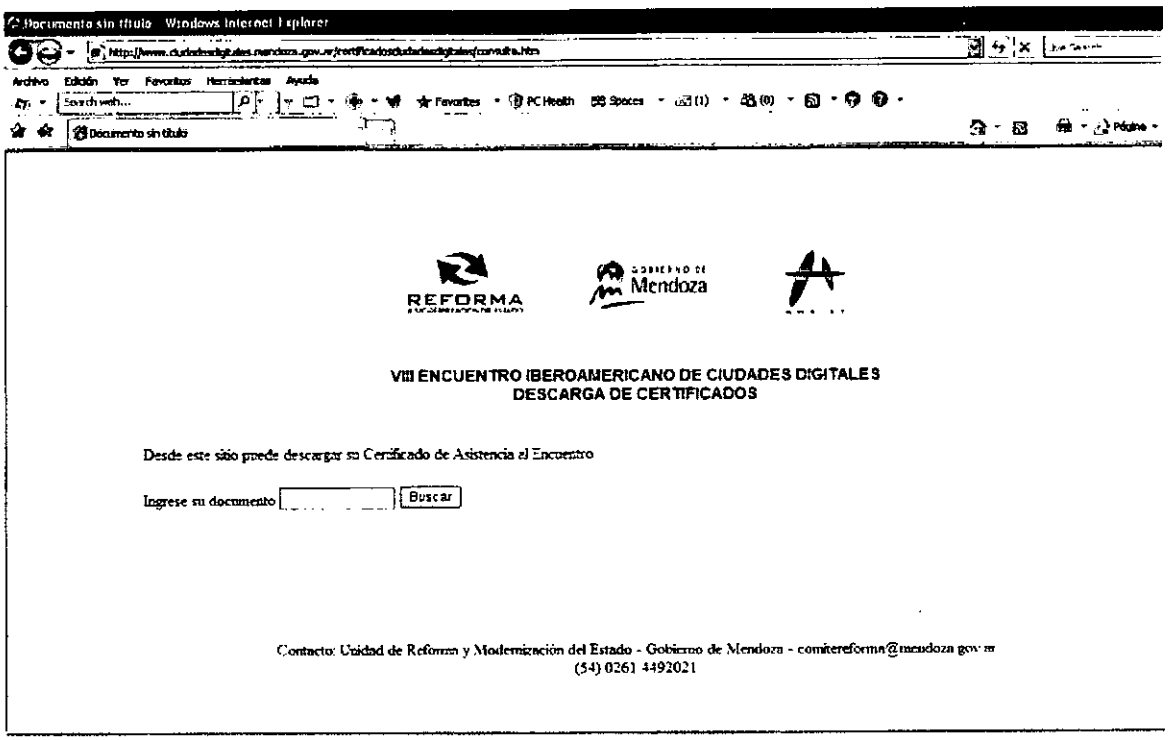
Ante cualquier duda comunicarse con: Unidad de Reforma del Estado - Gobierno de Mendoza - 4492021
comitereforma@mendoza.gov.ar

Ficheros adjuntos:
6104_f.pdf 49 k [application octet-stream] Descargar

Modelo de email de notificación

Paso 4: Proceso de Publicación de Certificados:

La aplicación permite subir el lote de Certificados de Asistencia emitidos, timbrados y firmados al servidor de aplicaciones JBoss público del Gobierno de Mendoza. A este punto pueden luego vincularse los sitios web del/los eventos, para implementar la publicación de Certificados.
Se provee en este servidor de aplicaciones, un módulo de búsqueda y descarga de certificados que utiliza una página de consulta por documento (DNI, pasaporte, Cédula de Identidad, otros) para permitir a los interesados acceder directamente al documento correspondiente.



Página de descarga de certificados

Plataforma de Producción

La plataforma de producción donde se montó la aplicación está compuesta del application Server, encargado de distribuir los servicios de la aplicación a sus usuarios y el Motor de Base de datos, en donde se implementa la persistencia de datos administrados por el desarrollo.

Servidor de Aplicaciones

Una vez concluido el desarrollo se instaló el paquete ***certificadosasistencia.ear*** en el Application Server de producción. Estas actividades implicaron tareas de configuración y ajuste de las aplicaciones en el lado del servidor. Se describe a continuación la plataforma tecnológica operativa en el servidor y las configuraciones realizadas.

Application Server: Entorno de producción en Intranet. Eventualmente abierto a Internet, mediante acceso restringido por SSL con validación de Certificado Digital del cliente.
Servidor Linux Red Hat
Servidor de Aplicaciones JBoss 4.0.4.GA
WebServer Tomcat 1.5
Plataforma J2EE – jdk1.5.0_08
Librerías criptográficas JCE – BouncyCasttle (Open Source)
Librerías PDF417 – iText (Open Source)

A nivel de configuraciones, se definió el contexto de activación de la plataforma web y un virtual host para el mismo en el archivo de configuración del servidor de aplicaciones. Se securizó el acceso lógico a la aplicación ***.ear*** que contiene la aplicación compilada y se definieron usuarios autorizados para su administración.

Para favorecer la portabilidad futura de la aplicación, las librerías de clases Java necesarias para su correcto funcionamiento fueron empaquetadas junto al resto del código en el módulo .ear. Entre ellas, la API iText 1.5.jar y la API firmadigital.jar con clases subsidiarias programadas internamente por el Equipo de Desarrollo de este proyecto.

Motor de Base de Datos

Se migró la estructura de la Base de Datos de desarrollo al motor de base de datos en producción, Postgres 8.01 corriendo sobre servidor Linux RedHat en un equipo independiente, sin interconexión a la red pública.

La estructura de la base de datos se ajusta, según prescripciones de diseño, al siguiente ***modelo***:

Charset: windows-1252 o ANSI1
Esquema: único

Vistas: ninguna

StoreProcedures y Triggers: ninguno

Funciones: ninguno

Usuario de conexión: inscripcion1, consulta1

Lenguaje de Consulta: ajustarse a ANSI SQL

Tabla de Inscripciones - Acreditaciones:

Campo	***Tipo***	***Descripción***
id_inscripto	INTEGER OID AUTOINCREMENT not null	Nº Interno de inscripción, generado automáticamente por la base como un OID para cada nuevo individuo que concreta su inscripción en el sistema.
nombre	VARCHAR 120 not null	Nombre y Apellido del individuo inscripto.
documento	VARCHAR 15 not null	N° de documento que acredite identidad del inscripto.
Email	VARCHAR 60 not null	Dirección de correo registrada por el inscripto. A este email deberán ser remitidas las notificaciones de emisión de Certificados. Así como también cualquier notificación intermedia que se remita.
acredita	BOOLEAN not null	Variable lógica que indica el estado de la efectiva acreditación del inscripto en un evento en particular: √ *false:* no acreditado

		√ *true:* acreditado
calidad	INTEGER not null	Calidad o rol de participación del inscripto en el evento: √ 0 – Asistente √ 1 – Expositor √ 2 – Organizador √ 3 – Patrocinador/Auspiciante
entidad	VARCHAR 120	Empresa u organización que representa el inscripto
Cargo	VARCHAR 120	Función que desarrolla en su institución
domiciliopar	VARCHAR 120	Domicilio postal particular del inscripto
domiciliolab	VARCHAR 120	Domicilio postal laboral del inscripto
provincia	VARCHAR 40	Provincia de residencia
País	VARCHAR 40	País de residencia
teléfono	VARCHAR 40	Teléfono de contacto del inscripto
Móvil	VARCHAR 40	Teléfono celular de contacto del inscripto
Fax	VARCHAR 40	Fax de contacto con el inscripto
observación	VARCHAR 120	Campo alfanumérico para indicar observaciones pertinentes sobre el inscripto.

La conexión desde los módulos de la aplicación a la Base de Datos se resuelve mediante el Driver de conexión JDBC jdbcpostgresql 7.3, el cual fue empaquetado como librería java en el módulo certificadosasistencia.ear. Dicho driver recibe y gestiona las cadenas de conexión a la base de datos con identificación de usuarios y claves de conexión.

B) Puesta en marcha

Concluida la etapa de desarrollo e implementación se dispuso de la aplicación para utilizarla en experiencias concretas de Certificación Digital.

A la fecha, se han realizado ***tres experiencias*** de Certificación Digital de Asistencia a foros y seminarios, realizados por dependencias del Gobierno de Mendoza en colaboración con otras entidades de los sectores académico y privado. Se certificó por este medio, a los asistentes, organizadores, expositores o patrocinadores de los siguientes eventos.

- **VIII Encuentro Iberoamericano de Ciudades Digitales**, organizado por el Gobierno de Mendoza y la Asociación Hispanoamericana de Empresas de Informática y Telecomunicaciones (AHCIET), en Mendoza, Argentina los días 13, 14 y 15 de Junio de 2007. Se emitieron en esta experiencia quinientos nueve (509) Certificados de Asistencia con timbre y firma digital.

REFORMA & MODERNIZACIÓN DEL ESTADO — GOBIERNO DE Mendoza — AHCIET

Certificado

CERTIFICAMOS que el Sr./Sra. ***Dimarco, Jorge*** con Documento N° ***18.336.366*** ha participado en calidad de ***ASISTENTE*** en el VIII Encuentro Iberoamericano de Ciudades Digitales, realizado en la ciudad de Mendoza - Argentina, los días 13, 14 y 15 de junio de 2007.-

firma/d
Elida Rodriguez
Coordinadora Unidad de Reforma y Modernización del Estado
Gobierno de Mendoza
Secretaría Administrativa Legal y Técnica
Fecha de firma:20/06/2007

Modelo de Certificado Generado

- **II Foro Regional de Gobierno Electrónico**, organizado por el Gobierno de Mendoza y el Consejo Federal de la Función Pública (CoFeFuP), en Mendoza, Argentina, los días 29 y 30 Agosto de 2007. Se emitieron en esta oportunidad doscientos treinta y un (231) Certificados de Asistencia con timbre y firma digital.

REFORMA

Gobierno de Mendoza

UNCP Argentina

SGP

Jefatura de Gabinete de Ministros

CERTIFICAMOS que el Sr./Sra. ***Cabrera Hernán*** con Documento N° ***25396446*** ha participado en calidad de ***ASISTENTE*** en el 2° FORO REGIONAL DE GOBIERNO ELECTRÓNICO, REGIÓN CUYO - "Hacia una estrategia Federal de Gobierno Electrónico", realizado en la ciudad de Mendoza - Argentina, los días 29 y 30 de agosto de 2007.-

firma

Juan Manuel [illegible]
Subsecretario de la Gestión Pública
Jefatura de Gabinete de Ministros
Subsecretaría de la Gestión Pública

Fecha de firma:30/08/2007

Modelo de Certificado Generado

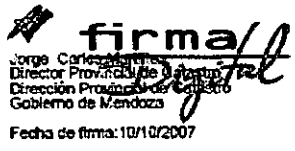
- **Jornada Institucional del Servicio Argentino de GNSS y 5° Taller Nacional de Estaciones GPS Permanentes**, organizado por la Dirección Provincial de Catastro del Gobierno de Mendoza y otras instituciones científico académicas provinciales y nacionales, en Mendoza, *Argentina, los días 26, 27 y 28 de Setiembre de 2007*. Se emitieron en esta oportunidad ciento sesenta y nueve (169) Certificados de Asistencia con timbre y firma digital.

JORNADA INSTITUCIONAL DEL SERVICIO ARGENTINO DE GNSS

5° TALLER NACIONAL DE ESTACIONES GPS PERMANENTES

CERTIFICAMOS que *Mariana Brachetta* ha participado en calidad de *ASISTENTE* en la Jornada Institucional del Servicio Argentino de GNSS y 5° Taller Nacional de Estaciones GPS Permanentes, realizados en el Centro Regional de Investigaciones Científicas y Tecnológicas, los días 26, 27 y 28 de septiembre de 2007.-

Mendoza, 28 de septiembre de 2007



Modelo de Certificado Generado

La puesta en marcha de la implementación para cada una de estas experiencias implicó las siguientes actividades:

- ***Coordinación de actividades con los referentes de las dependencias gubernamentales y organizadores asociados involucrados en cada una de las experiencias***. Se mantuvieron reuniones con los responsables de la organización de cada

evento para explicar los servicios de la implementación, sus ventajas y la validez de las certificaciones emitidas por este medio. Una vez acordada la realización de la experiencia, se interactuó con los referentes de cada sector o empresa participante para obtener información, marcas y logos, modelos de certificados, datos de autoridades firmantes y toda otra información relevante para la adaptación y parametrización del sistema.

- ***Configuración y adaptación de la aplicación a los requerimientos de la experiencia de Certificación particular, para un evento específico.*** Se parametrizó el sistema con los logos y marcas, título y fecha del evento, información institucional, mensajes de comunicación, direcciones de correo electrónico, vínculos, teléfonos y otros datos de referencia.

- ***Emisión de Certificados de firma digital para las autoridades firmantes.*** En etapa de desarrollo se trabajó con un Certificado de Prueba a nombre de usuario de prueba 1, emitido por la AC-URME (Autoridad Certificante prototipo de la Unidad de Reforma y Modernización del Estado), con un período de validez de un año. Una vez concluido el desarrollo y comprobado el correcto funcionamiento de todo el circuito de generación, firma y timbrado digital de los Certificados de Asistencia y el correcto funcionamiento de la aplicación en la plataforma de producción, se procedió, en instancia de realización de cada experiencia, a solicitar y emitir el Certificado a nombre de la Autoridad firmante de las certificaciones del evento. También se emitieron los Certificados AC-URME de acceso al sitio seguro SSL para los operadores de acreditación. Dichos certificados

digitales fueron emitidos por la ONTI y la AC-URME (Autoridad Certificante prototipo de la Unidad de Reforma y Modernización del Estado) respectivamente, con un período de validez de un año y respetando los procedimientos establecidos en la política de certificación. Una vez concluida la experiencia se revocaron los certificados emitidos.

- ***Capacitación a operadores*** Se instruyó a los operadores del sistema, encargados de acreditar a los participantes en la comprensión del concepto de Timbre y Firma Digital, las garantías que provee, sus alcances y los beneficios que genera para los usuarios finales. Es importante lograr la adhesión de estos operadores a la experiencia por cuanto fueron ellos multiplicadores de sus efectos hacia el público en general. En este sentido, se realizó con el grupo de operadores un entrenamiento intensivo tanto en los aspectos operativos del sistema adaptado a la experiencia particular, como en la toma de conciencia sobre la mejora de procesos y principios básicos introducidos por la firma y el timbrado digital. La capacitación se realizó en oficinas de la Unidad de Reforma y Modernización del Estado durante una jornada de 4hs. Se trabajó sobre la aplicación puesta en producción y se mostró además la operación de la aplicación de validación del timbre. Por la simplicidad operativa de la aplicación de verificación, no se utilizó documentación específica, distinta de la ayuda incluida en la aplicación.

- ***Difusión de la experiencia.*** En instancia de realización de los eventos, se dispuso un momento para difundir la experiencia de Certificación Digital de Asistencia y explicar a los participantes sobre la metodología de acreditación y posterior recepción

o descarga de certificados. Así mismo se explicaron brevemente los alcances de la firma y timbre digital sobre sus Certificados de Asistencia.

c) Evaluación de la experiencia:

Se definen métricas de evaluación que a futuro permitirán evaluar el éxito de la implementación

Describimos a continuación el sistema de evaluación de resultados que se aplicará. El modelo reúne un conjunto de indicadores y aspectos observables que permitirán identificar las ventajas comparativas del circuito y obtener conclusiones válidas sobre la experiencia.

Dicho diseño respeta el enfoque particular a los procesos específicos de la presente aplicación.

Este modelo se basa en métricas con las que, razonablemente, se puedan cuantificar las dimensiones que son de nuestro interés.

La siguiente tabla define los indicadores generales utilizados para medir el rendimiento de la aplicación.

EXPERIENCIA DE SOLICITUD/ENTREGA DE CERTIFICADO DE ASISTENCIA DIGITALES CON FIRMA DIGITAL Instrumento de Evaluación	
Indicadores Cualitativos	Métricas y Resultados

Satisfacción de los usuarios:

- Grado de aceptación de los asistentes – Nivel de Confianza

Beneficios diferenciales:

- Reducción de gastos en formularios preimpresos
- Disponibilidad
- Seguridad
- Integridad de la Información
- Ahorros de tiempo

Marco legal:

- Impacto en normativa interna

Alcance:

- Participación de los sectores relacionados
- Difusión pública

Indicadores Cuantitativos	Métricas y Resultados

Eficiencia:

- % de timbres emitidos correctamente
- Nro. de cert. emitidas válidas / Total de cert. emitidas
- Nro. de cert. emitidas rechazadas / Total de cert. emitidas
- % de fallas de sistema
- % de interrupciones del servicio
- Tiempos comparados
- Ahorros generados

Asistencia:

- Nivel de reclamos atendidos

Calificación de la experiencia ponderada final

.....