GOBIERNO DE MENDOZA

SECRETARÍA ADMINISTRATIVA LEGAL Y TÉCNICA

UNIDAD DE REFORMA DEL ESTADO

Informe Final

CONSEJO FEDERAL DE INVERSIONES

CONSULTOR: LIC. PABLO GUILLERMO LIOY

Fecha de impresión 10/02/2006 10:38

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. ***Transferencia:***

   - Diseño de Metodología y elaboración de documentos: se determinaron los pasos a seguir para realizar una transferencia y se desarrollaron los contenidos explicativos necesarios.

2. ***Investigación de nuevas tecnologías de firma digital:***

   - Investigación de tecnología de timbrado digital: se recopiló y analizó información sobre la tecnología que permite de certificación de las operaciones realizadas por Internet facilitando su lectura y control de autenticidad y se presentaron las principales conclusiones.

3. **Identificación *de experiencia de timbrado digital:***

   - Identificación de la necesidad: se recopiló y analizó información sobre la experiencia, se entrevistó a los posibles usuarios y se precisó la necesidad de aplicación de tecnología de timbrado digital
   - Análisis del sistema: se relevó el circuito actual, y se definió el alcance de la experiencia.

4. **Diseño de experiencia de timbrado digital:**

   - Diseño de la implementación: se elaboró el diseño conceptual de la experiencia.
   - Diseño de un Plan de Pruebas: se elaboró un Plan de Pruebas.

5. **Participación en el proceso de Reglamentación del la Ley 7234:**

   - Reuniones con el equipo legal de la Gobernación: se realizaron reuniones con el objeto de aclarar los alcances del proyecto de firma digital, las tendencias nacionales y el estado actual de la materia.
   - Participación en la redacción del decreto reglamentario: se brindó asesoramiento desde los conocimientos específicos y Know How adquirido en materia de Firma Digital por parte del equipo del proyecto y se prepararon eventuales informes sobre aspectos específicos requeridos por el equipo legal.

6. **Implementación de experiencia de timbrado digital:**

   - Desarrollo e implementación: se llevó a la práctica una experiencia piloto real. Se emitieron los certificados de firma digital, se realizaron las configuraciones, instalación de protocolos, ajustes y desarrollos necesarios en el equipamiento informático
   - Prueba del Sistema: se puso en práctica el Plan de Pruebas
   - Puesta en Marcha de la implementación: el sistema existente se reemplazó por el nuevo mejorado
   - Evaluación de la experiencia: se definieron 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 6 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 las líneas de acción planteadas:

LÍNEA DE IMPLEMENTACIÓN DE EXPERIENCIAS

Actividades:

Implementación de timbrado digital: intentaremos volcar los nuevos conocimientos adquiridos a través de nuestra línea de investigación y desarrollo en nuevas implementaciones de tecnologías de firma digital de vanguardia en el ámbito de los procesos susceptibles de generar ahorros, mayor efectividad operativa y acercamiento al ciudadano.

LÍNEA DE INVESTIGACIÓN Y DESARROLLO

Actividades

Investigación de nuevas tecnologías de firma digital: siguiendo la línea de investigación de nuestro proyecto, proponemos el estudio analítico de nuevos tipos de aplicaciones disponibles con tecnología de firma digital que nos permitan brindar nuevos y mejores servicios en el marco del proyecto

LÍNEA DE FORTALECIMIENTO Y CRECIMIENTO

Actividades

Participación en el proceso de Reglamentación del la Ley 7234: la inminente aprobación de la Ley de Adhesión provincial a la Ley nacional de firma digital, elaborada a instancias de nuestro equipo de firma digital, determina la obligación del PE provincial de reglamentar dicha Ley. Por ello, resulta necesario trabajar estrechamente con las oficinas legales de la Gobernación ase-

sorando desde los conocimientos específicos y experiencia técnica del equipo en materia de firma digital.

II. Investigación de nuevas tecnologías de firma digital:

A) Resumen ejecutivo

El timbrado digital propone la incorporación de una marca o sello con información codificada (timbre digital) a documentos emitidos electrónicamente e impresos en cualquier tipo de impresora. Este "timbre digital" tiene por objeto darle a estos documentos la misma validez que a los tradicionales documentos de oficina con timbre y firma de funcionario.

La tarea realizada consistió en indagar el marco teórico que soporta esta tecnología, reconocer experiencias concretas de aplicación a nivel mundial y evaluar distintas alternativas de desarrollo tecnológico.

B) Objetivos

Objetivo Principal

- Evaluar la tecnología de timbre digital como mecanismo alternativo para trasladar los efectos de la firma digital sobre documentos electrónicos, a documentos impresos.

Objetivos Particulares

- Identificar estándares y modelos, aplicados en desarrollos de timbre digital.
- Reconocer experiencias de aplicación concreta en el mundo.
- Seleccionar la plataforma tecnológica más adecuada para sustentar el desarrollo de una implementación prototipo.

C) Fundamentos del Estudio

La firma digital es un mecanismo que permite garantizar autoría e integridad de documentos electrónicos. Esta firma sustentada en algoritmos criptográficos, pierde todas sus propiedades cuando el documento firmado es impreso o cambia a un soporte no digital.

En este aspecto, la selección de procesos en donde es aplicable la tecnología de firma digital encuentra una restricción importante, dado que la mayor parte de los circuitos administrativos actuales involucran alguna instancia que requiere la impresión de los documentos.

Una estrategia posible, sería encarar trabajos de reingeniería global de estos procesos, para modelarlos como circuitos completamente digitales. Este camino, resulta ambicioso en el contexto actual, por cuanto requiere de sustanciales modificaciones normativas y alta disponibilidad de conectividad de todos los actores involucrados.

Bajo estas condiciones resulta significativo en el marco del Proyecto de Firma Digital, la búsqueda de alternativas tecnológicas que permitan trasladar los efectos de la firma digital de documentos electrónicos a documentos impresos, a fin de salvar aquellas instancias en las que el cambio de soporte de la información constituye un quiebre en el circuito.

Por los motivos expuestos y en base a un sondeo preliminar se decide encarar el presente estudio sobre la tecnología de timbrado, por cuanto se presume que la misma puede aportar una solución factible y de bajo costo al problema planteado.

D) Alcances

En esta primera instancia el trabajo se restringió a estudiar aplicaciones modelo de timbre digital, reconocer los estándares y plataforma tecnológica sobre los cuáles las mismas están desarrolladas, valorar distintas alternativas de desarrollo e implementación y concluir en la selección de una solución tecnológica adecuada para futuras aplicaciones prototipo.

E) Desarrollo

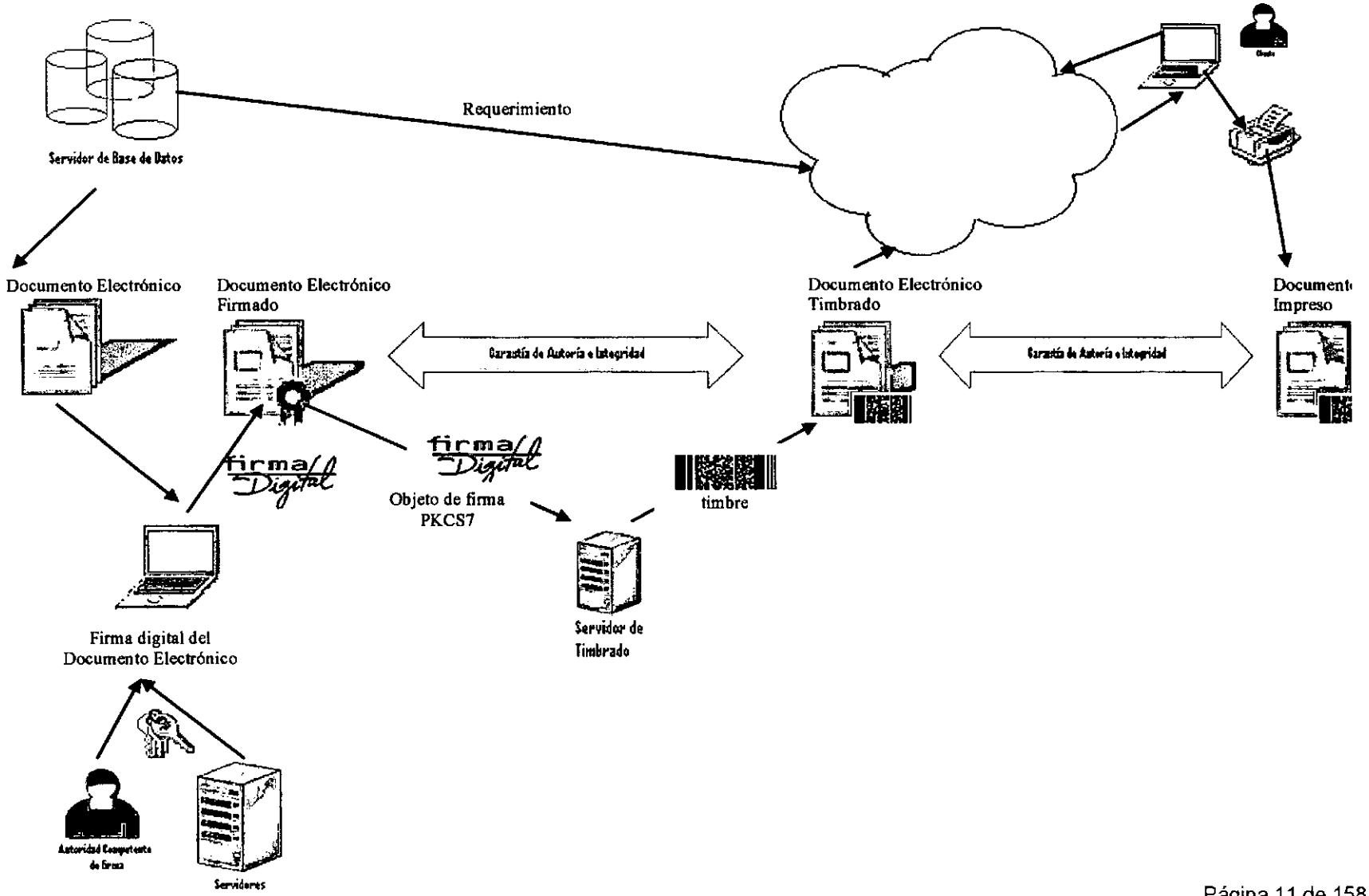
1. Modelo de Timbrado Digital

Un timbre o sello digital es un código inteligente impreso. Básicamente un código de barras con características especiales, impreso sobre el documento o certificado, el cual se obtiene a partir de un proceso de codificación de la firma digital de determinados campos del documento electrónico. Este código se genera mediante alguno de los estándares de codificación de barras y permite luego con el debido tratamiento, reconstruir el set de bits que constituyen la firma del documento electrónico y eventualmente la cadena de certificación de firma involucrada. De esta forma, a partir de la captura del timbre, se puede reconstruir la firma para verificar la validez de documentos impresos que fueron firmados digitalmente.

En síntesis, un timbre digital permite asegurar que el documento impreso fue emitido por un agente autorizado y que el texto corresponde con el originalmente impreso.

Los siguientes diagramas ilustran el proceso de timbrado y validación de documentos timbrados.

Fig. 1 - Esquema del Proceso de Timbrado



La *Figura 1- Esquema del Proceso de Timbrado* supone un ***usuario*** con la posibilidad de solicitar por medios electrónicos la emisión de un documento emitido, firmado y/o sellado por una ***Autoridad Competente***. Estos documentos pueden representarse en distintos formatos: archivos de texto, páginas html, documentos xml, archivos pdf, etc., y contener cualquier tipo de información. Típicamente serán actas, constancias o certificaciones que el usuario necesita para presentar ante otro organismo, al que llamaremos en este modelo, ***Oficina u Organismo Requirente***.

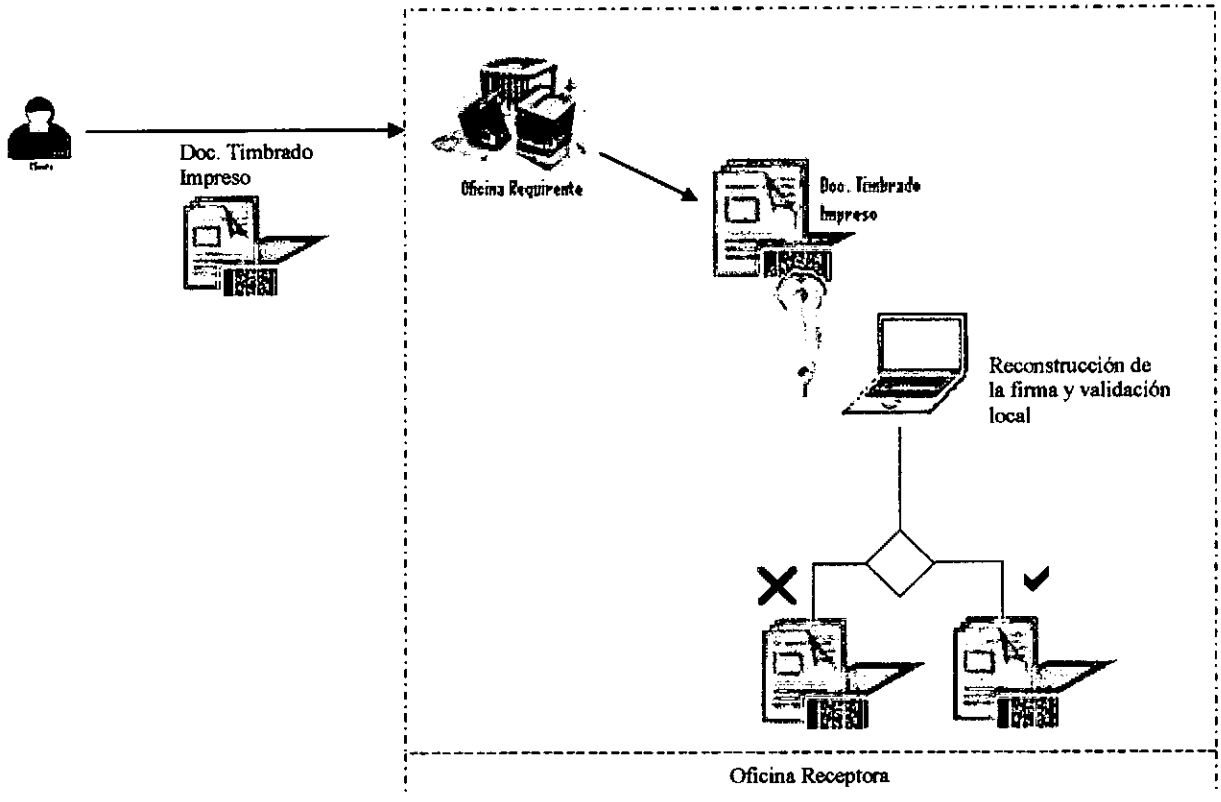
A partir del requerimiento de usuario, se construye dinámicamente en los servidores de datos pertinentes un documento electrónico con el formato e información que la aplicación prevea. Este documento electrónico es firmado digitalmente por una Autoridad Competente de firma o un servidor acreditado. Así se obtiene un documento electrónico firmado digitalmente.

La firma digital, representada en algún formato válido, es codificada por el Servidor de Timbrado, según alguno de los estándares de códigos de barra de alta densidad o bidimensionales (habitualmente PDF417), obteniéndose de este modo el timbre digital. Este timbre se complementa, opcionalmente, con un código numérico que permite identificar de manera unívoca al documento digital original en un servidor de archivos. Este código inteligente (timbre más código numérico) es agregado al documento electrónico, el cual se entrega al usuario requirente.

El usuario puede entonces guardar copia digital ***o impresa*** del documento timbrado que el sistema le entrega y, en ambos casos, estará contando con un documento avalado o firmado por la Autoridad Competente.

En el otro extremo del circuito; cuando el usuario que solicitó el documento timbrado lo presenta ante un organismo requirente, se debe contar con algún mecanismo que permita al organismo verificar la validez del documento timbrado impreso. Garantizar la validez implica asegurar que los datos impresos no han sido alterados (integridad) y que fue emitido por una Autoridad Competente (Autoría). Esta garantía de integridad y autoría puede obtenerse por dos esquemas de validación alternativos que se ilustran a continuación.

Fig. 2 – Esquema Proceso de Validación Off-Line

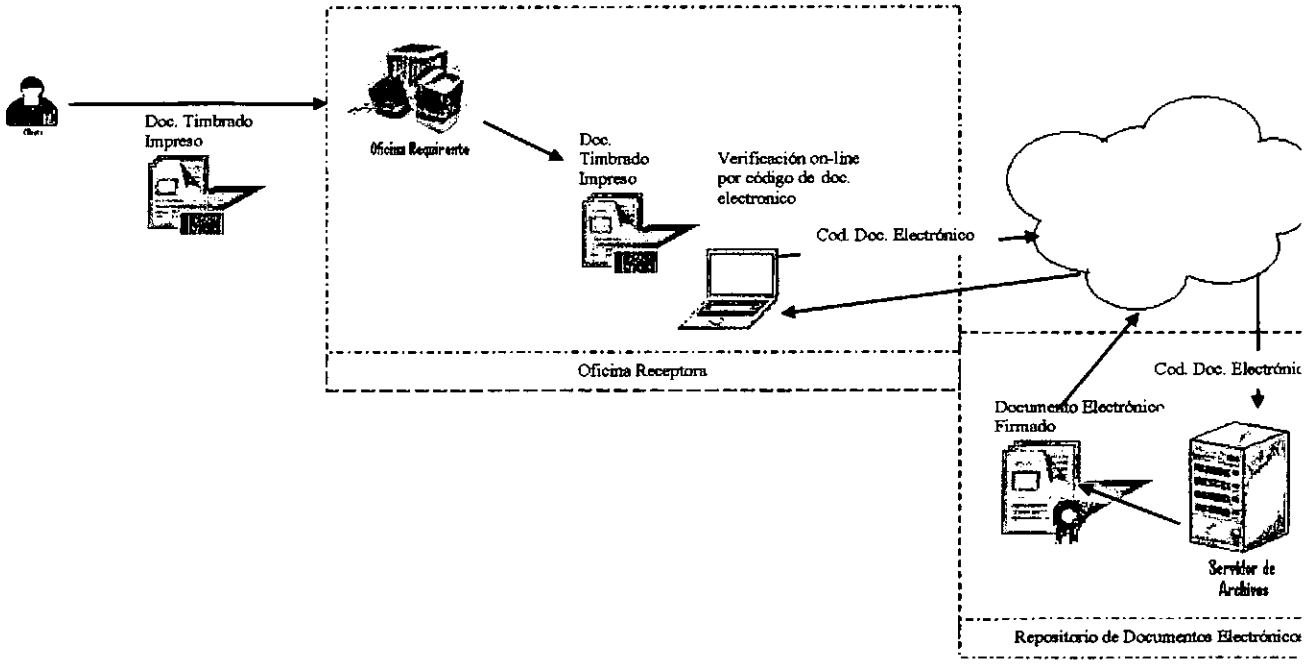


El primer esquema de validación supone la lectura del timbre digital impreso, mediante un dispositivo apropiado de escaneo de códigos de barra. El resultado de este proceso de escaneo es un archivo de texto que se somete luego a un proceso de recodificación de datos, para volver a obtener un objeto de firma PCKS7 codificado, por ejemplo, en CodeBase 64 u otra representación alternativa. Una vez obtenido este objeto de firma es sometido a los procesos habituales de validación de firmas digitales.

Como lo ilustra el esquema, este proceso de validación tiene la ventaja de que puede resolverse por completo en el mostrador del organismo requirente a través de una PC-standalone u otro tipo de dispositivos programables como EPVs, PDAs, notebooks, terminales móviles, etc., sin que se requiera ningún tipo de conexión a servidores centrales para garantizar la validez del documento timbrado impreso.

La desventaja de este modelo es que se requiere de lectores de código de barra en cada uno de los mostradores que realicen la recepción de los documentos timbrados. Esto último puede incrementar los costos para una aplicación particular.

Fig. 3 – Esquema Proceso de Validación On-Line



Un esquema de validación alternativo supone la utilización del código numérico que se generó junto al timbre digital. Este código, que permite identificar unívocamente cada documento emitido, opera como un índice para recuperar el documento electrónico original firmado digitalmente, desde un servidor de archivos.

Este modelo operativo si bien permite prescindir de lectores de código de barra en cada oficina requirente, supone disponer de conectividad al servidor central de archivos y requiere necesariamente que la Autoridad Competente guarde copia de cada documento digital emitido. Estos requerimientos, en ciertas aplicaciones, suponen mantener una infraestructura tecnoló-

gica compleja en términos de volúmenes de almacenamiento, sistemas de gestión de documentos y redes.

La forma de validación apropiada para una implementación de timbre en particular deberá sugerirse de acuerdo a un estudio de factibilidad previo, que contemple las características particulares del proceso o circuito que se modele, valorando aspectos técnicos, operativos, económico-financieros y normativos en cada caso.

2. Estándares

Implementar timbre digital supone contar con un mecanismo de generación de códigos de barra que permitan representar de manera fiable una firma digital. Esta tarea no es sencilla, por cuanto los estándares de código de barras mayormente conocidos y probados no cuentan con las características especiales requeridas para representar una firma digital.

Documentamos a continuación el análisis realizado sobre distintos estándares, los cuáles se dividen básicamente en dos categorías:

- ***Códigos Unidimensionales o Lineales:*** Estos códigos representan la información mediante una serie de barras organizadas en columnas. Este es el modelo más utilizado por la industria y el comercio para identificar productos, nomencladores, cobro de impuestos, etc.
- **Códigos Bidimensionales o Matriciales:** Estos códigos representan la información como una nube de puntos en un arreglo bidimensional de filas y columnas. Esta doble dimensión otorga a este tipo de código la posibilidad de codificar mayor cantidad de información en un espacio menor. Es decir, proporcionan mayor densidad de datos y mejoran la tolerancia a errores haciendo uso de mecanismos de codificación redundante de información.

Los códigos de barras lineales tradicionales actúan generalmente como un índice para encontrar un registro en una base de datos (por ejemplo, un número de parte en un almacén, un número de producto en un supermercado que se liga a un precio, etc.), mientras que los códigos bidimensionales pueden hacer la misma función utilizando significativamente menos espacio e incluso funcionar como la base de datos en si misma por cuanto podrían albergar toda la información que describe un artículo, un ítem o en nuestro caso una firma digital. Para ejemplificar esto, presentamos a continuación el mismo dato codificado: *"123456789012345678 90"* con el mismo ancho de barras o dimensión X de 0.03cms. o 10 ml. Los ahorros en espacio en las simbologías 2D son evidentes.

En contraste con los códigos lineales como el 39 ó el UPC que sólo necesitan codificar entre 10 y 20 caracteres la mayoría de las veces, los códigos bidimensionales pueden codificar varios miles de caracteres legibles por una máquina. Al emplear simbologías 2D, se puede codificar información más detallada y múltiples códigos lineales de una línea pueden ser reducidos a un solo código. Además, los códigos bidimensionales son mucho más resistentes a daños que los lineales, gracias a las fórmulas de corrección de errores que utilizan. Algunos códigos pueden perder hasta un tercio de su superficie y aún ser decodificados.

Los códigos bidimensionales son por tanto, bases de datos portátiles que viajan con una persona, paquete, producto, documento, tarjeta o etiqueta.

Los códigos 2D más empleados en la actualidad son: PDF417, Data-Matrix y MaxiCode. Los ***derechos de propiedad intelectual*** (patentes) para estos códigos son de dominio público, eliminando el pago de regalías para la utilización de esta tecnología.

Los códigos bidimensionales son representados generalmente en simbologías ***matriciales*** o ***apiladas*** (con múltiples renglones).

- Los ***códigos matriciales*** están hechos de un patrón de celdas que pueden ser cuadradas, hexagonales, o circulares y son similares en apariencia a un tablero de ajedrez. Los símbolos matriciales ofrecen mayores densidades de datos que los códigos apilados, a un radio de cerca de 3 ó 4 a 1.
- Los ***códigos de barras apilados*** son como un juego de códigos de barras lineales literalmente apilados uno sobre otro. PDF417 es el mejor ejemplo de un código de barras apilado y es el más común de todos los símbolos 2D de hoy en día.

De la investigación realizada se desprende el estándar ***PDF417*** es el código de barras bidimensional mayormente aplicado en la industria, el comercio y los gobiernos. Este es el estándar utilizado en las distintas experiencias de ***timbre digital*** observadas y el propuesto en la normativa y reglamentación técnica del uso de la ***factura digital*** en el mundo.

Por lo expuesto, profundizamos el estudio sobre esta simbología en particular.

PDF417 – Estándar para la construcción de timbres digitales

La especificación ***UNIFORM SYMBOLOGY SPECIFICATION – PDF417*** fue desarrollada por Symbol Technologies Inc. en 1990 y publicada por ***AIM***, asociación para el Desarrollo de Estándares acreditada por American National Standards Institute.

PDF significa *"Archivo de Datos Portable"* porque puede codificar más de 2725 caracteres de datos en un solo código de barras, comprendiendo *17 módulos*, cada uno conteniendo *4 barras y espacios* (por eso el número "417"). Consiste esencialmente de muchos códigos de barras pequeños apilados. La simbología es capaz de codificar todo el conjunto ASCII (255 caracteres). Cada símbolo tiene un grupo de barra de comienzo y de parada que extiende la altura del símbolo.

La especificación completa para PDF417 proporciona muchas opciones de codificación, incluyendo opciones de ***compresión de datos***, ***detección de errores*** y opciones de ***corrección***, así como tamaño variable y símbolos de proporción de aspecto.

La estructura de bajo nivel de un PDF417 consiste en un arreglo de palabras clave (patrones de barra pequeña y espacio), que están agrupadas y apiladas una encima de la otra para producir todo el símbolo impreso. Una palabra clave individual consiste de un patrón de barra y arreglo bidimensional de foto sensores para escanear la imagen en su totalidad.

Uno de los aspectos beneficiosos de los símbolos bidimensionales es su durabilidad potencial. Para sabotear la legibilidad de un símbolo 1D, basta con agregar otra barra al principio o al final de un símbolo o trazar una línea a través del símbolo, paralela a las rayas. Esto deshace las verificaciones construidas en el algoritmo descodificado de un descodificador 1D y hace el símbolo ilegible. En comparación, se pueden construir muchos ***grados de redundancia*** en un símbolo 2D. Mientras hace al símbolo un tanto más largo, el símbolo resultante es extraordinariamente seguro. Hoy día un número de simbologías 2D está en creciente uso y PDF417 resulta el líder entre ellas.

Principales aspectos a considerar sobre la simbología PDF417 en una implementación de timbrado digital:

Los organismos gubernamentales y empresas que han implementado desarrollos de timbrado digital, prescriben las siguientes recomendaciones a tener en cuenta:

- El principal requerimiento en una implementación de timbre digital, es que a partir de la lectura de los códigos generados se pueda regenerar la firma digital de los ficheros originales y eventualmente algunos o la totalidad de los datos contenidos en los documentos

electrónicos originales. Además es necesario mantener una redundancia de datos para posibilitar la lectura, incluso cuando el código se haya deteriorado en parte. Este rasgo se consigue utilizando el nivel de corrección de errores 5, de la especificación citada.

- Para representar una firma digital, se deberá utilizar la compactación en modo Byte (Byte compaction BC mode) para permitir la codificación de la información en formato BASE code 64.
- Para no limitar el tamaño máximo de datos se sugiere emplear el procedimiento MACRO PDF417. No se debe utilizar el procedimiento denominado Truncated PDF417, para garantizar la lectura de las marcas gráficas generadas.
- Un código de barras 2D 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. Considerando que el timbre puede incluir una o más firmas digitales (dependiendo de la aplicación), quedan fuera de posibles representaciones los estándares como PKCS#7[PKC93] debido a que son demasiado grandes. Las firmas digitales que se usan en el timbre, son en base a certificados digitales. Los certificados digitales se emiten hoy en día, para los algoritmos asimétricos RSA[RSA78] y DSS[Nat99] (con una clara preferencia por RSA). Se sugiere entonces, representar las firmas digitales por un identificador en ASCII (SHA1withRSA o SHA1withDSA), el separador ASCII "-" y el valor de la firma, en el caso RSA usando el estándar PKCS#1[KS98] y en el caso DSS con el estándar ASN.1[ASN97], esto último, por ser las formas más comunes de representar los valores por las aplicaciones y bibliotecas criptográficas. Por otra parte, el código contiene una llave pública. Se recomienda representar esta por un identificador del algoritmo en un código ASCII, seguido de los parámetros del algoritmo en un orden predefinido separados por el carácter ASCII "-".

Si el timbre incluye otros datos o códigos, se recomienda representarlos por código ASCII de una manera legible al ser humano.

Aspectos que se destacan como ventajas de la especificación PDF471

Los organismos y empresas que han elegido PDF417 en sus implementaciones de timbre y factura digital destacan las siguientes ventajas de esta especificación:

- La Tecnología más común en la impresión de etiquetas de Código de Barras es la Transferencia Térmica. Este proceso implica la impresión por medio de cintas (Ribbons), que actúan sobre la superficie mediante el calor generado en la impresora. Por el contrario, la impresión de códigos 2D no requiere de impresoras especiales. Se pueden utilizar impresoras de inyección de tinta o de tecnología láser lo que disminuye requerimientos técnicos especiales.
- Usa algoritmo de corrección de errores que le permite leer símbolos que estén destruidos o dañados en hasta un 50 %. No se tiene información de que este código sea más sensible a deterioros por manchas o arrugas del papel que un código de barras convencional excepto porque ocupa un área mayor en el papel. De todas formas, el daño malicioso al código se puede sancionar por la vía administrativa, tal como se hace actualmente con los documentos ilegibles.
- Es un estándar que se usa cada vez más, debido a que su capacidad de contener información es muy superior a la del código de barras unidimensional. A las pistolas que se utilizan para leer el código de barras unidimensional, se les está incorporando la capacidad de leer PDF417, por tanto se puede esperar que en un futuro próximo el costo y el procedimiento para leer ambos códigos tenderá a igualarse.
- La tecnología tiene una evolución tal que para los equipos móviles actualmente se pueden conseguir pistolas lectoras de códigos de barra

2D de buena manufactura por US$ 300 (las alternativas, de origen asiático, se pueden adquirir por un precio menor). Estas se pueden anexar a una notebook u otro dispositivo de validación portátil, sin incorporar más que los drivers que exige cualquier dispositivo.

F) Conclusiones Preliminares

Según el estudio realizado y las experiencias concretas observadas, se concluye en que el uso de la tecnología de timbre digital, debidamente implementada, aporta un mecanismo alternativo para trasladar los efectos de la firma digital sobre documentos electrónicos, a documentos impresos; con sus correspondientes beneficios para aquellos circuitos administrativos que involucran alguna instancia de impresión de documentos electrónicos firmados digitalmente.

Esta tecnología podría aportar soluciones en áreas tan variadas como:

- ✓ Control de acceso
- ✓ Identificación
- ✓ Fotocredencialización
- ✓ Control de inventario
- ✓ Control de recorridos
- ✓ Alta seguridad
- ✓ Etiquetado en línea
- ✓ Certificaciones y constancias
- ✓ Recepción de materiales
- ✓ Control de producción
- ✓ Control de alimentos perecederos
- ✓ Sanidad
- ✓ Seguridad social
- ✓ Certificación del pago de contribuciones

- ✓ Multas
- ✓ Operaciones de comercio exterior
- ✓ Impuestos fiscales
- ✓ otras.

Los beneficios concretos para una aplicación de gobierno en particular, deberían ser evaluados a la luz de un estudio de factibilidad y de experiencias piloto que permitan obtener algunos indicadores sustanciales, tales como rendimiento, aceptación social, costos, etc.

G) Recomendaciones

Para el desarrollo de la tecnología de timbre digital en el marco de los proyectos de la Unidad de Reforma y Modernización del Estado del Gobierno de Mendoza, se sugiere elaborar una base de ***criterios*** para la selección de procesos susceptibles de ser mejorados con el uso de timbrado digital. Posteriormente se deberá elegir un proceso en particular, para desarrollar una experiencia piloto de aplicación de timbre. En función de la experiencia adquirida y de una cuidadosa evaluación de resultados, se podrá sugerir la escalabilidad de los desarrollos a aplicaciones más ambiciosas.

En cuanto a los aspectos técnicos se recomienda adoptar el estándar de código de barras PDF 417 para la generación del timbre digital, por cuanto esta es la norma más aplicada a nivel mundial en este tipo de desarrollos. Los aspectos más críticos a estudiar en este sentido, son los formatos de representación, codificación, decodificación y validación de las firmas digitales involucradas.

La forma de validación apropiada para una implementación de timbre en particular deberá sugerirse de acuerdo a un estudio de factibilidad previo que contemple las características particulares del proceso o circuito que se modele, valorando aspectos técnicos, operativos, económico-financieros y normativos en cada caso.

III. Transferencia Tecnológica de Firma Digital

Proponemos a continuación la metodología general a seguir para realizar una transferencia tecnológica en materia de firma digital:

A) Nivel I: difusión y sensibilización

Objetivos:

Establecer el primer contacto con los entes u organismos interesados en la transferencia para difundir y sensibilizar acerca de las tecnologías de Firma Digital

Destinatarios:

Directivos de primer nivel y técnicos del ente, organismo o sector relacionado

Medio de Contacto:

Videoconferencia o jornada presencial

Duración estimada:

De una a dos horas (1/2 hs)

Contenidos:

- Exposición sintética de la experiencia de Firma Digital Mendoza
- Espacio para preguntas y debate relativo a la temática relacionada

Material:

Utilización de técnicas de presentación multimedia (Power Point, Flash, etc.)

Informes:

Elaboración de una minuta con los aspectos relevantes y principales conclusiones de la reunión virtual

B) Nivel II: capacitación y asesoramiento general

Objetivos:

Lograr en los destinatarios un conocimiento más profundo de las particularidades y alcances de la tecnología de Firma Digital, preparándolos para identificar implementaciones fundamentadas y con mayor probabilidad de éxito

Destinatarios:

- Funcionarios de primer, segundo y tercer nivel de gestión
- Personal Técnico y Administrativo

Medio de Contacto:

Jornada a realizarse preferentemente en el ente, organismo o sector relacionado

Duración estimada:

Jornada Doble (6 hs totales), divididas entre mañana y tarde

Contenidos:

- ***Conceptos Básicos:*** se explican y presentan las principales nociones en materia de firma digital

- ***Tecnologías de Firma Digital:*** se explican las diferentes líneas tecnológicas de implementación disponibles para transferencia de Firma Digital
  - Firma Digital de Formularios Web
  - Sitio Seguro
  - Correo Seguro
  - Firma Digital de Archivos
  - Firma Digital de Documentos PDF
  - Timbre Digital

- ***Análisis de Factibilidad:***
  - Factibilidad Operativa: se explicitan las condiciones que deben cumplirse y las acciones que deben desarrollarse para lograr con alto grado de seguridad, funcionalidad y operatividad del modelo a plantear. En tal sentido se presenta una enumeración de factores a tener en cuenta al pensar en implementaciones de Firma Digital
  - Factibilidad Económica-Financiera: desde una perspectiva amplia de costo/beneficio se aborda la factibilidad económico-financiera de implementaciones de Firma Digital y sus servicios asociados, desglosando las dos grandes dimensiones que implica ésta relación.
  - Factibilidad Legal: se presenta la estructura jurídica de la firma digital, como sustituto válido y seguro en los documentos digitales, de la firma ológrafa, además se presenta el Modelo Jurídico adoptado por la Provincia de Mendoza de Adhesión a la Ley Nacional de Firma Digital

- **Identificación de Procedimientos:** se presenta una estrategia práctica de identificación de circuitos y transacciones con el objeto de facilitar la elección y priorizar los circuitos administrativos adecuados para implementaciones piloto, según su alcance y los ámbitos de aplicación de los servicios de criptografía asimétrica para lograr ahorros y no incurrir en sobrecostos de implementación
- **Ejercicio práctico:** se propone a la audiencia desarrollar un taller consistente en la resolución de un ejercicio práctico relacionado con la temática del nivel II luego, se presentan y analizan las conclusiones obtenidas

Material:

Utilización de técnicas de presentación multimedia (Power Point, Flash, etc.)

Entrega de Material Didáctico impreso sobre los contenidos de la capacitación:

- Presentaciones
- Estrategia de Identificación de Procedimientos
- Caso Práctico

Entrega de Convenio Marco y documentación modelo para formalizar nivel III, en caso de existir probado interés por parte de la Provincia

Informes:

Elaboración de una minuta con los aspectos relevantes y principales conclusiones de la reunión

C) Nivel III: Talleres de Trabajo

Objetivos:

Identificar, Diseñar e implementar una experiencia concreta de firma digital en el ente, organismo o sector relacionado

Destinatarios:

- Funcionarios de primer, segundo y tercer nivel de gestión
- Personal Técnico y Administrativo

Medio de Contacto:

En función de la naturaleza particular de la actividad a realizar, se prevé instancias presenciales para las principales tareas de determinación y desarrollo de la experiencia y para el seguimiento instancias de videoconferencia, mail, chat, teléfono, etc.

Duración estimada:

Variable de 3 a 6 meses en función de las características particulares de la transferencia y del ámbito en el que se desarrollará. (Tiempo estimado

para la puesta en marcha de la implementación, una vez superadas las etapas previas de análisis y diseño)

Actividades:

- **Determinación de la Experiencia:** a partir de la identificación de procedimientos y transacciones aptas presentado en el nivel II, se precisa conjuntamente con los funcionarios y el personal del organismo la naturaleza y particularidades de la implementación que se desea llevar a cabo

- **Análisis y Diseño de la Experiencia:**
  - Identificación de la necesidad: se recopila y analiza información, se entrevista a los posibles usuarios y se precisa la necesidad de aplicación de la 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

  - Diseño de un Plan de Trabajo: se elabora un Plan de Trabajo para llevar adelante la implementación

- **Determinaciones sobre la provisión de certificados:** se analizan las alternativas de provisión de certificados en función del tipo de implementación, se elige la mejor alternativa factible y se realizan las gestiones, convenios y actividades necesarias en consecuencia

- **Determinación de Actores y condiciones previas:**

- Se precisan los perfiles de personal *(ver consideraciones finales)*, las decisiones de naturaleza política y los requerimientos tecnológicos necesarios para llevar a cabo una efectiva implementación

- Se identifican los actores y responsables de la experiencia y se le asignan actividades en función del Plan de Trabajo Propuesto

- Se confecciona Acta Complementaria al Convenio Marco que formaliza el Nivel III, con el detalle y precisiones del análisis y diseño de la experiencia (Plan de Trabajo, Designación de responsables, etc).

- **Implementación de la experiencia:**

  - Ejecución del Plan de Trabajo: se ejecuta el Plan de Trabajo para llevar adelante la implementación

  - Desarrollo e implementación: se lleva a la práctica la experiencia 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 que a futuro permitirán evaluar el éxito de la implementación

Informes:

Elaboración de informes periódicos con el avance de las actividades planificadas según el Plan de Trabajo, los aspectos relevantes y matices del desarrollo de la transferencia.

CONDICIONES PARTICULARES

En función de las características particulares de esta transferencia hemos incluido aquí algunas salvedades y aclaraciones para mejorar la comprensión de la Metodología propuesta:

Niveles: esta metodología de transferencia ha sido estructurada en tres niveles (I, II y III) con grado creciente de compromiso y profundidad. En consecuencia, de acuerdo a la conveniencia y las circunstancias, el desarrollo de la transferencia podrá definirse con el consenso de los referentes del CFI como sigue:

- Transferencia de Nivel I
- Transferencia de Nivel II (incluye nivel I y II)
- Transferencia de Nivel III (incluye nivel I, II y III)

Estimación de tiempos: para el caso de una transferencia de Nivel III, la estimación de tiempos se hará en cada caso particular en función de las características singulares de la experiencia, tales como tipo y diseño de implementación y circunstancias locales del organismo, dependencia o ente donde se desea aplicar.

Provisión de certificados: en principio existen dos alternativas para resolver el problema de la provisión de certificados, la primera y recomendada por nuestro equipo para dependencias de gobierno, es la de establecer

una Autoridad de Registro de la Autoridad Certificante de la Oficina Nacional de Tecnologías de Información (AC-ONTI), la segunda por supuesto es la tercerización por vía privada.

La primer alternativa implica el contacto con la Onti la realización de un convenio y una serie de requisitos administrativos necesarios para su puesta en marcha. En especial en el primero caso, ésta consultoría puede hacerse cargo de las tareas de contacto, asesoramiento implementación efectiva de la Autoridad de Registro previa autorización por parte de la Onti.

CONSIDERACIONES FINALES

Comunidad Virtual: se prevé la creación de un grupo de trabajo virtual, en donde se pueda intercambiar, compartir y consolidar los avances logrados por los "niveles III" de transferencia tecnológica de firma digital. De esta manera se espera lograr una sinergia tal, que ahorre costes en I+D y beneficie al desarrollo de aplicaciones en el ámbito particular de cada miembro participante del grupo.

Perfiles de personal: el desarrollo de aplicaciones de firma digital para la administración pública requiere de un equipo multidisciplinario que busque integrar desde sus conocimientos y experiencias previas, las tres dimensiones fundamentales desde la que se deben concebir este tipo de desarrollos: la dimensión legal, la dimensión tecnológica y fundamentalmente la dimensión operativa.

Independientemente de la experticia que aporte cada persona, se requieren ciertas características comunes en el equipo que garanticen un adecuado nivel de integración en la planificación y ejecución del proyecto. El dinamismo, la gestión por objetivos, la mentalidad abierta, el espíritu emprendedor y la diversidad son algunos de los rasgos distintivos que deben caracterizar al grupo. Poseer una manifiesta vocación por aprender, incorpo-

rar nuevos conceptos y pensar diferente es una premisa fundamental en toda experiencia que pretenda modernizar la administración pública.

Planteamos a continuación las competencias requeridas para cada uno de los perfiles que deberían constituir el equipo:

Consultor Legal

Se piensa en un abogado con amplios conocimientos en derecho administrativo y vasta experiencia en la Administración Pública local.

Se valorará significativamente la experiencia en informática jurídica, delito informático y la comprensión del marco legislativo nacional e internacional sobre firma digital.

Desarrollador

Se piensa en un profesional del área de Sistemas o carrera afín con experiencia en:

- desarrollo de aplicaciones web
- programación en lenguaje Java
- desarrollo de Bases de Datos y lenguaje SQL
- instalación, configuración y administración de webservers (Apache, IIS)

Se valorarán conocimientos y experiencia en:

- arquitecturas PKI.
- criptografía simétrica y asimétrica.
- instalación y configuración de servidores de aplicación (JBoss, Tomcat, etc.).
- administración y tuning de Bases de Datos.
- desarrollo sobre tecnología J2EE.
- Desarrollo en lenguaje php y asp.
- modelado UML.
- XML y webservices.

Se considera un aporte fundamental la experiencia previa de trabajo en la Administración Pública.

Integrador

Se piensa en un profesional con formación de grado en administración y especialización en gestión de tecnologías. Son requisitos mínimos:

- amplio dominio de TICs
- conocimientos de formulación y conducción de proyectos con administración por objetivos
- conocimientos sobre la estructura organizativa, la normativa y los procesos de la Administración Pública Local.
- visión innovadora de la administración pública y la gestión para el ciudadano
- habilidades para buscar oportunidades de financiamiento, obtener apoyo político e identificar grupos o comunidades de interés.
- experiencia en liderazgo de proyectos de integración tecnológica y de servicios.

D) Marco Jurídico

Presentamos a continuación un modelo de convenio marco que se podrá utilizar para otorgar validez jurídica a la experiencia:

CONVENIO MARCO

Provincia de Mendoza

.....

Consejo Federal de Inversiones

Entre el Gobierno de la Provincia de Mendoza, representado por el Sr. Gobernador Ing. Julio César Cleto Cobos; el Gobierno de la Provincia de ....., representado por el SR. Gobernador..... ; y el Consejo Federal de Inversiones, representado por su Secretario General, Ing. Juan José CIACERA;

CONSIDERANDO

Que la evolución de las tecnologías de la información y la comunicación permite la adopción de nuevas estrategias de seguridad y de gestión de los servicios que presta el Estado.

Que a la necesidad de un Estado más eficiente, se le suman, ahora, estímulos tecnológicos que permiten colocar a las TICs directamente al servicio de la comunidad y del propio Estado.

Que el Estado debe cumplir un rol fundamental en todo proceso de cambio y debe liderarlo, transformándose en usuario modelo de las tecnologías de la información y las comunicaciones, actuando como catalizador del desarrollo y la innovación en el uso de nuevas herramientas.

Que la política de modernizar y reformar el Estado se concibe como respuesta a las necesidades de la ciudadanía con servicios efectivos y de calidad.

Que el Consejo Federal de Inversiones viene desarrollando acciones tendientes a intercambiar experiencias exitosas relacionadas con la incorporación de tecnologías de información y comunicaciones a la gestión del Estado.

Que la Provincia de Mendoza, a través de la Unidad de Reforma del Estado, con financiamiento del Consejo Federal de Inversiones, ha desarro-

llado un considerable Know How y ha implementado prácticas exitosas en materia de Firma Digital

Que la Provincia de ..... ha manifestado interés en avanzar en la mejora de los servicios a los ciudadanos a través de la incorporación de nuevas herramientas tecnológicas.

ACUERDAN

PRIMERO: El Consejo Federal de Inversión y el Gobierno de la Provincia de Mendoza se comprometen a establecer un programa de colaboración, capacitación, asistencia técnica y transferencia tecnológica en materia de "Firma Digital", al Gobierno de la Provincia de .....

SEGUNDA: Las partes acuerdan la prestación recíproca de cooperación en todos aquellos aspectos que concurran al cumplimiento del acuerdo general señalado en la cláusula precedente, incluyendo el suministro de antecedentes, información general, estudios y proyectos con fines de mejoramiento y especialización y asistencia técnica, siendo la presente enunciación no taxativa, por lo que se considerarán incluidos todos aquellos aspectos que perfeccionen el objetivo del presente convenio.-

TERCERA: Las partes designan en la presente a los Coordinadores Técnicos en materia de sus respectivas competencias que tendrán a su cargo la supervisión de las actividades acordadas a realizar por cada una de ellas. En tal sentido, se designa como Coordinadores Técnicos, por el Gobierno de Mendoza a ....., por el Gobierno de ..... a ..... y por el Consejo Federal de Inversiones a.....

CUARTA: Las actividades a desarrollar serán definidas de acuerdo con las necesidades emergentes y con el nivel de transferencia y serán aprobadas por los Coordinadores Técnicos mediante la suscripción de Actas Complementarias numeradas correlativamente que integrarán el presente Convenio, en las cuales se establecerán las modalidades y condiciones de participación, los responsables de la ejecución, objetivos, tareas y los recursos a aportar por las partes.-

QUINTA: Las partes se comprometen a apoyar operativamente la organización de las distintas actividades que se realizan en su ámbito, disponiendo de recursos humanos y material técnico – administrativo que se requiera para el cumplimiento del presente Convenio.

Puntualmente, el Consejo Federal de Inversiones se compromete a designar los responsables técnicos para realizar la coordinación y seguimiento de la asistencia técnica y transferencia tecnológica de Firma Digital desde el gobierno de la Provincia de Mendoza al Gobierno de la Provincia de ..... y financiar los gastos de traslados y viáticos del personal técnico de la provincia de Mendoza que capacitará a los técnicos y usuarios designados para el proyecto por el Gobierno de la Provincia de.....

SEXTA: Toda cuestión que suscitare o que no estuviere contemplada en este Convenio o en las Actas Complementarias, será resuelta de común acuerdo entre las partes, teniendo en cuenta el fin público que se persigue.-

SEPTIMA: Este Convenio tendrá una duración de 1 (UN) año a partir de la fecha de celebración, pudiendo ser denunciado por cualquiera de las partes mediante comunicación expresa y fundada, realizada por lo menos con treinta (30) días de anticipación. En este supuesto y dentro de las posibilidades, las partes tratarán de dar finalización a la actividad y/o etapa en que se encuentre el desarrollo de las acciones. El Gobierno de Mendoza, El Conse-

jo Federal de Inversiones y la Provincia de ..... resolverán en forma expresa la prórroga o renovación del presente convenio.-

OCTAVO: Los derechos de propiedad, autor, reproducción, modificación, así como todo otro, cualquiera sea su naturaleza, se consideran propiedad del CFI, quién es el único habilitado para introducir las modificaciones que resulten necesarias para optimizar el uso de las herramientas y publicar los resultados obtenidos por cualquier medio.

NOVENO: Las partes deberán considerar información confidencial toda la que reciban o llegue a su conocimiento con motivo de las tareas que se les encomiende. En consecuencia quedarán obligados a no revelar o suministrar total o parcialmente la información a ninguna persona ajena a las partes involucradas en el presente, ya fuere durante o después de la expiración del presente convenio. El incumplimiento por parte de los participantes de las obligaciones asumidas será considerado falta grave y causa suficiente para que se deje sin efecto el presente convenio.

En prueba de conformidad, se firman tres (3) ejemplares de un mismo tenor y a un solo efecto, a los ..... días del mes de .....de 2003.

Consejo Federal de Inversiones
Lic. Pablo Guillermo Lioy
"Firma Digital"

IV. Identificación de experiencia de timbrado digital:

En función de las particularidades de la Tecnología de Timbre Digital y del nuevo desafío que plantea determinar a priori que condiciones deben asegurarse para lograr una aplicación con alta probabilidad de éxito, hemos realizado un estudio de investigación mucho más amplio, cuyas principales conclusiones nos permitirán realizar, de manera más precisa la elección del circuito adecuado que maximice la utilidad de la tecnología en la implementación

Concretamente, los circuitos analizados fueron los siguientes:

Circuito	Dependencia
Pago de Multas de Tránsito	Municipalidad de Godoy Cruz
Certificados de Libre Deuda	Municipalidad de Godoy Cruz
Certificados de Buena Conducta	Policía Científica de Mendoza
Certificaciones de Ingresos	Dirección General de Escuelas
Bonos de Sueldos	Dirección General de Escuelas
Constancias de designación en cargos	Dirección General de Escuelas
Constancias de Alumno Regular	Dirección General de Escuelas
Constancia de Pago	Dirección General de Rentas
Impresión de Boletos de Pago	Dirección General de Rentas
Libre Deuda	Dirección General de Rentas
Impresión de Boletos de Pago	Departamento de Irrigación
Tarjeta Única Migratoria (TUM)	Dirección Nacional de Migraciones
Constancia de Beneficio Sociales	Ministerio de Desarrollo Social
Registro de la Propiedad	Instituto Provincial de la Vivienda

Conclusiones

De la consideración analítica de los circuitos plasmados en la Tabla anterior surgieron algunas precisiones conceptuales que determinaron las características y los factores que resultan deseables a la hora de pensar en una aplicación de Timbre Digital que cuente con una alta probabilidad de éxito, a saber:

- **Tipo de Circuito:**

  Las características particulares de la tecnología de timbre digital, determinan la elección de aquellos procedimientos o circuitos que tienen como producto final la impresión en soporte papel de constancias, recibos de pago o certificados de cualquier naturaleza. Debemos dar prioridad a estos circuitos, teniendo en cuenta que este tipo de tecnología resulta ideal al momento de digitalizar con valor legal tales comprobantes ya que asegura la autenticidad y verificabilidad del mismo.

- **Carácter gratuito:**

  No resulta una condición del todo esencial, pero en tanto los medios de pagos por vías electrónicas como los instrumentados por banca electrónica, por tarjeta con seguridad añadida, dinero electrónico, sistemas tipo pay pal o tarjetas monedero (que se están estudiando conjuntamente con el proyecto de Medios de Pago, de la Unidad de Reforma y Modernización del Estado con financiación del CFI), no se constituyan en una realidad cierta en la Provincia de Mendoza, esta consultoría aconseja la elección de circuitos que se encuentren exentos de retribución monetaria por parte de los administrados. Tal aseveración corresponde mayormente a cuestiones de índole operativa en pos de la implementación inicial rápida y con plena funcionalidad en términos de utilidad para el ciudadano, de la tecnología de timbre digital

- **Sistematización de la información:**

También atendiendo a cuestiones que mejoran calidad de la implementación en términos de resultados en el tiempo, es recomendable la elección de procedimientos que manejen un alto porcentaje de información ya sistematizada y digitalizada. Como así también aquellos que gocen de una alta repetitividad y no requieran por norma legal de la intervención de una persona física autorizada para la firma, de esta manera se puede pensar en aplicaciones dónde quien firma sea un servidor seguro con acceso a bases de datos seguras de manera automática y transparente para el usuario

- **Disminución de tareas administrativas:**

Circuitos que por sus características insumen gran cantidad de personal abocado a tareas de atención al público, manuales y administrativas que son susceptibles de liberarse con la aplicación de timbre digital, liberando recursos para otras áreas y aumentando a la vez la eficiencia y eficacia en la prestación de servicios al ciudadano

- **Despapelización:**

Aquellos procedimientos que involucren mayor cantidad de papeleo que puede sustituirse por medios digitales de conservación resultado de la aplicación de la tecnología de firma y timbre en su fase final de producto. Por ejemplo bonos de sueldos digitalizados que sólo se imprimirán en caso de ser presentados ante oficinas que no cuenten con medios de validación on-line

- **Estrategia multicanal:**

Tal estrategia es la génesis de la necesidad de estudio y aplicación de esta tecnología determinada por ésta consultoría. Se trata de utilizar al timbre como forma de bajar la firma digital al papel y no frenar implementaciones de gran potencialidad en términos de beneficios, por la existencia de instancias en las que no existe otra alternativa por el momento que bajar al papel.

- **Utilidad para el usuario:**

Este factor es muy importante siempre que tengamos 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. Es decir, generalmente el costo de impresión en papel (por ejemplo de un certificado de libre deuda) se traslada enteramente al usuario que desde su casa realiza el trámite. Este costo debe resultar, como regla, menor a la retribución final por él percibida al utilizar este medio.

- **Ahorro de tiempos:**

  De forma consistente con las afirmaciones anteriores, debemos priorizar aquellos circuitos que determinen aplicaciones de timbre digital con mayor potencial de beneficios para el usuario en términos de ahorro de tiempo de ejecución, procurando agilizar significativamente la realización del trámite.

- **Disminución de Colas:**

  Aquellos circuitos o trámites que signifiquen grandes colas, mala atención al público o baja eficiencia por falta de personal en las dependencias de la Administración Pública Provincial

- **Distribución geográfica:**

  Trámites con alto grado de distribución geográfica de usuarios, tales como aquellos de nivel provincial en donde la aplicación de estas tecnologías determinan en gran ahorro en términos de costos y tiempo de traslado hasta la dependencia en dónde se realiza

V. Diseño de experiencia de timbrado digital

En función de las particularidades de la Tecnología de Timbre Digital y del nuevo desafío que plantea determinar a priori que condiciones deben asegurarse para lograr una aplicación con alta probabilidad de éxito, hemos realizado un estudio de investigación mucho más amplio, cuyas principales conclusiones nos permitirán realizar, de manera más precisa la elección del circuito adecuado que maximice la utilidad de la tecnología en la implementación

De la consideración analítica de los circuitos plasmados en la Tabla anterior surgieron algunas precisiones conceptuales que determinaron las características y los factores que resultan deseables a la hora de pensar en una aplicación de Timbre Digital que cuente con una alta probabilidad de éxito.

A través de un análisis más profundo de tales procedimientos hemos decidido trabajar sobre dos de ellos que cumplieron satisfactoriamente la mayoría de los factores exigidos.

Procedimiento de solicitud y emisión de Certificado de Buena Conducta

- **Tipo de Circuito:**

Este procedimiento tiene como producto final la impresión en soporte papel de una ***Certificación de Antecedentes Judiciales y Policiales o de Buena Conducta***. Priorizamos este circuito, teniendo en cuenta que este tipo de tecnología resulta ideal al momento de digitalizar con valor legal tales comprobantes ya que asegura la autenticidad y verificabilidad del mismo.

- **Carácter gratuito:**

Hemos elegido las modalidades para este procedimiento que se encuentran exentas de retribución monetaria por parte de los ciudadanos usuarios. Tal condición facilita considerablemente cuestiones de índole operativa en pos de la implementación inicial rápida y con plena funcionalidad en términos de utilidad para el ciudadano, siempre que este ***no necesita trasladarse personalmente, ni hacer colas*** para de realizar el trámite.

- **Sistematización de la información:**

Atendiendo a cuestiones que mejoran calidad de la implementación en términos de resultados en el tiempo, este procedimiento maneja un considerable porcentaje de información ya sistematizada y digitalizada, como lo es la consulta de antecedentes judiciales y penales por sistema. Además cuenta con una alta repetitividad ya que se solicitan alrededor de ***100 certificados diarios.***

- **Disminución de tareas administrativas:**

Este circuito, por sus características, insume gran cantidad de personal abocado a ***tareas de atención al público que son susceptibles de liberarse con la aplicación de timbre digital***, liberando recursos para otras áreas y aumentando a la vez la eficiencia y eficacia en la prestación de servicios al ciudadano

- **Estrategia multicanal:**

Tal estrategia es la génesis de la necesidad de estudio y aplicación de esta tecnología determinada por ésta consultoría. Se trata de utilizar al timbre como forma de bajar la firma digital al papel, es decir los certificados de buena conducta firmados digitalmente no necesitarán, en un futuro, ser impresos para presentarlos en instituciones

educativas o a empleadores, sino que ***se podrán chequear directamente de un repositorio digital accesible vía web.***

- **Utilidad para el usuario:**

Este factor es muy importante siempre que tengamos 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. Es decir, en este procedimiento, el costo de impresión en papel se traslada enteramente al usuario que desde su casa realiza el trámite. Este costo resultará ínfimo frente a la retribución final por él percibida al utilizar este medio, a saber:

  - **Ahorro de tiempos y Disminución de Colas:**

    La aplicación de este procedimiento, como se verá más adelante, agiliza significativamente la realización del trámite, ya que el usuario no debe realizar ningún tipo de cola ni para iniciar el trámite ni para retirarlo, lo que redunda en un considerable ahorro de su tiempo.

  - **Distribución geográfica:**

    Al tratarse de un trámite a nivel provincial tiene un alto grado de distribución geográfica de ciudadanos usuarios, es aquí donde la aplicación de estas tecnologías determinan un gran ahorro en términos de costos y tiempo de traslado hasta la dependencia en dónde se realiza ya que los suprime de plano.

Procedimiento de solicitud y emisión de Certificado de Servicios y Remuneraciones

- **Tipo de Circuito:**

Este procedimiento tiene como producto final la impresión en soporte papel de una ***Certificación de Servicios y Remuneraciones.*** Priorizamos este circuito, teniendo en cuenta que este tipo de tecnología resulta ideal al momento de digitalizar con valor legal tales comprobantes ya que asegura la autenticidad y verificabilidad del mismo.

- **Carácter gratuito:**

Este procedimiento se encuentra exento de retribución monetaria por parte de los solicitantes. Tal condición facilita considerablemente cuestiones de índole operativa en pos de la implementación inicial rápida y con plena funcionalidad en términos de utilidad para el ciudadano, siempre que este ***no necesita trasladarse personalmente*** para de realizar el trámite.

- **Sistematización de la información:**

Atendiendo a cuestiones que mejoran calidad de la implementación en términos de resultados en el tiempo, este procedimiento maneja un considerable porcentaje de información ya sistematizada y digitalizada, como lo es la consulta por sistema de recursos humanos de las remuneraciones percibidas por el solicitante.

- **Disminución de tareas administrativas:**

Este circuito, por sus características, insume gran cantidad de personal abocado a ***tareas administrativas manuales de confección de formularios que son susceptibles de liberarse con la digitalización y aplicación de timbre digital***, liberando recursos para

otras áreas y aumentando a la vez la eficiencia y eficacia en la prestación del servicio.

- **Despapelización:**

Este procedimiento involucra papeleo que puede sustituirse por medios digitales de conservación resultado de la aplicación de la tecnología de firma y timbre en su fase final de producto. De esta manera ***se reduce considerablemente el costo de confección e impresión de formularios y el espacio físico que insumen.***

- **Estrategia multicanal:**

Tal estrategia es la génesis de la necesidad de estudio y aplicación de esta tecnología determinada por ésta consultoría. Se trata de utilizar al timbre como forma de bajar la firma digital al papel, es decir los certificados servicios y remuneraciones firmados digitalmente no necesitarán, en un futuro, ser impresos para ser presentados en el Anses, sino que ***se podrán chequear directamente de un repositorio digital accesible vía web.***

- **Utilidad para el usuario:**

Este factor es muy importante siempre que tengamos 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. Es decir, en este procedimiento, el costo de impresión en papel se traslada enteramente al usuario que desde su casa realiza el trámite. Este costo resultará ínfimo frente a la retribución final por él percibida al utilizar este medio, a saber:

- **Distribución geográfica:**

La aplicación de estas tecnologías determina aquí un gran ahorro en términos de costos y tiempo de traslado hasta la dependencia en dónde se realiza el trámite ya que los suprime de plano.

- **Ahorro de tiempos y Disminución de Colas:**

La aplicación de este procedimiento, como se verá más adelante, agiliza significativamente la realización del trámite, ya que la Subdirección de Personal deja de realizar tareas administrativas manuales que insumen la mayor cantidad del tiempo total de solicitud/entrega del trámite.

A) Diseño de la implementación

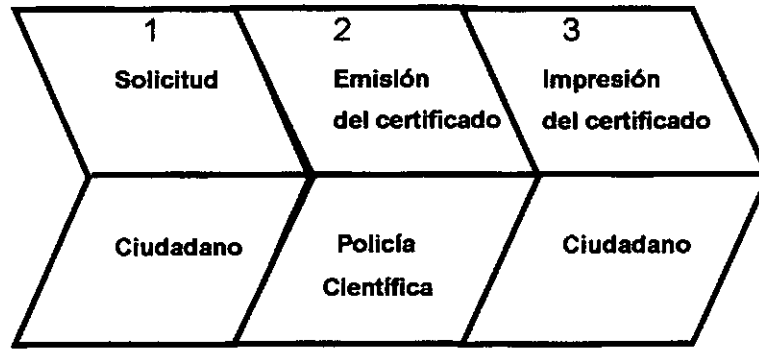
Procedimiento de solicitud y emisión de Certificado de Buena Conducta

El presente procedimiento describe el conjunto de pasos a realizar por el personal de la Policía Científica de Mendoza y los ciudadanos/usuarios que requieran Certificación de Buena Conducta.

Secuencia Sintética del Proceso

(Arrow chart)

Etapas



Principal sector interviniente

Objetivo:

A través de la redacción de este procedimiento se busca formalizar las tareas que lo conforman y fortalecer el diseño administrativo con la implementación de tecnología de firma y timbre digital en el mismo. Además, se busca asegurar garantías de autenticidad e integridad de las certificaciones entregadas.

Alcance:

Este procedimiento es de aplicación en toda la Provincia de Mendoza y se aplica a las certificaciones de buena conducta requeridas con motivos laborales o de estudios.

Definición de Roles

Responsable del Procedimiento: Crio Insp Rubilar Juan Carlos
Oficina Policía Científica. Div. Antecedentes Personales
Ministerio de Justicia y Seguridad

Descripción del Procedimiento:

1. ***Ciudadano/Solicitante:*** ingresa al Sitio Web de la Guía de Trámites, en e-trámite por Internet http://www.tramite.mendoza.gov.ar/ y elige la opción Cerificado de Buena Conducta. A continuación, si cumple con los *requisitos establecidos, completa y envía un formulario de solicitud web con sus datos y toma nota del código único de identificación de su trámite y de la dirección del repositorio digital dónde estará sus certificado dentro de los siguientes 2 días hábiles.

2. ***Policía Científica de Mendoza:*** recibe la solicitud web, procesa los datos y controla que la persona solicitante no tenga antecedentes. En caso que esté todo correcto emite certificado de buena conducta, lo firma y lo timbra digitalmente dejándolo disponible para ser bajado en un repositorio digital. En caso de tener antecedentes o cualquier tipo de inconveniente por el cual no se pueda emitir el certificado a su nombre, se le emite por sistema la advertencia con las instrucciones a seguir y se deja constancia en el repositorio digital.

3. ***Ciudadano/Solicitante:*** ingresa al repositorio digital con su código único de identificación, retira su certificado de buena conducta digital y lo im-

prime con timbre digital. En este certificado consta que su periodo de validez será de tres meses a partir de la fecha de emisión y las instrucciones pertinentes para validarlo a partir de su timbre digital.

Requisitos

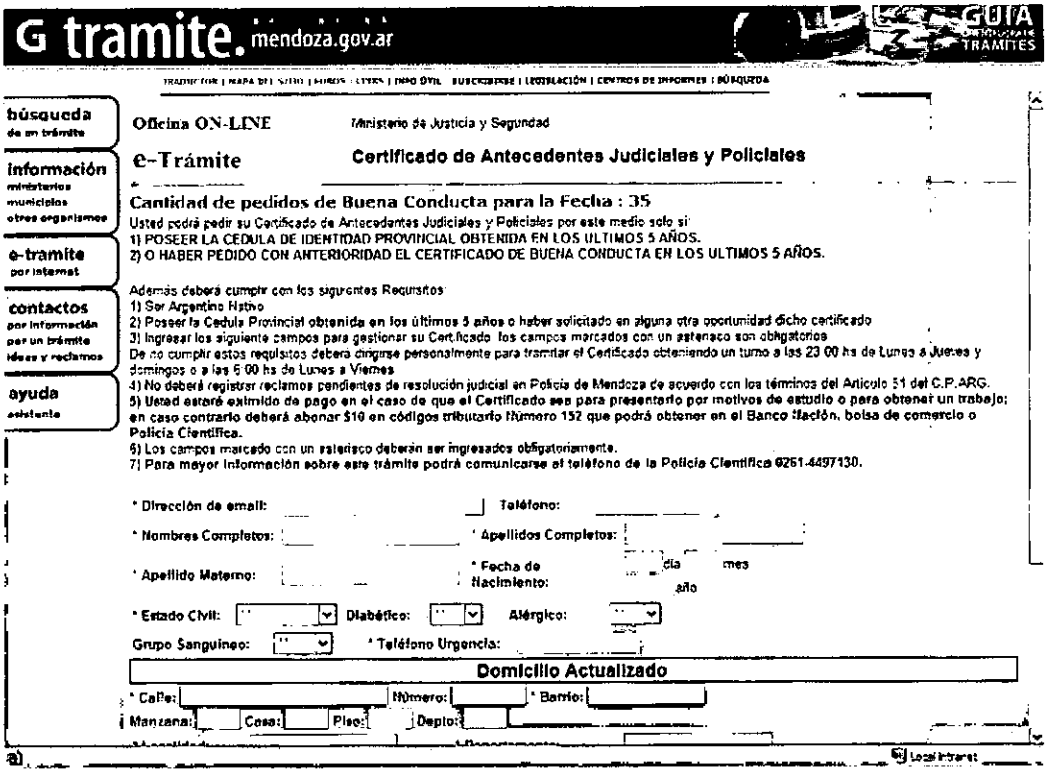
Podrá pedir su Certificado de Antecedentes Judiciales y Policiales por este medio solo si:

1) Posee la cedula de identidad provincial obtenida en los últimos 5 años.
2) o haber pedido con anterioridad el certificado de buena conducta en los últimos 5 años.

Además deberá:
1) Ser Argentino Nativo.
2) Poseer la Cedula Provincial obtenida en los últimos 5 años o haber solicitado en alguna otra oportunidad dicho certificado.
3) Ingresar los campos para gestionar su Certificado, los campos marcados con un asterisco son obligatorios.
De no cumplir estos requisitos deberá dirigirse personalmente para tramitar el Certificado obteniendo un turno a las 23:00 hs de Lunes a Jueves y domingos o a las 6:00 hs de Lunes a Viernes.
4) No deberá registrar reclamos pendientes de resolución judicial en Policía de Mendoza de acuerdo con los términos del Artículo 51 del C.P.ARG.
5) Usted estará eximido de pago en el caso de que el Certificado sea para presentarlo por motivos de estudio o para obtener un trabajo.

Adjuntos

Formulario de solicitud web de certificación de buena conducta



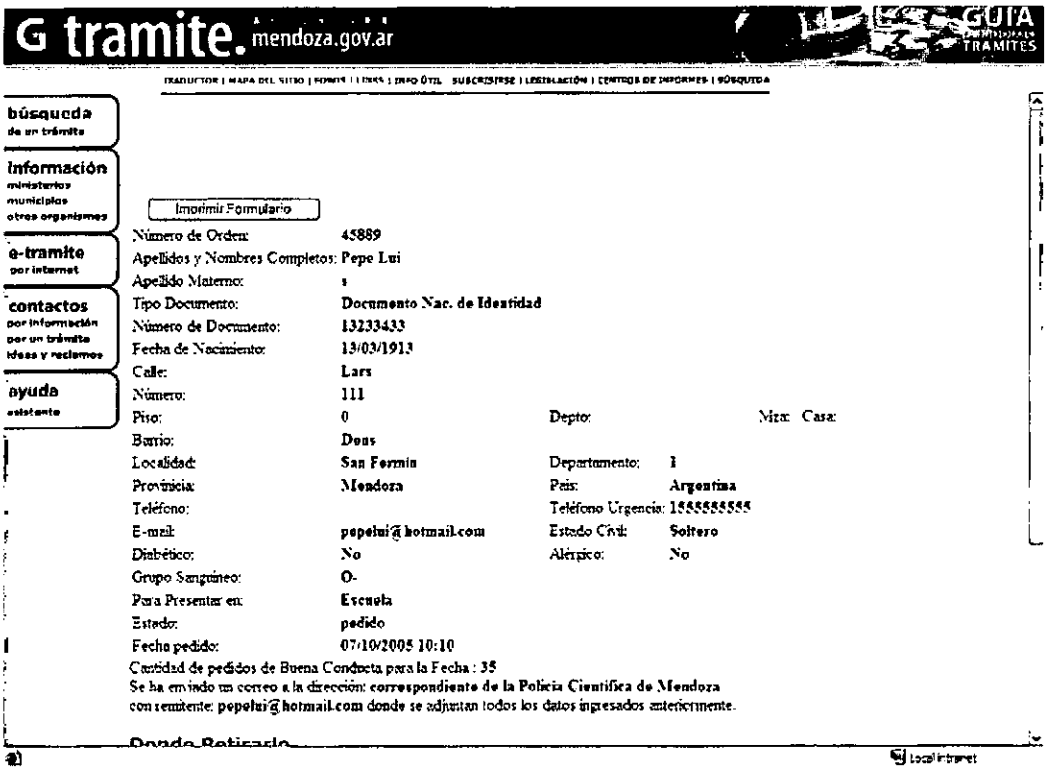
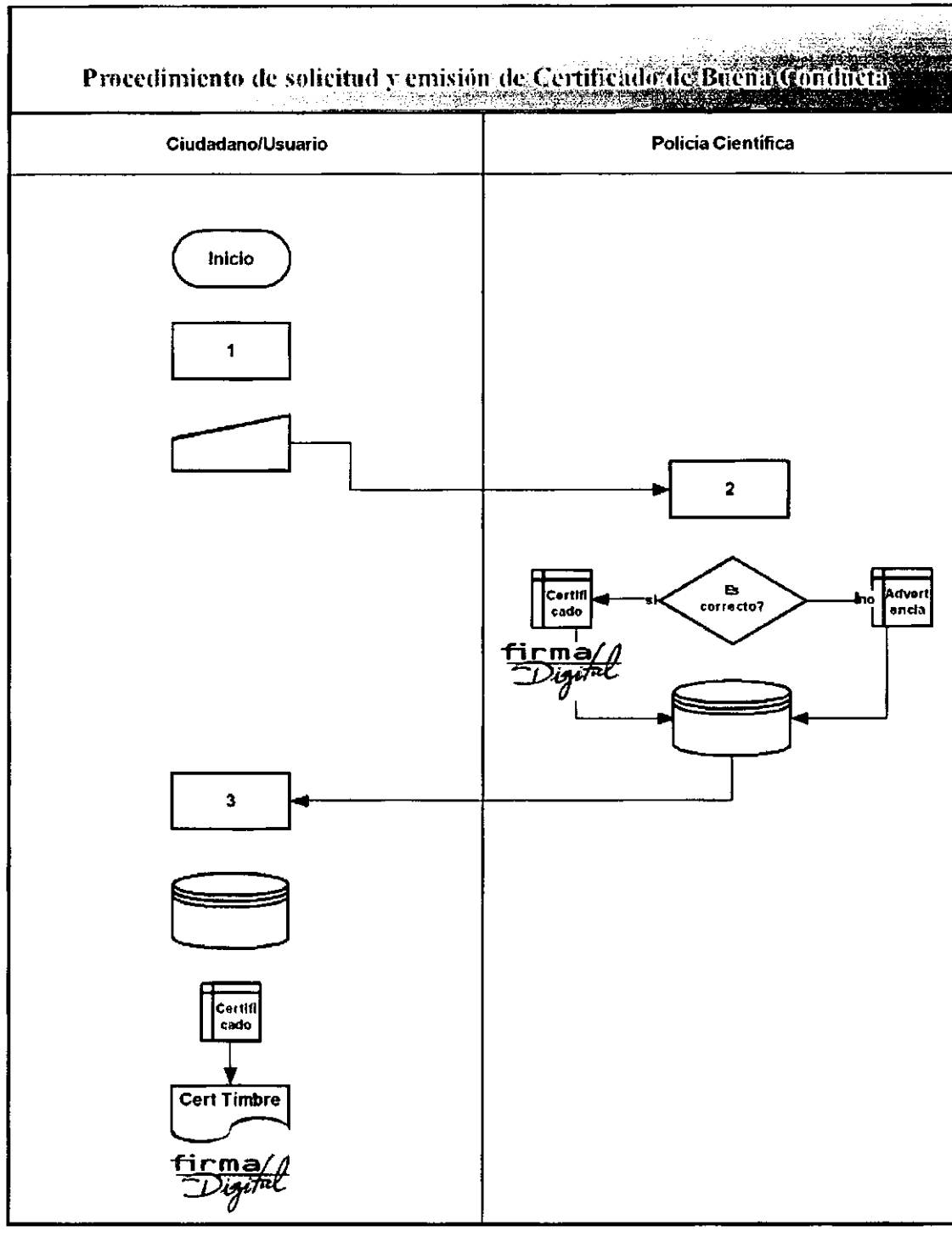


Diagrama del Procedimiento



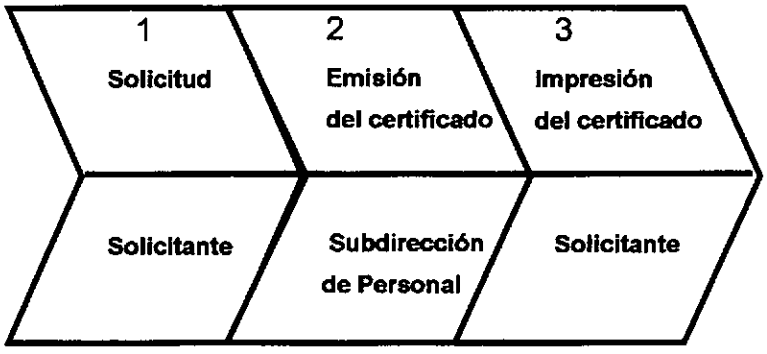
Procedimiento de solicitud y emisión de Certificado de Servicios y Remuneraciones

El presente procedimiento describe el conjunto de pasos a realizar por el personal de la Subdirección de Personal de la Gobernación y los Solicitantes que requieran Certificación de Servicios y Remuneraciones para tramitar su jubilación y/o pensión en el Anses.

Secuencia Sintética del Proceso

(Arrow chart)

Etapas



Principal sector interviniente

Objetivo:

A través de la redacción de este procedimiento se busca formalizar las tareas que lo conforman y fortalecer el diseño administrativo con la implementación de tecnología de firma y timbre digital en el mismo. Además, se busca asegurar garantías de autenticidad e integridad de las certificaciones entregadas.

Alcance:

Este procedimiento es de aplicación en la Gobernación de la Provincia de Mendoza y se aplica a las Certificación de Servicios y Remuneraciones para tramitar su jubilación y/o pensión en el Anses.

Definición de Roles

Responsables del Procedimiento:

- Subdirectora de Personal: Florencia Edit P. de Farias
- Subdirectora de Liquidaciones: Genoveva Chaves de Guardia

Subdirección de Personal

Dirección de Administración

Gobernación de la Provincia de Mendoza

Descripción del Procedimiento:

1. ***Solicitante:*** ingresa al Sitio Web de la Guía de Trámites, en e-trámite por Internet http://www.tramite.mendoza.gov.ar/ y elige la opción Cerificado de servicios y remuneraciones. A continuación, si cumple con los *requisitos establecidos, completa y envía un formulario de solicitud web con sus datos. A continuación toma nota del código único de identificación de su trámite y de la dirección del repositorio digital dónde estará sus certificado dentro de los siguientes 2 días hábiles.

2. ***Subdirección de Personal:*** recibe la solicitud web, ingresa al sistema de recursos humanos, emite a partir de la información allí almacenada las certificación de servicios y remuneraciones necesaria para tramitar una jubilación y/o pensión, la firma digitalmente y la deja disponible para su retiro en un repositorio digital

3. ***Solicitante:*** ingresa al repositorio digital con su código único de identificación, retira su certificación de servicios y remuneraciones y lo imprime con timbre digital. En este certificado se indica la oficina de Anses a la

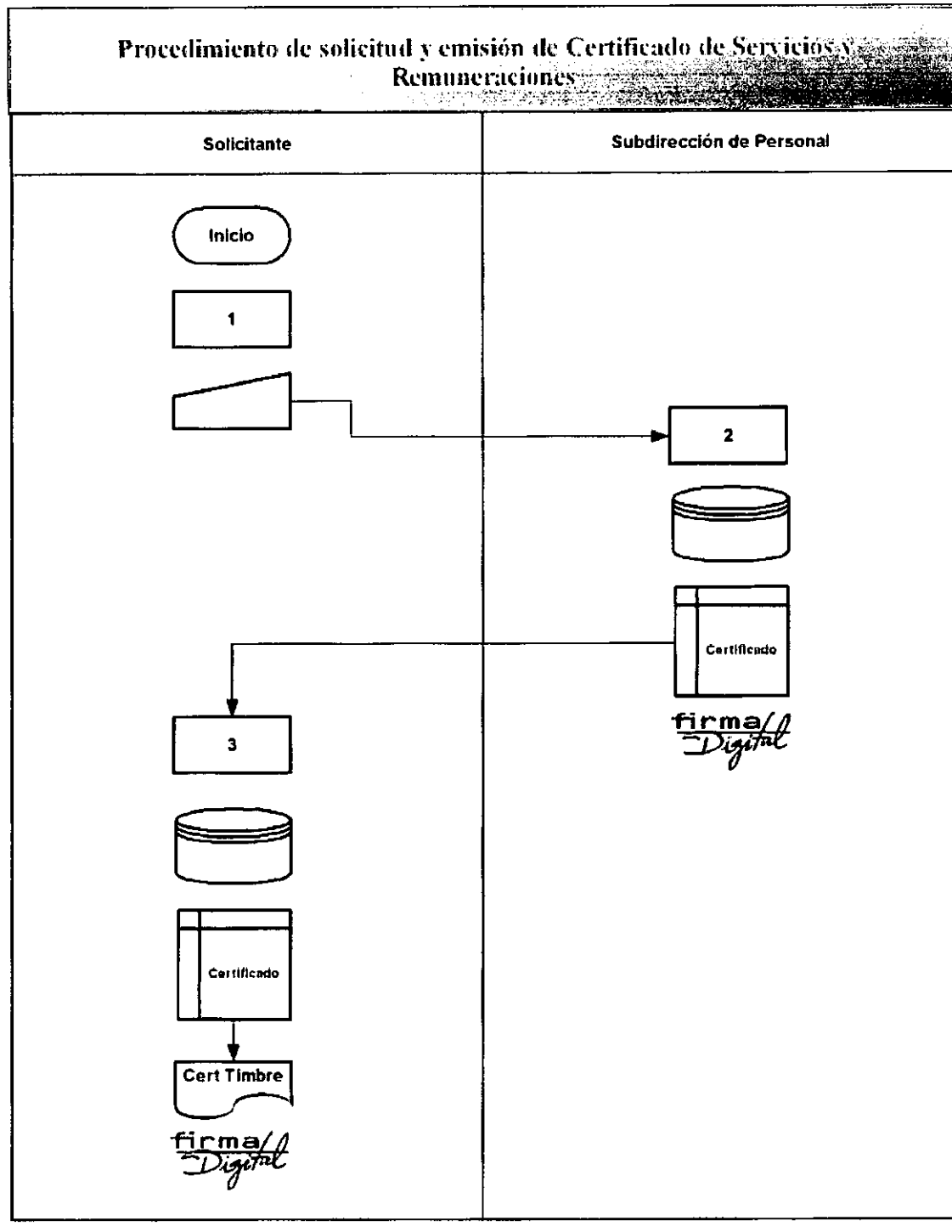
que debe dirigirse y las instrucciones pertinentes para validarlo a partir de su timbre digital.

Requisitos

Podrá pedir su Certificado de Servicios y Remuneraciones por este medio solo si:

1. Es empleado de la Gobernación de la Provincia de Mendoza
2. Es ex -empleado de la Gobernación de la Provincia de Mendoza
3. Es familiar de las figuras anteriores

Diagrama del Procedimiento



B) Consideraciones Especiales

La efectiva implementación de alguna de las alternativas anteriores estará sujeta a decisiones de carácter político que aún se están sopesando. En cuanto tales decisiones se tomen, la presente consultoría se encuentra en condiciones de empezar con la implementación sin demoras.

Los cambios u alteraciones de último momento que deriven de estas decisiones serán plasmados oportunamente en informes subsiguientes.

VI. Plan de Pruebas

Introducción

La calidad y confiabilidad de los sistemas de información, del software y la plataforma de hardware asociada constituyen en la actualidad un tema central que debe ser cuidadosamente abordado en todas las etapas del CVS (Ciclo de vida de sistemas), desde su diseño hasta la etapa de implementación y puesta a punto e incluso durante su mantenimiento. Garantizar la calidad y confiabilidad del sistema en base a herramientas metodológicas y estándares es aún un requisito mayormente crítico cuando hablamos de aplicaciones de firma digital que incluyen garantías de autoría e integridad de la información.

En este sentido es importante establecer qué entendemos por calidad y por confiabilidad.

Según la UNE 66-001-92 [AENOR, 1992], se define la calidad como la: *"Totalidad de características de un producto o servicio que le confieren su aptitud para satisfacer unas necesidades expresadas o implícitas"*.

La confiabilidad abordada desde la óptica de las aplicaciones de firma digital es la capacidad de asegurar a la comunidad de usuarios de un sistema que el mismo no solo cumple con los requerimientos y funcionalidades que se definieron, sino que lo hace bajo todas las garantías de seguridad e integridad pertinentes.

Múltiples son las condiciones a considerar durante el ciclo de vida de un sistema para garantizar calidad. Una cuidadosa metodología de relevamiento y definición de requerimientos, uno adecuado trabajo de documentación, la participación de los distintos perfiles de usuario durante todo el CVS, el uso de métricas de software y normas de calidad evaluadas por especialistas, el uso de estándares y normas de desarrollo permiten, entre otras cosas, que se consiga mejorar la calidad técnica de un producto. No obstante

esto, el diseño, planificación, ejecución y documentación de un Plan de Pruebas que acompañe las fases de diseño, desarrollo e implementación de un producto de software será el instrumento que nos permita ***verificar*** niveles de calidad y, en función de esto, generar confiabilidad en el producto.

Bajo estas premisas, concebimos un ***Plan de Pruebas*** como el conjunto de actividades planificadas y sistemáticas, necesarias para aportar la confianza en que el producto (SW) satisfará los requisitos dados de calidad y seguridad.

La ejecución de este conjunto de actividades se planifica en distintas fases durante todo el proceso mediante el cual se desarrolla el producto, dado que calidad y confiabilidad no sólo deben ser evaluadas sobre el producto terminado sino que son aspectos del diseño que debe incorporarse desde la génesis del mismo.

Hechas estas aclaraciones introductorias, documentamos a continuación el Plan de Pruebas que se ha diseñado para la experiencia de Timbre Digital.

Tipos de prueba a realizar

Se deberán realizar los siguientes tipos de prueba:

- ***Pruebas Unitarias:*** Se prueba cada uno de los componentes del sistema en forma individual para comprobar su correcto funcionamiento.

- ***Pruebas de Integración:*** Se prueba la integración entre los componentes del sistema para demostrar que las interfaces de vinculación operan correctamente.

- ***Pruebas de Usabilidad:*** Se prueba la accesibilidad y usabilidad del sistema por parte de los usuarios para evaluar su facilidad de uso y

la medida en que interfaz de usuario conduce al correcto uso del producto.

- ***Pruebas de sistemas:*** Se prueba el sistema globalmente.

En cada una de las fases de prueba, se realizarán pruebas tanto de caja blanca como de caja negra.

- Las pruebas del tipo ***caja blanca*** son aquellas que permiten examinar la estructura interna del programa

- Las pruebas del tipo ***caja negra***, son aquellas donde los casos de prueba se diseñan considerando exclusivamente las entradas y salidas del sistema, sin preocuparse por la estructura interna del mismo.

Fases de prueba

Se establecen las siguientes fases de prueba para las distintas etapas del CVS.

Fase de Investigación preliminar: esta fase prevé todas las pruebas a ser desarrolladas en la etapa de Investigación y Desarrollo Preliminar de la tecnología de timbre digital. La misma incluye todas las comprobaciones tendientes a determinar cuáles son las condiciones básicas a tener en cuenta en el diseño y desarrollo de la experiencia. Estas pruebas están vinculadas a aspectos de configuración del hardware, plataforma y lenguajes de desarrollo, compatibilidad y portabilidad de los mecanismos de timbrado y verificación, algoritmos de hash y firma aplicables, formatos de representación de datos, capacidad de almacenamiento de datos en los timbres, escalas de representación de las matri-

ces de punto, esquemas de manejo y control de errores y comprobaciones de redundancia de datos sobre los códigos de barra bidimensionales entre otras. Los resultados de estas pruebas deben conducir a un documento que describa detalladamente la plataforma de hardware y software a utilizar para el desarrollo de timbre digital, los estándares tecnológicos aplicables, las librerías criptográficas y de representación PDF417 más adecuadas y todo otro requisito que deba ser considerado como premisa básica de diseño y desarrollo.

Fase de diseño y desarrollo: esta fase prevé la realización de pruebas unitarias y de integración, tanto de caja blanca como de caja negra, que permitan verificar si el sistema cumple, tanto modularmente como en forma integrada, con las especificaciones funcionales, de compatibilidad, portabilidad, interoperabilidad y fundamentalmente de seguridad e integridad pertinentes. Se medirán aquí las respuestas del sistema ante casos de prueba con datos válidos e inválidos, se comprobará su funcionamiento con distintos Certificados y distintos paquetes de datos a timbrar, se realizarán comprobaciones sobre timbres válidos e inválidos, sobre timbres dañados y sobre variantes en la codificación PDF417. El resultado de estas comprobaciones y mediciones debe conducir a conclusiones certeras sobre los niveles de calidad y confiabilidad del desarrollo en términos de identificación de errores, tolerancia a fallos y vulnerabilidades.

Fase de implementación: esta fase acompaña la etapa de implementación y puesta a punto del sistema en su CVS y prevé pruebas de usabilidad y de sistemas, de caja negra, en el entorno de producción, que permitan verificar su correcta utilización por parte de los usuarios y la correcta respuesta del desarrollo ante situaciones de uso no previstas en las fases previas. En esta etapa se medirá también la calidad de la documentación, manuales de usuario, interfaces, etc. Como resulta-

do de esta etapa se deberán instrumentar las correcciones finales al sistema que se hayan identificado como necesarias para lograr la aceptación final de los organismos usuarios.

Objetivos

Fase de Investigación Preliminar:

- Documentar requerimientos técnicos sustanciales que deben ser incluidos en el desarrollo de timbre digital en términos de plataforma, lenguajes y librerías, algoritmos criptográficos, formatos de representación, codificación PDF417, niveles de corrección de errores y estándares.

Fase de Diseño y Desarrollo:

- Comprobar el correcto funcionamiento de los módulos de timbrado y verificación según los requerimientos técnicos y funcionales establecidos.
- Comprobar la correcta integración modular del sistema.
- Documentar condiciones de fallo del sistema y la plataforma de hardware asociada.
- Obtener conclusiones de calidad y confiabilidad del desarrollo.

Fase de Implementación y puesta a punto:

- Lograr la aceptación final del desarrollo por parte de los organismos usuarios.

Criterios de terminación

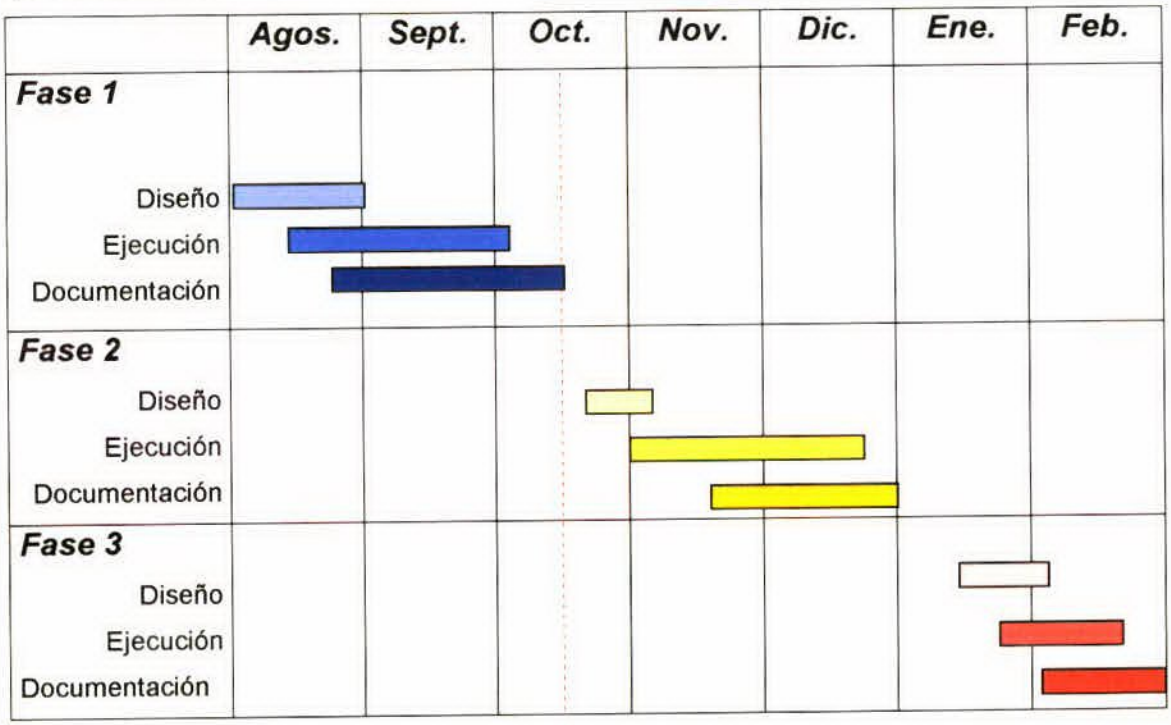
Entendiendo que un sistema podría ser sometido a pruebas indefinidamente y que los casos de prueba son potencialmente infinitos, es importante incluir en todo Plan de Pruebas un conjunto de criterios que permita determinar en que momento un conjunto de pruebas puede darse por terminado y las conclusiones obtenidas de su ejecución pueden considerarse seguras.

Atendiendo a esto para el presente plan se fijan los siguientes criterios de terminación:

1. Para cada fase de prueba, se diseñarán casos de prueba, cada uno de los cuáles contendrá un conjunto de datos de prueba que conducirán el desarrollo de las actividades de testing.
2. Para cada conjunto de datos de prueba se establecerán valores esperados a obtener producto de su ejecución. Las pruebas podrán darse por terminadas si a repetición de la prueba los resultados coinciden y se aproximan al valor esperado.
3. En caso de que los resultados de la prueba se alejen significativamente de los valores esperados se realizará un testing de caja blanca que permita identificar las causas del desvío y una vez realizadas las correcciones correspondientes se diseñará un nuevo conjunto de datos de prueba para el caso que se está testeando.
4. La fase de pruebas podrá darse por terminada cuando se haya obtenido la aceptación de los responsables para todos los casos de prueba.

Cronología

Se detalla a continuación el cronograma de tiempos para cada fase de pruebas. En este cronograma se contemplan los tiempos de diseño de los casos de prueba y conjuntos de datos de prueba, ejecución y documentación de resultados.



Responsables

Las pruebas comprendidas en las Fases 1 y 2 serán diagramadas, ejecutadas y documentadas por el equipo de Firma Digital. Las pruebas de aceptación contempladas en la Fase 3 serán diseñadas por el equipo de Firma Digital, realizadas por los usuarios del sistema y documentadas en conjunto.

Entorno de prueba

En condiciones ideales sería necesario disponer de un entorno de pruebas especial para desarrollar los casos de testing. Sin embargo, de acuerdo a la infraestructura tecnológica disponible se ha decidido utilizar como entorno de pruebas para la Fase 1 y 2 el entorno de desarrollo, compuesto por

Servidor:

Servidor Linux Red Hat 9.0

Servidor de Aplicaciones JBoss 3.0.1

WebServer Tomcat 4.1.2.

Plataforma de desarrollo J2EE (Open Source)

Librerías criptográficas JCE – BouncyCasttle (Open Source)

Librerías PDF417 – iText (Open Source)

Workstation:

Estación de trabajo con Windows XP

Plataforma de desarrollo J2EE

IDE J2EE – Jdeveloper

Certificados X.509 v.3.

Tokens de firma digital – Aladin eToken 16K

Impresoras:

Impresora chorro de tinta estándar

Impresora láser estándar

Scanner de Código de Barras:

Scanner de mano Metrologic MS44 con entrada por Keyboard y RS232

Software de configuración MetroSet v 1.0 – Metrologic.

La Fase 3 será desarrollada en el entorno de producción provisto por el organismo usuario.

Casos de Prueba

Se documenta a continuación el diseño a priori de casos de prueba que deberá guiar la ejecución y documentación de pruebas.

Dado que el proceso de pruebas es un proceso dinámico que convive y se adapta a los cambios producidos durante el CVS, los casos propuestos y la caracterización de los conjuntos de datos de prueba para cada caso no constituyen una enumeración taxativa y completa de todos los cursos de acción a comprobar sino que intentan aportar un plan guía para la ejecución de pruebas. Plan que se enriquecerá y adaptará posteriormente con las variantes que en tiempo de ejecución y documentación de pruebas se entienda oportuno realizar.

El diseño de casos de prueba se ha estructurado de acuerdo a las fases de realización establecidas, a fin de poder observar claramente la etapa del CVS en donde estas pruebas se insertan e identificar a que etapa del desarrollo retroalimentan.

Fase 1: Investigación preliminar

Durante esta fase se aplicará la estrategia de *Walkthrough* para la realización de los testings. Esta modalidad prevé inspecciones conducidas únicamente por miembros del grupo de desarrollo, durante las cuáles se siguen cursos de acción de caja blanca que permiten examinar una parte específica del desarrollo. En general, también se utilizan pruebas de caja negra tomando en cuenta los input/output del caso de prueba correspondiente.

En aquellos casos para los cuáles no se cuenta con métricas históricas o documentación previa que permita postular resultados esperados o aceptables, se indica la forma de documentar los resultados obtenidos del testing a fin de obtener luego conclusiones en función de los mismos.

Fase 2: Diseño y desarrollo

En esta etapa se proponen casos para la prueba modular del desarrollo de timbre digital y su integración. No se indican los resultados esperados porque estos dependerán en gran medida de los conjuntos de datos de prueba que se ejecuten en cada corrida de prueba. Para cada caso de prueba deberá diseñarse un conjunto de datos de prueba que se corresponda con la caracterización prescrita y deberán ejecutarse un mínimo de tres corridas de prueba por lote. La integración modular seguirá una estrategia top-down para la realización de pruebas.

Fase 3: Implementación y puesta a punto

Esta última fase de pruebas implica la aceptación final del producto por parte de los organismos usuarios a partir de un conjunto de pruebas de sistemas y de usabilidad. Para la misma se sugiere como mínimo la ejecución de los casos de prueba aquí descriptos sin perjuicio de que el Organismo usuario decida mejorar las pruebas tomando cursos de acción adicionales. Complementariamente a la ejecución y documentación de las corridas de prueba deberían realizarse evaluaciones independientes sobre el cumplimiento de estándares, planes de desarrollo, procedimientos de calidad y seguridad, etc.

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

A) Reuniones

Se realizaron reuniones con el equipo legal de la Gobernación con el objeto de aclarar los alcances del proyecto de firma digital, las tendencias nacionales y el estado actual de la materia. En éstas reuniones se pactó una dinámica de trabajo a seguir consistente en la elaboración de papers por parte del equipo de Firma Digital y una reunión mensual desde el inicio del presente proyecto para aclarar puntos de discusión relacionados a los contenidos, con el objeto de avanzar en la conciencia común y, concretamente en la selección conceptual de los temas a ser incluidos en la reglamentación de la Ley de adhesión provincial. Cabe señalar que en tanto la Legislación nacional no avance en la publicación y promulgación de los procedimientos de licenciamiento, nuestra tarea es en grande parte anticipar la temática relacionada sobre la cual versará la reglamentación provincial.

Sobre la base de los textos legales de la Ley nacional de Firma Digital 25506 y su Decreto Reglamentario con el cual ya hemos venido trabajando desde el proyecto pasado, la decisión conjunta del equipo de Firma Digital y del equipo legal de la Gobernación de la Provincia de Mendoza es la de prepararse en la temática relacionada para que, en cuanto la Nación defina los procesos de Licenciamiento, rápidamente pueda emitirse y promulgarse una reglamentación acorde de nuestra Ley provincial de Adhesión que ya cuente con los consensos necesarios.

Por lo antedicho, el equipo de Firma Digital, elaboró durante este proyecto con tales motivos, una serie de papers con los que se ha estado trabajando conjuntamente con las dependencias legales de la Gobernación, que se transcriben en el siguiente apartado.

B) Papers elaborados

La primera serie de papers elaborados fue de corte netamente tecnológico y con el objeto de aclarar los conocimientos del equipo legal sobre el funcionamiento, garantías y aplicaciones de la tecnología de Firma Digital.

De esta serie se presentaron los siguientes temas:

ENCRIPTACIÓN

CERTIFICADOS DE SEGURIDAD

SSL: SECURE SOCKETS LAYER

LA FIRMA DIGITAL

Luego, a expreso pedido del equipo legal de Gobernación, se realizaron una serie de papers de corte legal relacionados con la Legislación Española de Firma Digital, uno de los pilares en los que se ha reflejado la Legislación Nacional por ser una de las más avanzadas y ordenadas del mundo. El objetivo buscado al tratar dicha legislación ha sido poder anticipar la temática legal relacionada y entenderla a través de un andamiaje jurídico en funcionamiento y a las claras muy avanzado. Lo que además permite hacerse una idea acabada sobre la forma y tenor de los textos y artículos a incluir en nuestra reglamentación.

De esta serie se elaboraron los siguientes papers

sobre Legislación Española :

LA LEY 59/2003 DE FIRMA ELECTRÓNICA

LA FIRMA ELECTRÓNICA Y EL DOCUMENTO ELECTRÓNICO EN ESPAÑA

CONTENIDO Y ESTRUCTURA DE LA LEY DE FIRMA ELECTRÓNICA

CONCEPTO JURÍDICO DE FIRMA ELECTRÓNICA EN LA LFE

EFECTOS JURÍDICOS DE LA FIRMA ELECTRÓNICA

RESPONSABILIDAD DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

RÉGIMEN JURÍDICO DE LOS CERTIFICADOS

EL DNI ELECTRÓNICO

LA FIRMA ELECTRÓNICA DE LAS PERSONAS JURÍDICAS

Finalmente se entregaron dos informes, el primero versa sobre los últimos avances legislativos y acciones realizadas en materia de Reglamentación de Firma Digital a nivel nacional, y el segundo contiene la bibliografía utilizada para la elaboración de todos los papers que además permite ampliar la información de los temas que resulte necesario.

ENCRIPTACIÓN

La encriptación es el proceso de modificar una información de tal forma que sólo las personas autorizadas sean capaces de invertir el proceso y recuperar la información original, mientras que los usuarios no autorizados se encuentran con una secuencia ininteligible de la que es imposible extraer información. La criptografía o criptología es la rama de las matemáticas que se dedica a diseñar y estudiar sistemas de encriptación. El criptoanálisis es la disciplina que estudia los métodos para romper esos sistemas de encriptación sin el conocimiento de la clave.

Para conseguir pasar información de forma segura de un sitio a otro a través de cualquier medio, no solamente una red de ordenadores, se utilizan algoritmos de cifrado. En el caso de redes de ordenadores, donde se dispone de las herramientas para realizar complicados y costosos cálculos matemáticos, el cifrado de mensajes se puede llevar o extremos hasta la fecha imposibles. La criptología es una rama de las matemáticas que se encarga del estudio del cifrado de documentos. Los algoritmos de cifrado son la implementación práctica de estos estudios. La historia de la criptografía es una apasionante novela de intrigas, sobre todo en periodos de guerras o turbulencias políticas. El primer cifrado conocido históricamente es el cifrado del Cesar, usado por éste en las guerras de las Galias. Simplemente era un desplazamiento de las letras una determinada cantidad para alterar el mensaje original. En este caso, la clave de cifrado era el número de desplazamiento de las letras. Como regla general, un sistema de cifrado dispone de unas claves que sólo conocen las personas permitidas. Esas claves son transmitidas por un canal seguro (un fiel mensajero, un encuentro personal), y sirven para cifrar el mensaje a enviar, que viajará por un canal inseguro y, posteriormente, descifrarlo. Un buen sistema criptográfico se fundamenta por sí mismo, y la seguridad debe ser independiente de que el público conozca el algoritmo o método de cifrado. Si la seguridad del sistema se basa en el desconocimiento de éste, no se considera un buen método. La robustez del método depende, en buena medida, de la clave. Por ejemplo, en el cifrado de Cesar,

el espacio de claves es 27, que son las posibles letras del alfabeto. Bastará con ir probando una por una hasta descifrar el mensaje. Por tanto, el espacio de claves o, lo que es la mismo, la longitud debe ser grande, cuanto más mejor. La clave puede ser una frase, palabra o número. El problema de estos sistemas de cifrado, llamados de claves simétricas, es que los usuarios tienen que ponerse de acuerdo en qué clave utilizan para cifrar/descifrar.
Esa información, la clave, tiene que viajar por un canal seguro para que sólo esas dos personas la sepan y ahí surgen muchos inconvenientes del método. El método más famoso y usado de criptosistemas de clave simétrica es el DES (Data Encription Standard), durante muchos años sistema de criptografía oficial en los Estados Unidos.
Su algoritmo se basa en dividir el mensaje en bloques y realizar sustituciones y permutaciones. La clave tiene una longitud de 64 bits.
La solución de este problema de gestión de claves vino de las manos de Rivest, Shamir y Adelman y su método de cifrado de clave pública RSA. Es un método de claves asimétricas: se usa una clave para cifrar y otra para descifrar. La clave de cifrado es pública, cualquiera puede verla y, por tanto, enviar un mensaje cifrado a la persona en cuestión. La clave de descifrado sólo es conocida por el usuario. La seguridad del sistema no se ve afectada por el hecho de que se conozca una de las claves. Este sistema se basa en la dificultad de factorización de números primos. La longitud de la clave es de hasta 2.048 bits. Los criptosistemas de clave pública también permiten la firma digital de documentos, con el fin de garantizar la autenticidad del remitente. De lo contrario, alguien podría usurpar la personalidad electrónica de otro individuo y mandar mensajes en su nombre. Esto lo consigue encriptando una firma con la clave privada que, con la clave pública, sale a la luz. Sólo el verdadero autor puede encriptar un mensaje de tal modo que se lea con la clave pública.
La firma se genera mediante funciones de hash, que también garantizan la integridad (que nadie haya agregado nada o modificado el mensaje en modo alguno).

Existe un teorema que dice que un criptosistema es incondicionalmente seguro sí y sólo si la longitud de la clave es similar a la longitud del mensaje. Prácticamente es imposible de garantizar esa premisa para todo mensaje. La tarea de la criptografía es hacer que descifrar el mensaje sin la clave sea tan lento y tan caro que, cuando lo consigan, haya perdido todo su valor.
Habitualmente se utilizan tres tipos básicos de algoritmos de cifrado cuando se trabaja con ordenadores y redes.

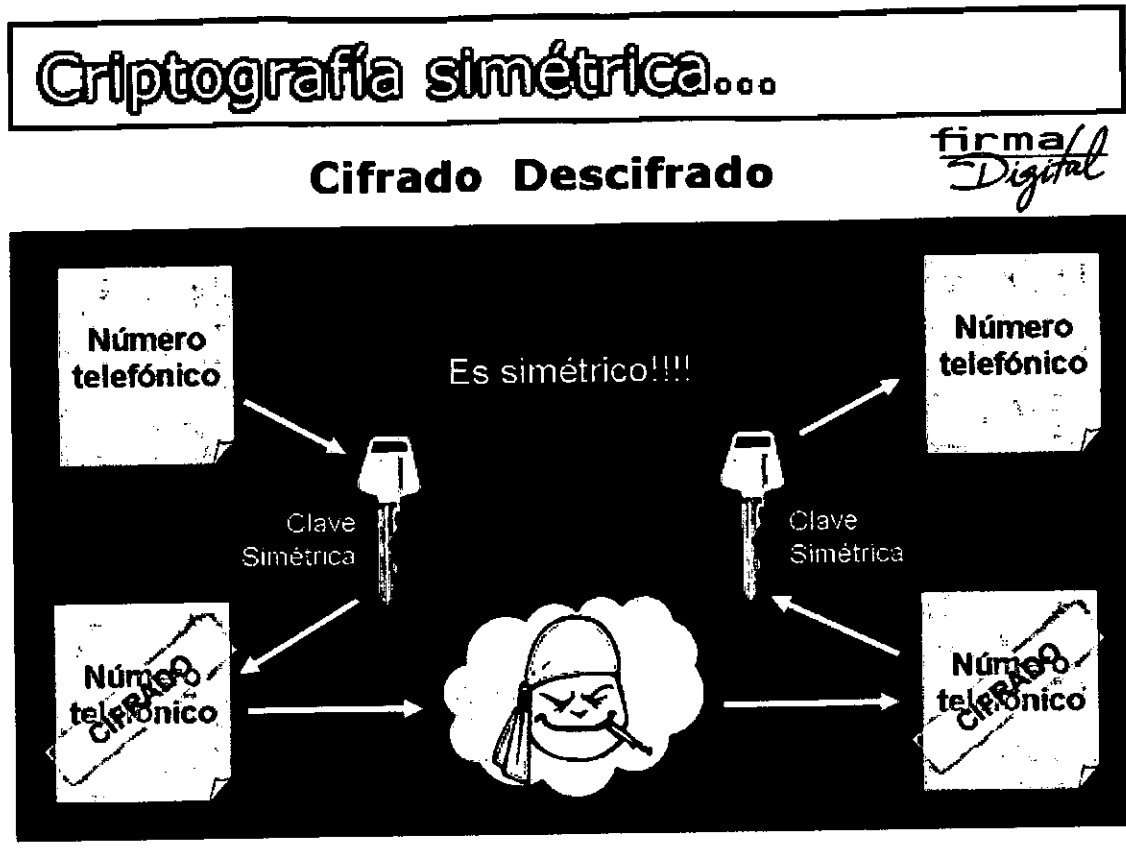
- ALGORITMOS HASH

Son algoritmos de una sola dirección. Al aplicar uno de estos algoritmos sobre un mensaje a codificar este se convierte en otro codificado. Estos algoritmos tienen dos propiedades fundamentales: la primera es que a partir del mensaje codificado no es posible obtener el mensaje original. La segunda es que cada mensaje original es codificado de manera distinta, o en otras palabras, que mensajes originales distintos deben dar mensajes codificados distintos.
Pero para qué pueden servir estos algoritmos si no es posible la reconstrucción del mensaje original. Existen varias aplicaciones para este tipo de algoritmos. La más conocida es para el cifrado de contraseñas de usuario en ordenadores. Cuando un usuario introduce por primera vez su contraseña en un ordenador, ésta es cifrada mediante un algoritmo hash y se almacena en esta forma. Cuando el usuario se vuelve a introducir en el sistema, nuevamente se codifica su contraseña de acceso con el mismo algoritmo hash y se comprueba si la clave cifrada coincide con la almacenada. La ventaja de hacerlo así es que si el fichero donde se almacenan las contraseñas de los usuarios cae en malas manos lo que se ve es un mensaje cifrado a partir del cual es imposible obtener el mensaje original.
Otra posible aplicación de algoritmos hash es para la verificación de firmas Digitales, como trataremos más adelante.
La ventaja de los algoritmos hash frente a otros tipos de codificación es su

rapidez, asociada a su vez a su bajo coste computacional. Es decir, los cálculos necesarios para cifrar el mensaje no son costosos y una computadora puede hacerlos con poco consumo de tiempo y memoria. Su principal desventaja es que es posible romperlos mediante ataques de fuerza bruta. Este tipo de ataques consiste en probar combinaciones de posibles originales mensajes hasta dar con aquel que da el mensaje codificado. Protecciones contra este tipo de ataque son que el mensaje original sea suficientemente largo (más de una palabra), que el mensaje no tenga sentido en ningún idioma conocido y que incorpore signos de puntuación, letras mayúsculas, minúsculas y números.
Ejemplos de este tipo de algoritmos son MD5 ó SHA.

- ALGORITMOS DE CLAVE SIMÉTRICA.

Este tipo de algoritmos se basan en una función matemática que mediante una clave es capaz de cifrar y descifrar un mensaje dado. Son algoritmos utilizados para pasar información entre dos fuentes en las que ambos conocen la contraseña de cifrado y descifrado.



Esquema de cifrado descifrado simétrico

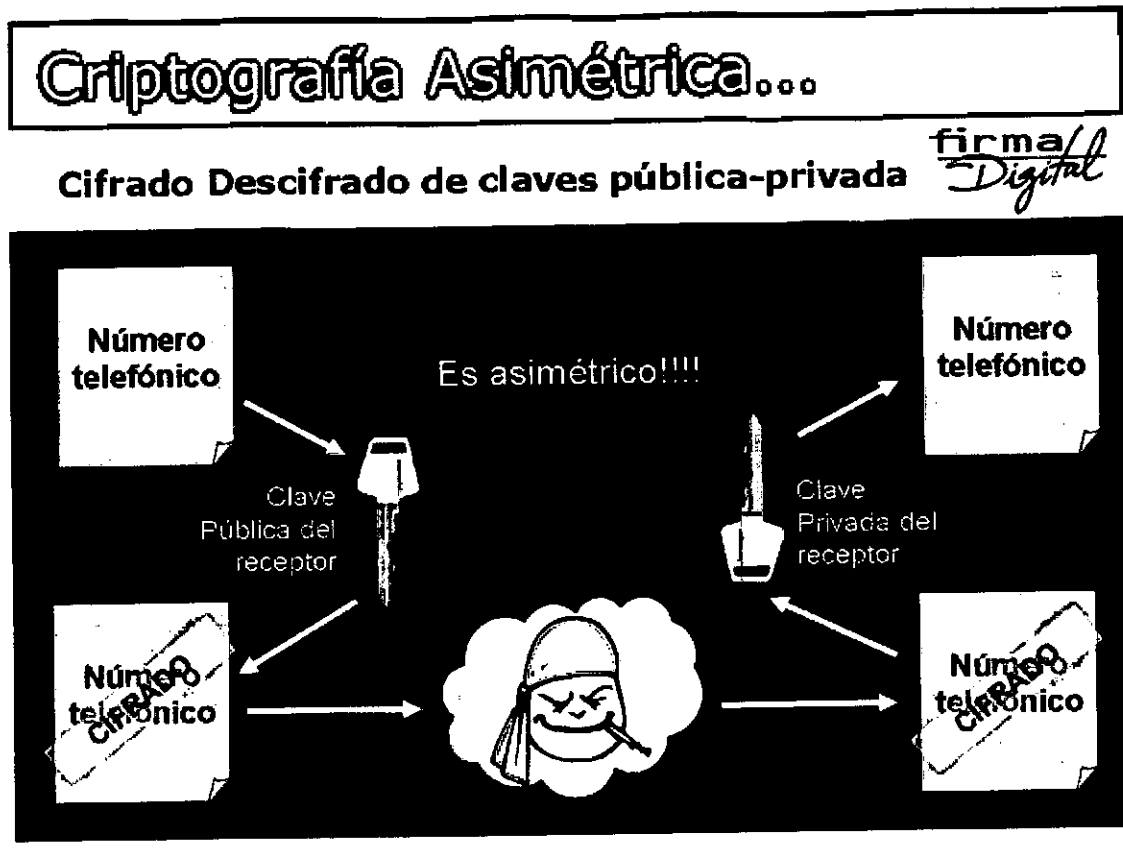
Su mayor desventaja reside en el hecho de que para poder realizar la transmisión segura los participantes en la misma deben conocer la clave secreta. Para ello debe de disponerse de alguna forma de transmitir dicha clave de forma segura. En ocasiones, como en las transmisiones SSL, lo que se hace es utilizar un algoritmo de clave asimétrica (ver más adelante) para pasar la clave secreta y después utilizar estos algoritmos para el resto de la comunicación. La ventaja de estos algoritmos frente a los algoritmos de llave asimétrica es que éstos requieren de un menor gasto de CPU. Por el contrario los algoritmos de clave asimétrica son, en conjunto, más seguros.
Ejemplos de este tipo de algoritmos son DES (Data Encription Standard), Triple DES, RC2, RC5 ó IDEA.

- ALGORITMOS DE CLAVE ASIMÉTRICA.

Este tipo de algoritmos son la base de la llamada criptografía de doble llave, o de llave pública. La idea de estos algoritmos es utilizar dos claves en vez

de una para cifrar y descifrar los mensajes. Las llaves funcionan de manera que lo que cifra una de las claves solamente puede ser descifrado por la otra y viceversa. Además, conociendo una de ellas no es posible averiguar la otra. De esta forma lo que se hace es tomar una de las dos claves y almacenarla como privada. La otra clave se toma como pública y se distribuye. Una de las aplicaciones de estos algoritmos es para mandar mensajes cifrados de un sitio a otro. Supongamos que A quiere hacer llegar un mensaje a B. A conoce la llave pública de B, así que la utiliza para cifrar el mensaje que quiere hacerle llegar. Una vez cifrado el mensaje sólo B puede leer su contenido puesto que es el único que tiene la llave capaz de descifrarlo. Otra de las aplicaciones bien conocidas de los algoritmos de clave asimétrica son las firmas electrónicas. Si A cifra un mensaje con su llave privada este solamente podrá ser descifrado con su llave pública. Esta es la garantía de que el mensaje ha sido enviado por A dado que sólo A está en posesión de su llave privada. En la práctica en la firma digital se utilizan más algoritmos, como trataremos más adelante. Otra de las propiedades interesantes de este tipo de algoritmos es que si en el transcurso del transporte del mensaje éste es modificado lo más mínimo es posible detectar esta modificación al realizar el descifrado. Esto asegura que el mensaje transmitido, si es descifrado correctamente, no ha sufrido alteración alguna durante su transporte.

La ventaja de este tipo de algoritmos es su probada robustez, sobre todo es sus versiones largas de 128 bits o más (las versiones de 56 bits o menos fueron rotas hace ya algún tiempo por métodos de fuerza bruta utilizando redes de ordenadores convencionales). La desventaja principal es que son computacionalmente costosos debido a las complejas operaciones matemáticas en las que se basan.



Esquema de cifrado descifrado asimétrico

El más conocido y utilizado de este tipo de algoritmos es el RSA, siglas que corresponden a los nombres de sus creadores Rivest, Shamir y Adelman.

CERTIFICADOS DE SEGURIDAD

Visto que se dispone de las herramientas, habrá que integrarlas en la informática para obtener esa privacidad e intimidad. Se entiende por Certificado "la certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad".

CERTIFICADOS DIGITALES

Concepto

firma Digital

Es un documento que simplemente dice: "Oficialmente certifico la correspondencia entre este usuario y ésta clave pública"

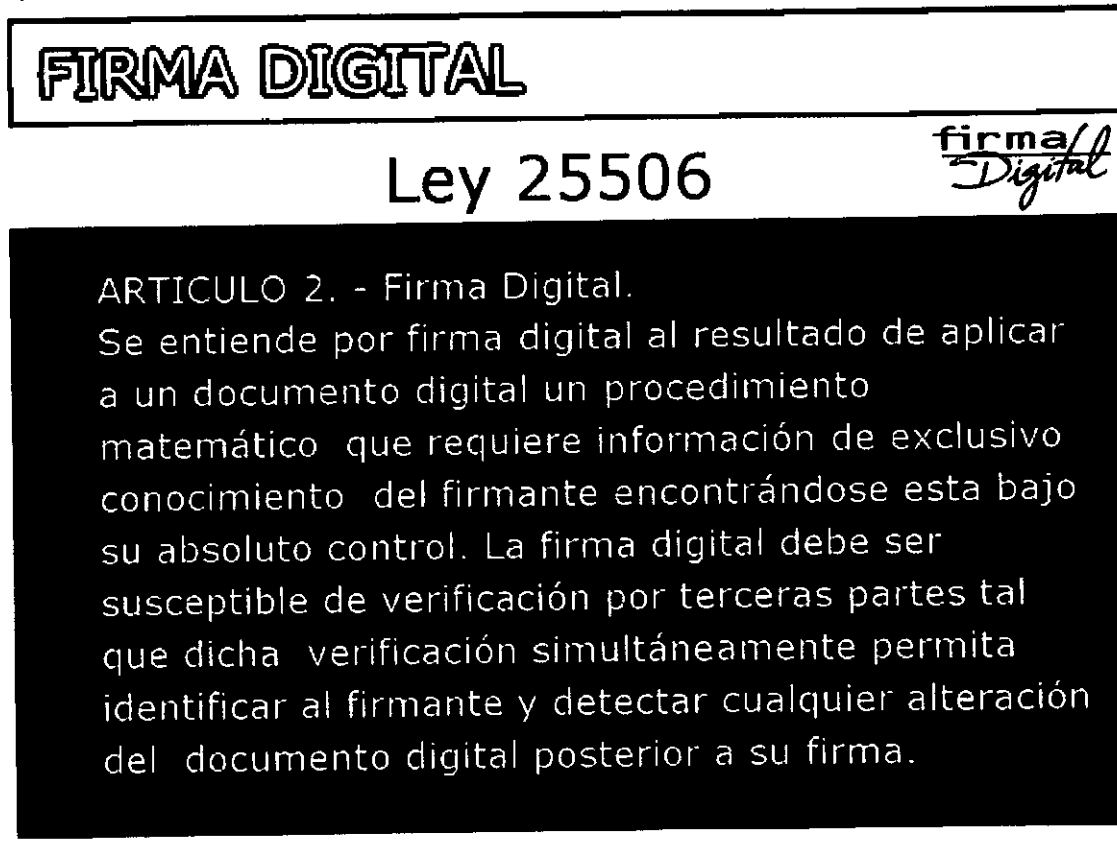
- Contiene los datos del usuario
- Contiene una copia de su clave pública
- Está firmado por la Autoridad Certificante de Confianza

Certificado Reconocido "es el certificado que contiene la información descrita anteriormente y es expedido por un prestador de servicios de certificación que cumple los requisitos legales de la Ley 25.506. Con esta distinción se quiere diferenciar los certificados genéricos de aquellos que son oficiales o capaces para ser utilizados en cualquier transacción de comercio electrónico.

En principio, hay dos aplicaciones en la que es muy interesante tener sistemas digitales de cifrado: el navegador y el lector de correo. El navegador las precisa para poder realizar transacciones seguras con éste, y el lector de correo para proteger la correspondencia electrónica. Pero para conseguirlo hay que tener en cuenta dos particularidades: que los programas soporten esa encriptación, y que todos los usuarios empleen los mismos métodos de encriptación. Por un lado, los navegadores ya soportan desde sus versiones 3.0 algoritmos de encriptación. Para ello basan todas las operaciones en certificados digitales. Estos certificados son parejas de claves públicas y privadas generadas por una empresa u organización autorizada. Estas empre-

sas, autorizadas por los gobiernos, dan certificados únicos y válidos para cada usuario, aseguran que funciona de forma correcta y dan herramientas para verificar su integridad. Establecen periodos de validez del certificado (por motivos de seguridad) y hacen pública la clave pública de cada usuario para que con ésta se le puedan enviar mensajes encriptados. Hay que advertir que, aunque un usuario tenga un certificado, no sirve de nada si el resto del mundo no conoce su clave pública.

Los certificados digitales tienen mucha más aplicación en correo electrónico que en navegación. En correo electrónico se pueden encriptar mensajes, firmar, estampar la fecha y hora y asegurar su integridad. Navegando, el certificado digital de cada usuario sólo sirve para autenticar su identidad. En el caso de que se realice una conexión segura con otro ordenador (cifrada), será éste el que tenga el certificado, el cual tendrá que aceptar el ordenador que se conecte.



La firma digital tiene soporte legal en Argentina desde el 2001, y tiene la misma validez que la firma convencional.

Se tiene que advertir que en Estados Unidos y Canadá califican los sistemas de criptografía como inherentes a la seguridad nacional, y está prohibida su exportación con pena de cárcel. Por eso, las versiones internacionales de los navegadores y demás programas tienen módulos criptográficos más débiles que los americanos. No obstante, se puede conseguir módulos específicos de mayor seguridad, realizados por empresas no norteamericanas.

Una vez definido el concepto de certificado digital se plantea una duda: ¿cómo confiar si un determinado certificado es válido o si está falsificado? La validez de un certificado es la confianza en que la clave pública contenida en el certificado pertenece al usuario indicado en el certificado. La validez del certificado en un entorno de clave pública es esencial ya que se debe conocer si se puede confiar o no en que el destinatario de un mensaje será o no realmente el que esperamos. La manera en que se puede confiar en el certificado de un usuario con el que nunca hemos tenido ninguna relación previa es mediante la confianza en terceras partes.

La idea consiste en que dos usuarios puedan confiar directamente entre sí, si ambos tienen relación con una tercera parte ya que ésta puede dar fe de la fiabilidad de los dos.

La necesidad de una Tercera Parte Confiable (TPC o TTP, Trusted Third Party) es fundamental en cualquier entorno de clave pública de tamaño considerable debido a que es impensable que los usuarios hayan tenido relaciones previas antes de intercambiar información cifrada o firmada. Además, la mejor forma de permitir la distribución de las claves públicas (o certificados digitales) de los distintos usuarios es que algún agente en quien todos los usuarios confíen se encargue de su publicación en algún repositorio al que todos los usuarios tengan acceso.

En conclusión, se podrá tener confianza en el certificado digital de un usuario al que con anterioridad no conocemos si dicho certificado está avalado por una tercera parte en la que sí confiamos. La forma en que esa tercera parte avalará que el certificado es de fiar es mediante su firma digital sobre el certificado. Por tanto, podremos confiar en cualquier certificado digital fir-

mado por una tercera parte en la que confiamos. La TPC que se encarga de la firma digital de los certificados de los usuarios de un entorno de clave pública se conoce con el nombre de Autoridad de Certificación (AC).
Entidades que ofrecen certificados digitales son, en el mundo, Verisign (http://www.verisign.com), que ofrece versiones de prueba, es una excelente empresa con muchos años de experiencia. Otra es British Telecommunications (http://www.trustwise.com). Una muy buena es Thawte (http://www.thawte.com), que da certificados personales gratuitos de un año de validez. GlobalSign (http://www.globalsign.net) es un consorcio europeo para ofrecer certificados digitales.
En Argentina está la Oficina Nacional de Tecnologías de Información (ONTI) (https://ca.pki.gov.ar) , que se encarga de estos asuntos. Estos certificados aún no son plenamente válidos para la presentación telemática de documentos, ya que aún no existen los procedimientos para ser reconocidos por las Administraciones Públicas.
El proceso para obtener un certificado digital, por lo general, es el siguiente: Hay que conectarse a la página Web de la empresa certificadora y solicitarlo. Tras su solicitud e instalación, normalmente inmediata, el certificado será válido para el navegador con el que se acceda a la página, y para su lector de correo. Si se usa Eudora como lector de correo, hay que seguir un proceso diferente: en Europa no se puede usar los módulos criptográficos de Eudora, ya que éste es un producto americano.

SSL: SECURE SOCKETS LAYER

SSL (Secure Sockets Layer) fue diseñado y propuesto en 1994 por Netscape Communications Corporation junto con su primera versión del Navigator. Sin embargo, no fue hasta su tercera versión, conocida como SSL v3.0 que alcanzó su madurez, superando los problemas de seguridad y limitaciones de sus predecesores. En su estado actual, proporciona cifrado de datos, autenticación de servidores, integridad de mensajes y, opcionalmente, autenticación de cliente para conexiones TCP/IP.
SSL v3.0 goza de gran popularidad, por lo que se encuentra ampliamente

extendido en Internet. Viene soportado por los dos principales navegadores del mercado, Netscape Navigator 3.0 ó superior, así como por Internet Explorer 3.0 ó superior.

No se necesita realizar ninguna acción especial para invocar el protocolo SSL, basta con seguir un enlace o abrir una página cuya dirección empieza por https://. El navegador se encarga del resto. Eso sí, hay que asegurarse que tiene SSL habilitado en su navegador. El rasgo que distingue a SSL de otros protocolos para comunicaciones seguras es que se ubica en la pila OSI entre los niveles de transporte (TCP/IP) y de aplicación (donde se encuentran los conocidos protocolos HTTP para Web, FTP para transferencia de ficheros, SMTP para correo electrónico, Telnet para conexión a máquinas remotas, etc.). Gracias a esta característica, SSL resulta muy flexible, ya que puede servir para asegurar potencialmente otros servicios, además, de HTTP para Web, sin más que hacer pequeñas modificaciones en el programa que utilice el protocolo de transporte de datos TCP.

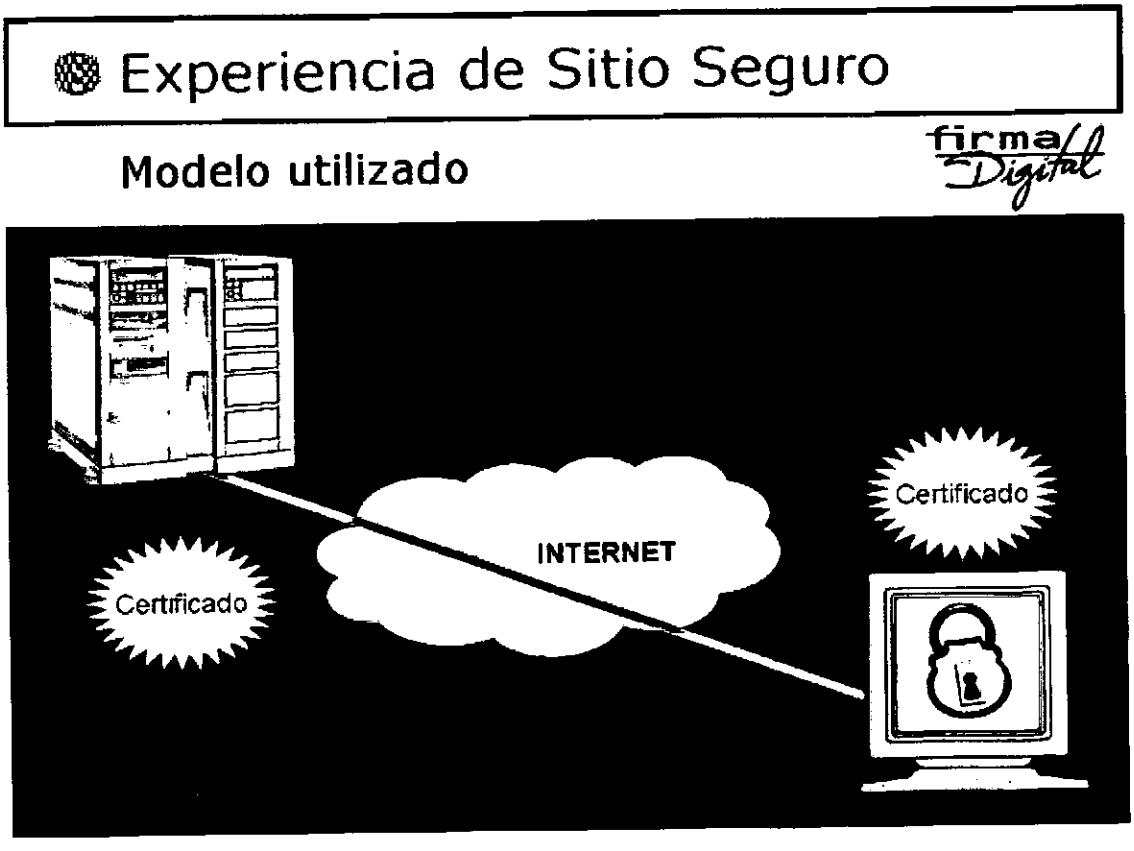
SSL proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico, que puede elegirse entre DES, triple-DES, RC2, RC4 ó IDEA, y cifrando la clave de sesión de los algoritmos anteriores mediante un algoritmo de cifrado de clave pública, típicamente el RSA. La clave de sesión es la que se utiliza para cifrar los datos que vienen y van al servidor seguro. Se genera una clave de sesión distinta para cada transacción, lo cual permite que aunque sea reventada por un atacante en una transacción dada, no sirva para descifrar futuras transacciones. MD5 ó SHA se pueden usar como algoritmos de resumen digital (hash). Esta posibilidad de elegir entre tan amplia variedad de algoritmos dota a SSL de una gran flexibilidad criptográfica.

Las fases de dicho protocolo son:

- Primera fase donde se acuerdan los algoritmos de cifrado. El navegador indica al servidor de qué algoritmos dispone, y normalmente se usa el más fuerte que ambos dispongan.

- Segunda fase de autenticación en la cual el servidor envía un certificado x.509v3 con su clave pública y solicita, si la aplicación lo requiere así, el certificado x.509v3 del cliente.
- Tercera fase de creación de clave de sesión, donde el cliente envía una clave maestra a partir de la cual se cifrarán los datos de la sesión en curso utilizando el algoritmo acordado en la primera fase. El navegador envía dicha clave cifrada usando la clave pública del servidor y el algoritmo RSA.
- Cuarta y última fase de verificación, donde se valida la autenticidad de ambas partes y que el canal está correctamente configurado.

Es este el modelo utilizado por equipo de Firma Digital de la Unidad de Reforma y Modernización del Estado en la Guía de Trámites de la Provincia de Mendoza.



Hoy por hoy SSL es el protocolo que mayor implantación tiene en las Web que ofrecen servicios de comercio electrónico, seguramente por su sencillez

de instalación por parte del comerciante y de uso por parte del cliente, puesto que casi todos los navegadores lo tienen implementado por defecto. Además, protege de manera bastante fiable los datos del cliente, con lo cual éste pierde el miedo a introducirlos y enviarlos a través de Internet.
Sin embargo, SSL carece de algunas características deseables en un protocolo para realizar compras en Internet, al tratarse tan sólo de un protocolo que cifra el canal de comunicaciones. Algunas de estas desventajas son:

- No permite verificar la validez de números de tarjetas de crédito, ni autorizar la transacción entre el banco del cliente y el banco del comerciante SSL sólo asegura que los datos llegarán correcta y confidencialmente desde el cliente al servidor, pero una vez allí nadie nos garantiza qué ocurrirá con ellos. Un ataque a la máquina del servidor puede hacerse con los datos del cliente una vez estén estos allí.
- Una forma de ataque a algunos servidores consiste en ir probando aleatoriamente números de tarjetas de crédito. El servidor informará cuando el número de tarjeta es válido o no, de manera que el programa atacante puede hacerse con una valiosa lista de números de tarjeta válidos.

A menudo se considera SSL erróneamente como un medio de pago y no lo es. SSL sólo es un protocolo estándar que define y da una forma para establecer una conexión segura entre dos ordenadores, nada más. El uso masivo de SSL como medio para garantizar la integridad y autenticidad de los datos en las transacciones que se llevan a cabo en muchos sitios Web de comercio electrónico conduce a esta visión incorrecta de este protocolo como un medio de pago en sí.

LA FIRMA DIGITAL.

Como vimos, según el artículo 2 de la Ley 25506/2001 "Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante encontrándose esta bajo su absoluto control. La firma digital debe ser

susceptible de verificación por terceras partes tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma".

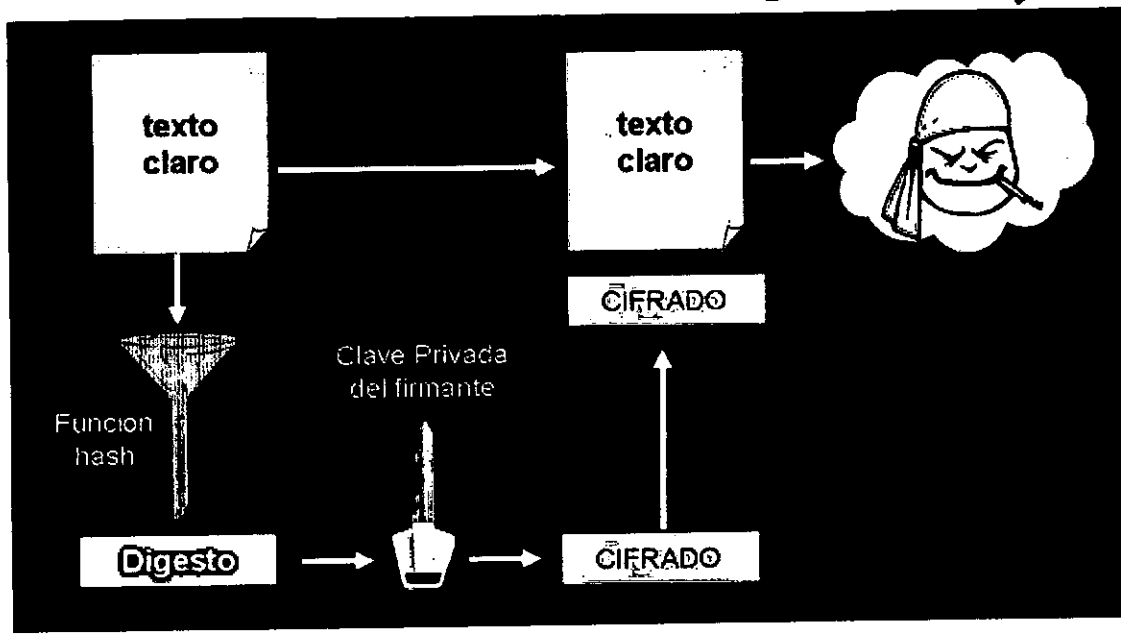
La Firma Digital se basa en criptografía de doble llave, también llamada de clave asimétrica o de llave pública. La idea inicial proviene de un artículo de Diffie y Hellman de 1976 donde por primera vez se expone la idea de codificar y decodificar un documento mediante el uso de dos llaves, una pública y una privada. Todo aquello que esté codificado mediante la llave pública solamente podrá ser decodificado por el propietario de la clave privada. Recíprocamente, aquello que sea codificado mediante la llave privada sólo podrá ser decodificado mediante la llave pública.

Visto desde el punto de vista que si algo puede ser decodificado mediante una llave pública implica necesariamente que sólo pudo haber sido codificado mediante el uso de su llave privada asociada, la firma digital sólo pudo estamparla aquel que posee la llave privada.

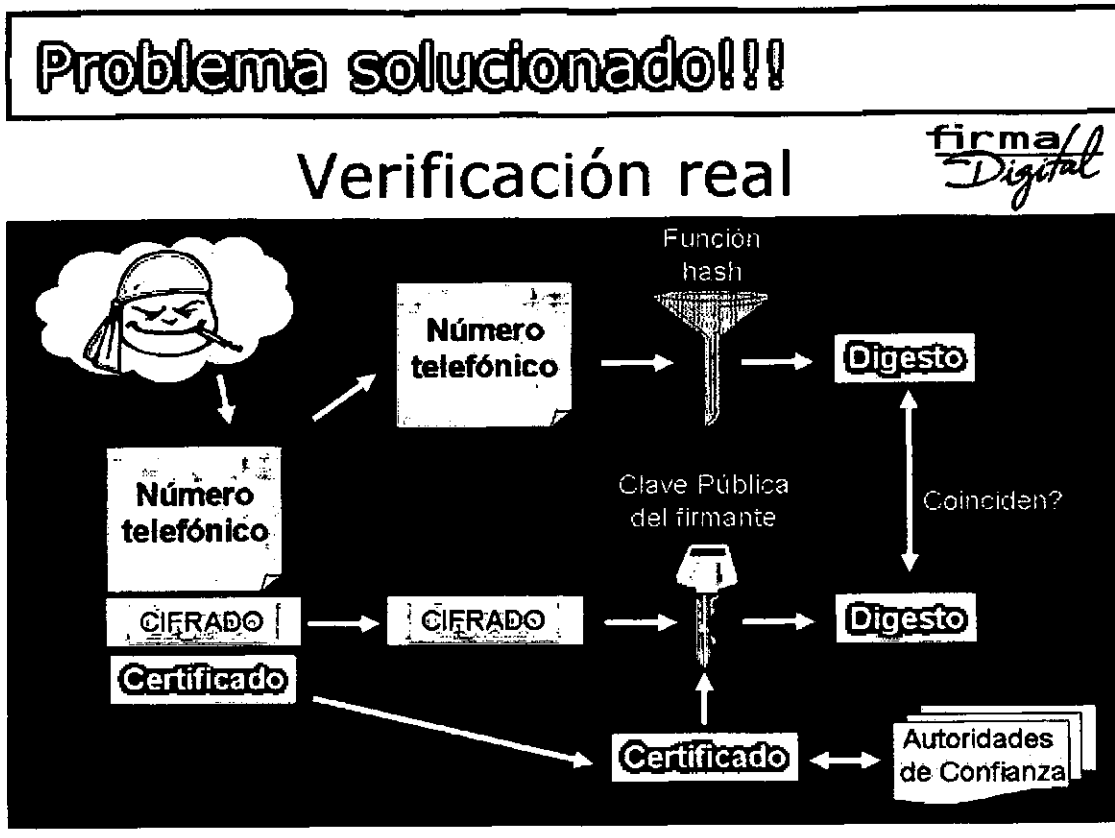
La criptografía de llave pública no aporta solamente autenticidad, también aporta integridad al documento firmado puesto que cualquier modificación en el mismo será automáticamente detectado por el algoritmo decodificador. De esta manera, cuando un documento nos llegue cifrado utilizando este tipo de algoritmo de llave pública podemos tener la seguridad casi absoluta de que el que lo manda es quien dice ser, y de que no ha sufrido alteraciones por el camino.

FIRMA DIGITAL

Creación de una firma digital



Para poder estar seguros de que una llave pública pertenece a una determinada persona y no a un suplantador, como ya mencionamos, existen la Agencias Certificadores que expiden los Certificados, consistentes en la información acerca del titular, su llave pública y la agencia certificadora que lo emitió. El estándar utilizado para certificados es el X.509.v3.



Las agencias certificadoras deben de ofrecer al público los listados de los usuarios reconocidos por ellas y sus claves públicas. Asimismo, también deben de ofrecer un listado de revocación de certificados (CRL, el acrónimo en inglés), donde se muestran las llaves públicas suspendidas por cualquier motivo. Actualmente la firma digital se basa en la llamada Infraestructura de Clave Pública, más conocida por su acrónimo inglés PKI (Public Key Infrastructure).

Podemos entender por esta infraestructura todos los elementos necesarios (algoritmos, agencias certificadoras, etc.), para poder llevar a cabo un sistema seguro de firmas digitales. El mayor problema de implementar la firma electrónica mediante algoritmos de llave pública es que estos algoritmos son hoy en día todavía bastante lentos y codificar un documento completo lleva demasiado tiempo. La solución por la que se opta en la mayoría de los casos es codificar solamente un resumen del documento y enviarlo junto a éste como prueba de autenticidad. Para generar el resumen de manera automáti-

ca se utilizan funciones unidireccionales hash que permiten al receptor del documento a su vez comprobar que el documento recibido no ha sido alterado.

En resumen los pasos, como se ve en las figuras, para el envío de un documento serían:

- El emisor escribe un documento
- Se crea un resumen del documento mediante una función unidireccional hash, y se cifra el resumen usando la llave privada del emisor. Acto seguido se envía al receptor.
- El receptor recibe el documento y un resumen del mismo cifrado. Con la llave pública el emisor el receptor descifra el resumen.
- El receptor utiliza la misma función hash que el emisor para crear el resumen del documento y compara el resultado con el resumen descifrado. Si son iguales, el documento es correcto.

Los certificados se pueden revocar, si el usuario así lo desea o precisa. Revocar un certificado es anular su validez antes de la fecha de caducidad que consta en el mismo. La revocación puede ser solicitada en cualquier momento, y en especial, cuando el titular crea que sus claves privadas son conocidas por otros. La revocación tiene efectos a partir de la fecha efectiva de revocación que consta junto al número de serie del certificado revocado en un documento firmado y publicado por la Autoridad de Certificación. Cualquier firma digital realizada con la clave privada asociada a ese certificado con posterioridad a la fecha efectiva de revocación no tendrá validez.

LA LEY 59/2003 DE FIRMA ELECTRÓNICA

Introducción

Con el desarrollo de Internet y el resto de redes de telecomunicaciones cuando, tanto técnica como jurídicamente, se ha planteado la conveniencia y la necesidad de que el documento electrónico vaya acompañado de una firma para poder realizar válidamente determinados actos jurídicos, tales como presentar la declaración de impuestos o emitir un documento electrónico con función de giro. Incluso en aquellos supuestos donde la firma no es un requisito de validez para el concreto acto o negocio jurídico, ésta puede ser un medio de prueba útil para demostrar la existencia del consentimiento y la voluntad de adhesión de los sujetos respecto del contenido de documentos electrónicos.

Evidentemente el documento electrónico enviado a través de redes de comunicación no admite la tradicional firma autógrafa. Pero la técnica permite también a través del medio electrónico crear y utilizar determinados signos o combinaciones de signos que añadidos al documento electrónico pueden cumplir la función de la firma autógrafa, y ese es el cometido de la firma electrónica.

Por tanto, la firma electrónica será necesaria en aquellos actos y negocios jurídicos

realizados a través de documentos electrónicos y que requieren de firma para su validez, pero no en el resto de actos, donde ésta también será útil como un elemento de prueba.

Además, las transacciones y operaciones comerciales, tales como la conclusión de contratos o el pago con tarjeta (de crédito, débito o monedero), así como las relaciones Administración Pública-Administrador realizas online a través de documentos electrónicos o telemáticos exigen, al menos, el cum-

plimiento de una serie de garantías y unos requisitos mínimos de seguridad en los siguientes aspectos:

Confidencialidad, en el sentido de que ningún tercero pueda acceder a la información enviada.

Integridad, para evitar que un tercero pueda modificar la información enviada sin que lo advierta el destinatario.

Autenticación, lo que permite asegura que la persona que envía un mensaje es realmente quien dice ser.

A estas condiciones se añade una cuarta, que popularmente se conoce en el sector como "no repudio o irrefutabilidad del contenido del mensaje", que permite a ambas partes de la comunicación probar fehacientemente que la otra parte ha participado en la comunicación, impidiendo tanto el repudio de origen (cuando el remitente del documento niega haberlo enviado) como el repudio de destino (cuando el destinatario niega haberlo recibido).

Ahora bien, determinados tipos de firma electrónica, como la firma digital, pueden, además de identificar al autor del documento, garantizar que los documentos firmados que se envían a través de redes de comunicación no han podido ser modificados por terceros, asegurando la confidencialidad de los mismos; con lo cual la finalidad inicial de la firma electrónica, que era exclusivamente la de identificar al sujeto y hacer prueba de su adhesión a un texto, cumple en las redes de comunicación otro tipo de cometidos adicionales, como garantizar la confidencialidad, integridad y no repudio.

En todo caso, la evitación del repudio de destinto se puede garantizar a través de mecanismos como el previsto en el artículo 25 de la Ley 34/2002, de Servicios de la Sociedad de la Información y Comercio Electrónica, sobre la intervención de terceros de confianza, pues las partes pueden pactar que un tercero archive las declaraciones de voluntad que integran los contratos electrónicos y que consigne la fecha y la hora en que dichas comunicaciones han tenido lugar. El tercero deberá archivar en soporte informático las declaraciones que hubieran tenido lugar por vía telemática entre las partes por el tiempo estipulado que, en ningún caso, será inferior a cinco años. Eso sí, La

intervención de dichos terceros no podrá alterar ni sustituir las funciones que corresponde realizar a las personas facultadas con arreglo a Derecho para dar fe pública.

LA FIRMA ELECTRÓNICA Y EL DOCUMENTO ELECTRÓNICO EN ESPAÑA

La regulación en España de la firma electrónica se encuentra actualmente en la Ley 59/2003, de 19 de diciembre, de firma electrónica, que viene a sustituir la regulación general jurídica de los criptosistemas de claves asimétricas), inicial de la firma electrónica del Real Decreto Ley 14/1999(5), de 17 de septiembre, convalidado por la Resolución de 21 de octubre de 1999. Pero lejos de lo que pudiera pensarse, España, ya contaba con anterioridad al RD.14/1999, de firma electrónica, con un entramado de normas legales y disposiciones de rango inferior a la ley que sostenían la validez y eficacia de la firma electrónica para determinados ámbitos.

Así, entre las leyes y normas con fuerza de ley debe destacarse el artículo 45.5 de la Ley del Régimen Jurídico de la Administración del Estado y Procedimiento Administrativo Común, que ya en su redacción de 1992 establecía que los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de los originales almacenados por estos mismos medios, gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos establecidos por esta y otras leyes.

La Ley del Mercado de Valores de 1988 regula las operaciones de Bolsa que se llevan a cabo mediante el Sistema de Interconexión Bursátil, integrado, como señala la propia Exposición de Motivos de la Ley, mediante una red informática. En esa línea debe encuadrarse el acuerdo de 11 de marzo de 1998 de la CNMV sobre implantación del CIFRA-5 El Real Decreto-ley 14/1999, de 17 de septiembre, sobre Firma Electrónica, fue aprobado con el

objetivo de fomentar la rápida incorporación de las nuevas tecnologías de seguridad de las comunicaciones electrónicas en la actividad de las empresas, los ciudadanos y las Administraciones públicas. De este modo, se coadyuvaba a potenciar el crecimiento y la competitividad de la economía española mediante el rápido establecimiento de un marco jurídico para la utilización de una herramienta que aporta confianza en la realización de transacciones electrónicas en redes abiertas como es el caso de Internet. El citado Real Decreto-ley incorporó al ordenamiento público español la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, incluso antes de su promulgación y publicación en el «Diario Oficial de las Comunidades Europeas».

Tras su ratificación por el Congreso de los Diputados, se acordó la tramitación del Real Decreto-ley 14/1999 como proyecto de ley, con el fin de someterlo a una más amplia consulta pública y al posterior debate parlamentario para perfeccionar su texto. No obstante, esta iniciativa decayó al expirar el mandato de las Cámaras en marzo de 2000. Esta Ley, por tanto, es el resultado del compromiso asumido en la VI Legislatura, actualizando a la vez el marco establecido en el Real Decreto-ley 14/1999 mediante la incorporación de las modificaciones que aconseja la experiencia acumulada desde su entrada en vigor tanto en España como en el ámbito internacional:

Las facturas puedan emitirse por vía telemática; posibilidad que ha sido más detallada en la Orden Ministerial de 22 de marzo de 1996 (RCL 1996, 1114). También existe un conjunto de órdenes que regulan la declaración de IRPF para grandes empresas, PYMES y contribuyentes, disponibles online en http://aeat.es. Además, el procedimiento para la obtención e instalación de certificado con firma electrónica para hacer la declaración del IRPF puede obtenerse en http://aeate.es/certfnmt.html. La Orden, de 19 de julio de 1999, por la que se aprueba el Registro de compraventa de bienes muebles a plazo, en su Disposición Adicional 6ª, autoriza a la DGRN para aprobar modelos en soporte informático o con firma electrónica, siempre que se garantice

la identidad indubitada de los contratantes y la integridad e inalterabilidad del documento.

En el ámbito judicial también se ha admitido tanto la validez del documento electrónico como la eficacia del documento electrónico firmado electrónicamente. Respecto de la validez del documento electrónico en el proceso, el artículo 230 LOPJ, dispone que podrán utilizarse en el proceso cualesquiera medios técnicos de documentación y reproducción, siempre que ofrezcan las debidas garantías de autenticidad.

Respecto de la validez, a efectos probatorios, de la firma electrónica, en la STS de 3 de noviembre de 1997, Sala 3ª, la Asociación Española de la Banca Privada discutía la legalidad, entre otros, del artículo 76.3.c).2 del Reglamento general del Impuesto de Transmisiones Patrimoniales y Actos Jurídicos Documentados, aprobado por el RD 828/1995, de 29 de mayo, y, en concreto, el que se pudiese someter a gravamen documentos electrónicos mercantiles con función de giro por ser necesaria la firma "escrita" del emisor.

A los efectos de lo dispuesto anteriormente, se entenderá por documento "cualquier soporte escrito, incluido los informáticos, por los que se pruebe, acredite o se haga constar alguna cosa".

Pues bien, la Asociación Española de la Banca Privada, argumentaba que si bien es cierto que toda la jurisprudencia, con base en los artículos 578 LEC y 1215 CC, aboga por la virtualidad jurídica del documento en soporte electrónico siempre que se den todas las cautelas para asegurar su autenticidad, "no puede emitirse un título valor o documento mercantil sino con la firma de su emisor, y tal firma y/o su constancia por escrito no puede suplirse por ningún soporte informático".

La respuesta del Tribunal Supremo a este problema parte de la admisión del documento electrónico, subconditione de acreditar su autenticidad, y en relación con la necesidad de la firma en los documentos con efectos de giro, a los que deber ir unida, señala lo siguiente:

"La firma gráfica no es la única manera de signar, pues hay otros mecanismos que, sin ser firma autógrafa, constituyen trazados gráficos, que así mismo conceden autoría y obligan.
Así, las claves, los códigos, los signos y, en casos, los sellos con firmas en el "sentido indicado".
En consecuencia, concluye el TS, "el documento electrónico (y en especial el documento con función de giro mercantil) es firmable, en el sentido de que la firma autógrafa o equivalente puede ser sustituida, por el lado de la criptografía, por medio de cifras, signos, códigos, barras, claves u otros atributos alfa-numéricos que permitan asegurar la procedencia y veracidad de la autoría y la procedencia de su contenido".
Tras el Real Decreto Ley 14/1999, de 17 de septiembre, que fue convalidado por la Resolución de 21 de octubre de 1999, e incorpora la Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco jurídico comunitario para la firma electrónica, debe citarse, entre otras la Instrucción DGRN de 30 de diciembre de 1999, sobre la presentación de las cuentas anuales en los Registros Mercantiles a través de procedimientos telemáticos (BOE nº 7, de 8 de enero de 2000), la instrucción DGRN de 31 de diciembre de 1999 (BOE nº 7, de 8 de enero de 2000) o el RD11 BOE 18 de septiembre de 1999.
Volviendo al Decreto Ley 14/1999, lo verdaderamente criticable y criticado del mismo fue que la normativa sobre firma electrónica se aprobase a través Decreto-Ley, figura que está prevista, según el artículo 87 CE, para casos de extraordinaria y urgente necesidad. Circunstancia que evidentemente no se daba en la regulación de la firma electrónica, máxime, como ya se ha visto, cuando el Derecho español atribuía efectos a los documentos electrónicos acompañados de firma electrónica.
Además, algunos aspectos operativos del RDL de firma electrónica de 1999 en marcha de la legislación sobre firma, como la creación del Registro de Prestadores de Servicios, estaban pendientes de realización, lo que ponían en entredicho la pretendida "urgencia" de la norma, si bien finalmente la Ley

59/2003 no los ha creado, ya que limitaba injustificadamente la libre competencia.

Finalmente, deben de destacarse dos hitos en materia de firma electrónica, el primero es el funcionamiento del registro de bienes muebles, que es el único en España que funciona de un modo totalmente telemático, y, de otro, la Ley 24/2001, que disipa todas las dudas sobre la validez y eficacia del "documento público electrónico", al permitir la plena operatividad de la firma electrónica y del documento público electrónico y su uso por Notarios y Registradores.

CONTENIDO Y ESTRUCTURA DE LA LEY DE FIRMA ELECTRÓNICA

Tal y como dispone el artículo 1, la Ley de Firma Electrónica regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación, sin que las disposiciones de la LFE alteren en modo alguno las normas relativas a la celebración, formalización, validez y eficacia de los contratos y cualesquiera otros actos jurídicos ni las relativas a los documentos en que unos y otros consten.

La Ley consta de 36 artículos agrupados en seis títulos, 10 disposiciones adicionales, dos disposiciones transitorias, una disposición derogatoria y tres disposiciones finales.

El título I contiene los principios generales que delimitan los ámbitos subjetivo y objetivo de aplicación de la Ley, los efectos de la firma electrónica y el régimen de empleo ante las Administraciones públicas y de acceso a la actividad de prestación de servicios de certificación.

El régimen aplicable a los certificados electrónicos se contiene en el título II, que dedica su primer capítulo a determinar quiénes pueden ser sus titulares y a regular las vicisitudes que afectan a su vigencia. El capítulo II regula los certificados reconocidos y el tercero el documento nacional de identidad electrónico.

El título III regula la actividad de prestación de servicios de certificación estableciendo las obligaciones a que están sujetos los prestadores distinguien-

do con nitidez las que solamente afectan a los que expiden certificados reconocidos, y el régimen de responsabilidad aplicable.

El título IV establece los requisitos que deben reunir los dispositivos de verificación y creación de firma electrónica y el procedimiento que ha de seguirse para obtener sellos de calidad en la actividad de prestación de servicios de certificación.

Los títulos V y VI dedican su contenido, respectivamente, a fijar los regímenes de supervisión y sanción de los prestadores de servicios de certificación.

Por último, cierran el texto las disposiciones adicionales -que aluden a los regímenes especiales que resultan de aplicación preferente-, las disposiciones transitorias -que incorporan seguridad jurídica a la actividad desplegada al amparo de la normativa anterior-, la disposición derogatoria y las disposiciones finales relativas al fundamento constitucional, la habilitación para el desarrollo reglamentario y la entrada en vigor.

CONCEPTO JURÍDICO DE FIRMA ELECTRÓNICA EN LA LFE

El concepto jurídico de firma electrónica del Derecho español y comunitario es el de "conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos", que pueden ser utilizados como medio de identificación del firmante, aunque como ya se ha indicado la firma electrónica puede cumplir otras utilidades a parte, o al margen, de la identificación del sujeto firmante.

Así, por ejemplo, la firma del propio sujeto escaneada e incorporada a un documento electrónico es una firma electrónica e incluso la propia identificación del titular del documento al final del texto, y como tales han de ser tenida, si bien dicha firma, como ya sen ha dicho con anterioridad, ofrece pocas garantías sobre la integridad e identidad del mensaje y, en definitiva, contienen un elevado índice de inseguridad.

La firma electrónica más segura, desde un punto de vista técnico, es actualmente la llamada firma digital o de clave asimétrica. Es más, en muchas ocasiones se confunden las expresiones de firma digital y de firma electrónica,

pero queda claro que la firma digital es una clase de firma electrónica, si bien no la única.

La firma digital consiste en una combinación de signos que forman una cadena lo suficientemente larga como para garantizar que sea imposible la existencia de una cadena igual y identificar así, de un modo fiable, a una persona con la autoría de un documento y la adhesión de ésa a su contenido. A ello se añade dos elementos más: una clave privada y una clave pública, cuya finalidad es encriptar el documento electrónico al que se añade la firma como el documento en el que se contiene la firma y que va unido al documento gracias a una función del correo electrónico.

Además, la firma electrónica suele estar en un documento electrónico expedido por una autoridad de certificación (que añade a dicho certificado su firma y otros datos que la ley especifica dependiendo del tipo de certificado), cuya finalidad primordial es certificar, bajo su responsabilidad, que determinada firma pertenece a una persona en concreto, pero que también disponen de la tecnología para crear y atribuir firma.

Pues bien, el artículo 3 LFE distingue entre "firma electrónica avanzada" y "firma electrónica reconocida". La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control. Pero si la firma electrónica avanzada está basada en un certificado reconocido y es generada mediante un dispositivo seguro de creación de firma tendrá la consideración de "firma electrónica reconocida", la cual tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel (art. 3 LFE).

En definitiva, existe muchos tipos de firma y muchos modos de utilizarla, todo ello con su debida y necesaria trascendencia jurídica, pero en el tipo de firma en el que está pensando la legislación es en la firma digital certificada (En Argentina Firma Digital con certificados licenciados) a través de una en-

tidad de certificación, de tal forma que ésta expide un documento (certificado) en el que consigna su propia firma digital, la cual puede confirmarse a través de otra entidad certificadora, y la firma digital del sujeto signatario junto con las claves pública y privada y el resto de requisitos que exija la legislación según el tipo de certificado. Dicho certificado, junto con la clave privada, quedan en manos del signatario, aconsejándose por razones de seguridad no guardar nunca el certificado en el disco duro del ordenador.

Entonces, si bien el concepto de firma electrónica, desde el punto de vista de jurídico es muy amplio, y en él tiene cabida desde la firma escaneada hasta la firma digital o de clave asimétrica y cualquier tipo de firma electrónica que se invente en el futuro, las distintas firmas electrónicas contenidas o no en distintas clases de certificados no pueden tener el mismo valor probatorio.

Eso sí, toda firma electrónica por simple que sea, y aún no certificada, debe tener eficacia jurídica, si bien los trámites conducentes a comprobar su veracidad serán más gravosos que los de "la firma electrónica reconocida".

En cuanto al empleo de firma electrónica por parte de las Administraciones Públicas, el artículo 4 LFE dispone que dicha Ley se aplicará al uso de la firma electrónica en el seno de las Administraciones públicas, sus organismos públicos y las entidades dependientes o vinculadas a las mismas y en las relaciones que mantengan aquéllas y éstos entre sí o con los particulares. Además, las Administraciones públicas, con el objeto de salvaguardar las garantías de cada procedimiento, podrán establecer condiciones adicionales a la utilización de la firma electrónica en los procedimientos. Dichas condiciones podrán incluir, entre otras, la imposición de fechas electrónicas sobre los documentos electrónicos integrados en un expediente administrativo (Se entiende por fecha electrónica el conjunto de datos en forma electrónica utilizados como medio para constatar el momento en que se ha efectuado una actuación sobre otros datos electrónicos a los que están asociado). Además, dichas condiciones sólo podrán hacer referencia a las características específicas de la aplicación de que se trate y deberán garantizar el cumplimiento de lo previsto en el artículo 45 de la Ley 30/1992, de 26 de no-

viembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Estas condiciones serán objetivas, proporcionadas, transparentes y no discriminatorias y no deberán obstaculizar la prestación de servicios de certificación al ciudadano cuando intervengan distintas Administraciones públicas españolas o del Espacio Económico Europeo. Las normas que establezcan condiciones generales adicionales para el uso de la firma electrónica ante la Administración General del Estado, sus organismos públicos y las entidades dependientes o vinculadas a las mismas se dictarán a propuesta conjunta de los Ministerios de Administraciones Públicas y de Industria Comercio y Turismo y previo informe del Consejo Superior de Informática y para el impulso de la Administración Electrónica.
De otra parte, podrá someterse a un régimen específico, la utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa. Asimismo, el Ministro de Economía y Hacienda, respetando las condiciones previstas en este Real Decreto-ley, podrá establecer un régimen normativo destinado a garantizar el cumplimiento de las obligaciones tributarías, determinando, respecto de la gestión de los tributos, la posibilidad de que el firmante sea una persona física o una persona jurídica.

EFECTOS JURÍDICOS DE LA FIRMA ELECTRÓNICA

El artículo 3 LFE, tan extenso como asistemático, se asienta en dos preceptos clave. De un lado el punto noveno del artículo 3 LFE, que señala que no se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica. De otro lado, el aparto 4º de dicho precepto, según el cual, la firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel. Además de la doble eficacia, la Ley parte de la existencia de un vínculo o nexo entre la firma electrónica y el documento electrónico con los datos en

él contenido, pues el precepto dice literalmente que la "firma (electrónica reconocida), tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita". Por tanto, los efectos de la firma lo son respecto de los contenidos del documento electrónico al que está unida la firma. Pero qué valor o eficacia tiene el documento electrónico firmado. El artículo 3 LFE, distingue entre documentos electrónicos firmados con firma reconocida y el resto de documentos que contiene otro tipo de firma electrónica o digital.

Al documento firmado con firma reconocida la Ley le otorga la equivalencia funcional con la firma manuscrita respecto de los datos consignados en forma electrónica. Mientras que al documento firmado electrónicamente, pero con una firma que no sea avanzada y basada en un certificado reconocido, no se le negarán efectos jurídicos ni será excluido como prueba en juicio, por el mero hecho de presentarse en forma electrónica, sin que la norma especifique cuál sea su eficacia. Ello se debe a que la existencia de múltiples clases de firmas electrónicas con distintos niveles o grados de seguridad no permiten adoptar una solución uniforme y única, sino que se deberá estar a cada caso en concreto, y la eficacia dependerá de la mayor o menor seguridad o fiabilidad de la firma respecto de la identidad de las personas e integridad y no repudio de los datos contenidos en el documento. Así, cualquier documento, por el solo hecho de estar firmado electrónicamente, no tiene porqué negársele eficacia o inadmitirse como prueba en juicio, pero deberán probarse los extremos relativos a la identidad, integridad, autenticación y no repudio.

Sólo el documento firmado electrónicamente mediante firma electrónica reconocida cumple los requisitos de identidad, integración, autenticación y no repudio, y por ello la eficacia de sus datos y su admisión como prueba en juicio se produce sin necesidad de adverar los extremos controvertidos de la integridad del documento, salvo que se plantee una controversia sobre los mismos y se consiga probar la falta de identidad o integridad del documento. Esta es la misma solución adoptada en la Directiva comunitaria de firma

electrónica que dispone, textualmente, que los Estados miembros procurarán que la firma electrónica avanzada basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma satisfaga el requisito jurídico de una firma en relación con los datos en forma electrónica del mismo modo que una firma manuscrita satisface dichos requisitos en relación con los datos en papel y sea admitida como prueba en procedimientos judiciales. Mientras que el artículo 5-2 de la Directiva dispone que los Estados miembros velarán por que no se niegue eficacia jurídica, ni la admisibilidad como prueba en procedimientos judiciales, a la firma electrónica por el mero hecho de que ésta se presente en forma electrónica, o no se base en un certificado reconocido, o no se base en un certificado expedido por un proveedor de servicios de certificación acreditado, o no esté creada por un dispositivo seguro de creación de firma. En ese sentido se debe interpretar los artículos 382 y ss. de la nueva LEC y en especial el artículo 384-1, que sí bien admiten el documento electrónico firmado como prueba en juicio, ello no impide el examen por el Tribunal ni las alegaciones por las partes sobre la autenticidad del documento en lo relativo a su contenido y autoría verdadera. Por ello, el apartado ocho del artículo tres dispone que el soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio. Si se impugnare la autenticidad de la firma electrónica reconocida, con la que se hayan firmado los datos incorporados al documento electrónico, se procederá a comprobar que por el prestador de servicios de certificación, que expide los certificados electrónicos, se cumplen todos los requisitos establecidos en la Ley en cuanto a la garantía de los servicios que presta en la comprobación de la eficacia de la firma electrónica, y en especial, las obligaciones de garantizar la confidencialidad del proceso así como la autenticidad, conservación e integridad de la información generada y la identidad de los firmantes. Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo

326 de la Ley de Enjuiciamiento Civil (cuyo tenor literal no estuvo diseñado para la aplicación a las nuevas tecnologías de la información, y que avoca a periciales informáticas y técnicas).

La diferencia, por tanto, entre el documento electrónico firmado con firma electrónica reconocida, respecto de los documento firmados con otro tipo de firmas menos seguras, es que los extremos de autoría, integridad, confidencialidad y no repudio (al menos en origen) se presumen existentes, salvo prueba en contrario, y siempre con una responsabilidad de estos extremos por parte del titular de la firma o de la entidad certificadora (artículo 14 LFE), no siendo necesaria su prueba, que se presume, lo que determina la carga de probar que la autoría e integridad del documento aparente no se corresponde con la realidad fáctica a quien invoque tales circunstancias.

Mientras que en los documento electrónicos con otras firmas, si bien no se les excluye por tal circunstancia (la de presentarse en formato electrónico), se deben de probar y acreditar los extremos controvertidos de autoría e integridad del documento. Evidentemente todo ello al margen de otras cuestiones que no se pueden acreditar por el mero hecho de que el documento vaya firmado electrónicamente, pero que también se presumen iuris tantum, como la plena capacidad de obrar del autor de la declaración de voluntad en el momento de emitirse la declaración de voluntad.

Asimismo es conveniente tener presente que las disposiciones contenidas en el Real Decreto ley de firma electrónica no alteran las normas relativas a la celebración, la formalización, la validez y la eficacia de los contratos y otros actos jurídicos ni el régimen jurídico aplicable a las obligaciones", debido posiblemente a la heterogeneidad de supuestos de contratación electrónica. Además, el segundo párrafo del punto segundo del artículo 1 RDLEF dispone que las normas sobre la prestación de servicios de certificación de firma electrónica que recoge este Real Decreto-ley no sustituyen ni modifican las que regulan las funciones que corresponde realizar a las personas facultadas, con arreglo a derecho, para dar fe de la firma en documentos o para intervenir en su elevación a públicos. Cuestión distinta, es si puede

existir un documento electrónico que firmado por fedatario o funcionario público en el cumplimiento de sus funciones pueda ser considerado como tal, esto es como "documento público electrónico" y desplegar la eficacia propia de un documento público cuando se trasmite y recibe a través de una red de telecomunicación para completar algún trámite relativo a la contratación o a la seguridad jurídica y en el tráfico.

En cuanto al carácter público o privado del documento firmado, el documento electrónico tendrá en todo caso la consideración de documento privado y, además, será soporte de documentos públicos cuando estén firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la Ley en cada caso o se trate de documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.

Finalmente, el apartado 10 del artículo 3 dispone que, cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta lo estipulado entre ellas respecto de la eficacia de la firma electrónica, primando pues el principio de autonomía de la voluntad, dentro del respeto a los aspectos de ius cogens de la Ley.

RESPONSABILIDAD DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Cuando ha intervenido una entidad de certificación bien expidiendo firma, bien certificando titularidades y claves de firma, la eficacia de la firma electrónica se ve reforzada mediante un sistema especial de responsabilidad, y que tiene un tratamiento peculiar y distinto del resto de prestadores de servicios de la información e intermediarios, cuya responsabilidad se regula en la

Directiva 31/2000/CE de comercio electrónico y en la Ley 34/2003, de Servicios de la Sociedad de la Información y Comercio Electrónico.

Así, el artículo 22 LFE dispone los prestadores de servicios de certificación responderán por los daños y perjuicios que causen a cualquier persona en el ejercicio de su actividad cuando incumplan las obligaciones que les impone esta Ley. La responsabilidad del prestador de servicios de certificación regulada en esta Ley será exigible conforme a las normas generales sobre la culpa contractual (arts. 1101 y ss. CC) o extracontractual (arts. 1902 y concordantes del CC), según proceda, si bien, tanto en el ámbito de la responsabilidad contractual como en el de la responsabilidad extracontractual, corresponderá al prestador de servicios de certificación demostrar que actuó con la diligencia profesional que le es exigible.

La responsabilidad, en principio, se configura como contractual en el caso de incumplimiento de las obligaciones legales o contractuales establecidas entre la Autoridad de Certificación y el titular de la firma y siempre que tenga su base en la contravención de aquello a lo que las partes se había obligado, mientras que la responsabilidad de la entidad de certificación frente a terceros será en principio extracontractual; si bien en la práctica resulta en ocasiones difícil discernir el carácter contractual o extracontractual de la responsabilidad, que se ve en todo caso atenuado por la doctrina de la "unidad de culpas".La llamada "unidad de la culpa civil" (Sentencias de 24 marzo y 23 diciembre 1952 [RJ1952\1209 y RJ 1952\2673], STS 1 febrero 1994 (RJ 1994\854) ,entre otras) se aplica los "supuestos de concurrencia de acciones de resarcimiento originadas en contrato y a la vez en un acto ilícito extracontractual". Con base en dicha "doctrina comúnmente admitida que el perjudicado puede optar entre una u otra acción cuando el hecho causante del daño sea al mismo tiempo incumplimiento de una obligación contractual y violación del deber general de no causar daño a otro", junto con los límites estrictos a que se ciñe la responsabilidad contractual en casos de coexistencia o conjunción con responsabilidad aquiliana, de manera "que no es bastante que haya un contrato entre partes para que la responsabilidad contractual

opere necesariamente con exclusión de la aquiliana sino que se requiere para que ello suceda la realización de un hecho dentro de la rigurosa órbita de lo pactado y como desarrollo del contenido negocial (Sentencia de 9 marzo 1983 [RJ 1983\1463], entre otras muchas)", criterios jurisprudenciales que gozan de manifestada continuidad en cuanto a la referida "unidad conceptual" (Sentencia de 20 diciembre 1991 [análoga a RJ 1998\2934]) que admite concurrencia de culpas por los mismos hechos (Sentencia del Tribunal Supremo 11 febrero 1993 [RJ 1993\1457]) o "yuxtaposición de las responsabilidades contractuales y extracontractuales que dan lugar a acciones que pueden ejercitarse alternativa o subsidiariamente u optando por una u otra e incluso proporcionando los hechos al juzgador para que éste aplique las normas de concurso de ambas responsabilidades que más se acomoden a ellos, todo en favor de la víctima y para el logro de un resarcimiento del daño lo más completo posible" (Sentencia del Tribunal Supremo de 15 febrero 1993 [RJ 1993\771]). Y más adelante añade: proyectado al caso el principio inspirador señalado y los criterios jurisprudenciales enunciados puede decirse que amparada una determinada pretensión procesal en unos hechos constitutivos de la "causa petendi" en términos tales que admitan, sea por concurso ideal de normas, sea por concurso real, calificación jurídica por culpa, bien contractual, bien extracontractual o ambas conjuntamente salvado por iguales hechos y sujetos concurrentes, el carácter único de la indemnización no puede absolverse de la demanda con fundamento en la equivocada o errónea elección de la norma de aplicación aducida sobre la culpa, pues se entiende que tal materia jurídica pertenece al campo del "iura novit curia" y no cabe eludir por razón de la errónea o incompleta elección de la norma el conocimiento del fondo, de manera que el cambio de punto de vista jurídico en cuestiones de esta naturaleza no supone una mutación del objeto litigioso. Por supuesto, aunque es obvio, el sistema de protección y de seguridad del tráfico económico a través de redes mediante documentos con firma electrónica basado en certificados expedidos por entidades de certificación se refuerza con la protección penal y con la responsabilidad civil deriva-

da del delito en los casos de falsificaciones y estafas cometidas mediante la manipulación de firmas electrónicas. Se observa claramente que la responsabilidad civil de las entidades se asienta primordialmente sobre la idea de responsabilidad subjetiva, esto es basada en la culpa o negligencia, sí bien hay una inversión legal de la carga de la prueba, no siendo necesario que el usuario pruebe la negligencia de la entidad de certificación, ya que ésta se presume iuris tantum. Es, por tanto, al prestador de servicios a quien corresponde demostrar que actuó con la debida diligencia para conseguir su exoneración. Además, los prestadores de servicios de certificación asumirán toda la responsabilidad frente a terceros por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de certificación.

Junto a ese régimen general, el artículo 22 prevé dos supuestos específicos en los que responderá la entidad de certificación. El primero deriva del incumplimiento las obligaciones señaladas en los párrafos b) al d) del artículo 12 de la Ley cuando garantice un certificado electrónico expedido por un prestador de servicios de certificación establecido en un Estado no perteneciente al Espacio Económico Europeo, siendo responsable por los daños y perjuicios causados por el uso de dicho certificado. El segundo deriva de los daños que se causen al firmante o a terceros de buena fe por la falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados de la extinción o suspensión de la vigencia del certificado electrónico. El artículo 22 termina señalando, en su apartado quinto, que la regulación contenida en esta Ley sobre la Responsabilidad del Prestador de Servicios de Certificación se entiende sin perjuicio de lo establecido en la legislación sobre cláusulas abusivas en contratos celebrados con consumidores. Este es un precepto que está en plena sintonía con los dispuesto en la Directiva sobre firma electrónica, por lo que dejaría sin efecto las cláusulas exoneratorias de responsabilidad para la entidad de certificación que contravengan el régimen de responsabilidad previsto en la LFE. Como novedad de la LFE caber citar el artículo 23, donde se regulan las limitaciones de res-

ponsabilidad de los prestadores de servicios de certificación. Así, el prestador de servicios de certificación no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe, si el firmante incurre en alguno de los siguientes supuestos:

a) No haber proporcionado al prestador de servicios de certificación información veraz, completa y exacta sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición o para la extinción o suspensión de su vigencia, cuando su inexactitud no haya podido ser detectada por el prestador de servicios de certificación.

b) La falta de comunicación sin demora al prestador de servicios de certificación de cualquier modificación de las circunstancias reflejadas en el certificado electrónico.

c) Negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación. Cabe excusar el pronunciamiento de fondo en materia de culpa civil si la petición se concreta en un resarcimiento aunque el fundamento jurídico aplicable a los hechos.

d) No solicitar la suspensión o revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma.

e) Utilizar los datos de creación de firma cuando haya expirado el período de validez del certificado electrónico o el prestador de servicios de certificación le notifique la extinción o suspensión de su vigencia.

f) Superar los límites que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él o no utilizarlo conforme a las condiciones establecidas y comunicadas al firmante por el prestador de servicios de certificación. Si el firmante fuese una persona jurídica, el solicitante del certificado electrónico asumirá todas estas obligaciones. Además, en el caso de los certificados electrónicos que recojan un poder de representación del firmante, tanto éste como la persona o entidad representada, cuando ésta tenga conocimiento

de la existencia del certificado, están obligados a solicitar la revocación o suspensión de la vigencia del certificado en los términos previstos en esta Ley. De otra parte, en el apartado cuarto del artículo 23 se dispone que el prestador de servicios de certificación tampoco será responsable por los daños y perjuicios ocasionados al firmante o a terceros de buena fe si el destinatario de los documentos firmados electrónicamente actúa de forma negligente. Se entenderá, en particular, que el destinatario actúa de forma negligente cuando no compruebe y tenga en cuenta las restricciones que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él, o cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado electrónico publicada en el servicio de consulta sobre la vigencia de los certificados o cuando no verifique la firma electrónica. Asimismo, el prestador de servicios de certificación no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe por la inexactitud de los datos que consten en el certificado electrónico, si éstos le han sido acreditados mediante documento público. En caso de que dichos datos deban figurar inscritos en un registro público, el prestador de servicios de certificación deberá comprobarlos en el citado registro en el momento inmediato anterior a la expedición del certificado, pudiendo emplear, en su caso, medios telemáticos. Eso sí, la exención de responsabilidad frente a terceros obliga al prestador de servicios de certificación a probar que actuó en todo caso con la debida diligencia. Otra fuente de responsabilidad, tanto civil como administrativa, es la derivada del artículo 17 LFE, que sujeta el tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y disposiciones dictadas en su desarrollo (especialmente en el árido terreno de la cesión inconsentida de datos personales).

El mismo régimen será de aplicación a los datos personales que se conozcan en el órgano que, en el ejercicio de sus funciones, supervisa la actua-

ción de los prestadores de servicios de certificación y el competente en materia de acreditación, así como el Registro de Prestadores de Servicios. Además, lo prestadores de servicios de certificación que expidan certificados a los usuarios, únicamente pueden recabar datos personales directamente de los titulares de los mismos o con su consentimiento explícito. Los datos requeridos serán, exclusivamente, los necesarios para la expedición y el mantenimiento del certificado.

Por último, los prestadores de servicios de certificación que hayan consignado un seudónimo en el certificado, a solicitud del signatario, están especialmente obligados a constatar su verdadera identidad y conservar la documentación que la acredite. Dichos prestadores de servicios estarán obligados a revelar la identidad de los titulares de certificados cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás supuestos previstos en la legislación de protección de datos y sin perjuicio de lo que, en la legislación específica en materia tributaria, de defensa de la competencia y de seguridad pública, se disponga sobre la identificación de las personas.

LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Como ya sabemos, los sujetos que hacen posible el empleo de la firma electrónica son los denominados prestadores de servicios de certificación. Para ello expiden certificados electrónicos, que son documentos electrónicos que relacionan las herramientas de firma electrónica en poder de cada usuario con su identidad personal, dándole así a conocer en el ámbito telemático como firmante. Así, según el artículo 2 LFE, dicha Ley se aplicará a los prestadores de servicios de certificación establecidos en España y a los servicios de certificación que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.

Se entenderá que un prestador de servicios de certificación está establecido en España cuando su residencia o domicilio social se halle en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios. En otro

caso, se atenderá al lugar en que se realice dicha gestión o dirección. Se presumirá asimismo que un prestador de servicios de certificación está establecido en España cuando dicho prestador o alguna de sus sucursales se haya inscrito en el Registro Mercantil o en otro registro público español en el que fuera necesaria la inscripción para la adquisición de personalidad jurídica. Pero la mera utilización de medios tecnológicos situados en España para la prestación o el acceso al servicio no implicará, por sí sola, el establecimiento del prestador en España.

Ahora bien, el artículo 5 LFE dispone que la prestación de servicios de certificación no está sujeta a autorización previa y se realizará en régimen de libre competencia. No podrán establecerse restricciones para los servicios de certificación que procedan de otro Estado miembro del Espacio Económico Europeo. Los órganos de defensa de la competencia velarán por el mantenimiento de condiciones de competencia efectiva en la prestación de servicios de certificación al público mediante el ejercicio de las funciones que tengan legalmente atribuidas. De otra parte, la prestación al público de servicios de certificación por las Administraciones públicas, sus organismos públicos o las entidades dependientes o vinculadas a las mismas se realizará con arreglo a los principios de objetividad, transparencia y no discriminación.

Además, la Ley obliga a los prestadores de servicios de certificación a efectuar una tutela y gestión permanente de los certificados electrónicos que expiden. Los detalles de esta gestión deben recogerse en la llamada declaración de prácticas de certificación, donde se especifican las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados electrónicos. Además, estos prestadores están obligados a mantener accesible un servicio de consulta sobre el estado de vigencia de los certificados en el que debe indicarse de manera actualizada si éstos están vigentes o si su vigencia ha sido suspendida o extinguida. Por otra parte, la Ley contiene las garantías que deben ser cumplidas por los dispositivos de creación de firma para que puedan ser considerados como dispositivos seguros y conformar así una firma electrónica reconocida. La certificación

técnica de los dispositivos seguros de creación de firma electrónica se basa en el marco establecido por la Ley 21/1992, de 16 de julio, de Industria y en sus disposiciones de desarrollo. Para esta certificación se utilizarán las normas técnicas publicadas a tales efectos en el «Diario Oficial de las Comunidades Europeas» o, excepcionalmente, las aprobadas por el Ministerio de Industria, Comercio y Turismo. Como novedad de la Ley 59/2003 respecto del régimen del Real Decreto Ley de Firma Electrónica es de destacar de manera particular, la eliminación del registro de prestadores de servicios de certificación, que ha dado paso al establecimiento de un mero servicio de difusión de información sobre los prestadores que operan en el mercado, las certificaciones de calidad y las características de los productos y servicios con que cuentan para el desarrollo de su actividad.

Por otra parte, la Ley modifica el concepto de certificación de prestadores de servicios de certificación para otorgarle mayor grado de libertad y dar un mayor protagonismo a la participación del sector privado en los sistemas de certificación y eliminando las presunciones legales asociadas a la misma, adaptándose de manera más precisa a lo establecido en la directiva. Así, se favorece la autorregulación de la industria, de manera que sea ésta quien diseñe y gestione, de acuerdo con sus propias necesidades, sistemas voluntarios de acreditación destinados a mejorar los niveles técnicos y de calidad en la prestación de servicios de certificación. El nuevo régimen nace desde el convencimiento de que los sellos de calidad son un instrumento eficaz para convencer a los usuarios de las ventajas de los productos y servicios de certificación electrónica, resultando imprescindible facilitar y agilizar la obtención de estos símbolos externos para quienes los ofrecen al público. Si bien se recogen fielmente en la Ley los conceptos de «acreditación» de prestadores de servicios de certificación y de «conformidad» de los dispositivos seguros de creación de firma electrónica contenidos en la directiva, la terminología se ha adaptado a la más comúnmente empleada y conocida recogida en la Ley 21/1992, de 16 de julio, de Industria.

Otra modificación relevante es que la Ley clarifica la obligación de constitución de una garantía económica por parte de los prestadores de servicios de certificación que emitan certificados reconocidos, estableciendo una cuantía mínima única de tres millones de euros, flexibilizando además la combinación de los diferentes instrumentos para constituir la garantía.

Dado que la prestación de servicios de certificación no está sujeta a autorización previa, resulta importante destacar que la Ley refuerza las capacidades de inspección y control del Ministerio de Industria, Comercio y Turismo, señalando que este departamento podrá ser asistido de entidades independientes y técnicamente cualificadas para efectuar las labores de supervisión y control sobre los prestadores de servicios de certificación.

Finalmente, conviene tener presente lo dispuesto en el artículo 20, donde se señala las obligaciones de los prestadores de servicios de certificación que expidan certificados reconocidos, pues demás de las obligaciones generales prevista en la Ley, los prestadores de servicios de certificación que expidan certificados reconocidos deberán cumplir las siguientes obligaciones:

a) Demostrar la fiabilidad necesaria para prestar servicios de certificación.

b) Garantizar que pueda determinarse con precisión la fecha y la hora en las que se expidió un certificado o se extinguió o suspendió su vigencia.

c) Emplear personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y de gestión adecuados en el ámbito de la firma electrónica.

d) Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.

e) Tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación y su entrega por un procedimiento seguro al firmante.

f) Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.
g) Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.
Además, los prestadores de servicios de certificación que expidan certificados reconocidos deberán constituir un seguro de responsabilidad civil por importe de al menos 3.000.000 de euros para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados que expidan (rebajándose así los 6.000.000 euros que se exigían en el RDLFE de 1999). Dicha garantía podrá ser sustituida total o parcialmente por una garantía mediante aval bancario o seguro de caución, de manera que la suma de las cantidades aseguradas sea al menos de 3.000.000 de euros.

RÉGIMEN JURÍDICO DE LOS CERTIFICADOS

Según el artículo 6 LFE, un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.
Además, según el artículo 11 son "certificados reconocidos" los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.
Los certificados reconocidos incluirán, al menos, los siguientes datos:
a) La indicación de que se expiden como tales.

b) El código identificativo único del certificado.
c) La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.
d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.
e) La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.
f) Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.
g) El comienzo y el fin del período de validez del certificado.
h) Los límites de uso del certificado, si se establecen.
i) Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.
Los certificados reconocidos podrán asimismo contener cualquier otra circunstancia o atributo específico del firmante en caso de que sea significativo en función del fin propio del certificado y siempre que aquél lo solicite y si los certificados reconocidos admiten una relación de representación incluirán una indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales, de conformidad con el apartado 2 del artículo 13.
Ahora bien, según el artículo 12, antes de la expedición de un certificado reconocido, los prestadores de servicios de certificación deberán cumplir las siguientes obligaciones:

a) Comprobar la identidad y circunstancias personales de los solicitantes de certificados con arreglo a lo dispuesto en el artículo siguiente.

b) Verificar que la información contenida en el certificado es exacta y que incluye toda la información prescrita para un certificado reconocido.
c) Asegurarse de que el firmante está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.
d) Garantizar la complementariedad de los datos de creación y verificación de firma, siempre que ambos sean generados por el prestador de servicios de certificación.
Respecto de la comprobación de la identidad y otras circunstancias personales de los solicitantes de un certificado reconocido, el artículo 13 LFE dispone que la identificación de la persona física que solicite un certificado reconocido exigirá su personación ante los encargados de verificarla y se acreditará mediante el documento nacional de identidad, pasaporte u otros medios admitidos en derecho. Podrá prescindirse de la personación si su firma en la solicitud de expedición de un certificado reconocido ha sido legitimada en presencia notarial. El régimen de personación en la solicitud de certificados que se expidan previa identificación del solicitante ante las Administraciones públicas se regirá por lo establecido en la normativa administrativa.
En el caso de certificados reconocidos de personas jurídicas, los prestadores de servicios de certificación comprobarán, además, los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante, bien mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, bien mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente, cuando aquéllos no sean de inscripción obligatoria. Además, si los certificados reconocidos reflejan una relación de representación voluntaria, los prestadores de servicios de certificación comprobarán, los datos relativos a la personalidad jurídica del representado y a la extensión y vigencia de las facultades del representante, bien mediante consulta en el registro público en el que estén inscritas, bien mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente, cuando aquéllos no sean de inscripción obligato-

ria. Si los certificados reconocidos admiten otros supuestos de representación, los prestadores de servicios de certificación deberán exigir la acreditación de las circunstancias en las que se fundamenten, en la misma forma prevista anteriormente. Cuando el certificado reconocido contenga otras circunstancias personales o atributos del solicitante, como su condición de titular de un cargo público, su pertenencia a un colegio profesional o su titulación, éstas deberán comprobarse mediante los documentos oficiales que las acrediten, de conformidad con su normativa específica. Los prestadores de servicios de certificación podrán realizar las actuaciones de comprobación previstas en este artículo por sí o por medio de otras personas físicas o jurídicas, públicas o privadas, siendo responsable, en todo caso, el prestador de servicios de certificación. De todos modos, cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados constaran ya al prestador de servicios de certificación en virtud de una relación preexistente, en la que, para la identificación del interesado, se hubieran empleado los medios señalados en este artículo y el período de tiempo transcurrido desde la identificación es menor de cinco años, o cuando para solicitar un certificado se utilice otro vigente para cuya expedición se hubiera identificado al firmante en la forma prescrita en este artículo y le conste al prestador de servicios de certificación que el período de tiempo transcurrido desde la identificación es menor de cinco años, se podrá omitir los trámites de comprobación de identidad. Por otra parte, todo certificado tiene una vigencia limitada que se justifica por motivos técnicos, ya que un certificado no puede estar vigente más allá del tiempo en que un tercero puede descifrar la clave privada y hacer uso de la firma electrónica ajena. En ese sentido, el artículo 8 LFE, apartado segundo, dispone que el período de validez de los certificados electrónicos será adecuado a las características y tecnología empleada para generar los datos de creación de firma y que en el caso de los certificados reconocidos este período no podrá ser superior a cuatro años.

Además, según el artículo 8, apartado primero, son causas de extinción de la vigencia de un certificado electrónico:

a) Expiración del período de validez que figura en el certificado.
b) Revocación formulada por el firmante, la persona física o jurídica representada por
éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.
c) Violación o puesta en peligro del secreto de los datos de creación de firma del firmante o del prestador de servicios de certificación o utilización indebida de dichos datos por un tercero.
d) Resolución judicial o administrativa que lo ordene.
e) Fallecimiento o extinción de la personalidad jurídica del firmante; fallecimiento, o extinción de la personalidad jurídica del representado; incapacidad sobrevenida, total o parcial, del firmante o de su representado; terminación de la representación; disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica.
f) Cese en la actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos por aquél sean transferidos a otro prestador de servicios de certificación.
g) Alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.
h) Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.
La extinción de la vigencia de un certificado electrónico surtirá efectos frente a terceros, en los supuestos de expiración de su período de validez, desde que se produzca esta circunstancia y, en los demás casos, desde que la indicación de dicha extinción se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación. De igual modo, el artículo 9 dispone que los prestadores de servicios de certificación

suspenderán la vigencia de los certificados electrónicos expedidos si concurre alguna de las siguientes causas:

a) Solicitud del firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.

b) Resolución judicial o administrativa que lo ordene.

c) La existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los certificados contempladas en los párrafos c) y g) del artículo 8.1.

d) Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

La suspensión de la vigencia de un certificado electrónico surtirá efectos desde que se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación. En caso de extinción o suspensión de la vigencia de certificados electrónicos, la Ley impone al prestador de servicios de certificación la obligación de que haga constar inmediatamente, de manera clara e indubitada, la extinción o suspensión de la vigencia de los certificados electrónicos en el servicio de consulta sobre la vigencia de los certificados en cuanto tenga conocimiento fundado de cualquiera de los hechos determinantes de la extinción o suspensión de su vigencia. Además, el prestador de servicios de certificación informará al firmante acerca de esta circunstancia de manera previa o simultánea a la extinción o suspensión de la vigencia del certificado electrónico, especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto. En los casos de suspensión, indicará, además, su duración máxima, extinguiéndose la vigencia del certificado si transcurrido dicho plazo no se hubiera levantado la suspensión. Eso sí, la extinción o suspensión de la vigencia de un certificado electrónico no tendrá efectos retroactivos y se mantendrá accesible en el servicio de consulta sobre la vigencia de los certificados al menos hasta la fecha en que hubiera finalizado su período inicial de validez.

Finalmente, el artículo 14 prevé la equivalencia internacional de certificados

reconocidos, en el sentido de que los certificados electrónicos que los prestadores de servicios de certificación establecidos en un Estado que no sea miembro del Espacio Económico Europeo expidan al público como certificados reconocidos de acuerdo con la legislación aplicable en dicho Estado se considerarán equivalentes a los expedidos por los establecidos en España, siempre que se cumpla alguna de las siguientes condiciones:

a) Que el prestador de servicios de certificación reúna los requisitos establecidos en la normativa comunitaria sobre firma electrónica para la expedición de certificados reconocidos y haya sido certificado conforme a un sistema voluntario de certificación establecido en un Estado miembro del Espacio Económico Europeo.

b) Que el certificado esté garantizado por un prestador de servicios de certificación establecido en el Espacio Económico Europeo que cumpla los requisitos establecidos en la normativa comunitaria sobre firma electrónica para la expedición de certificados reconocidos.

c) Que el certificado o el prestador de servicios de certificación estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad Europea y terceros países u organizaciones internacionales.

EL DNI ELECTRÓNICO

También ha de destacarse la regulación que la Ley contiene respecto del documento nacional de identidad electrónico, que se erige en un certificado electrónico reconocido llamado a generalizar el uso de instrumentos seguros de comunicación electrónica capaces de conferir la misma integridad y autenticidad que la que actualmente rodea las comunicaciones a través de medios físicos. Así, el artículo 15 dispone que el documento nacional de identidad electrónico es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos. Además, la Ley impone a todas la personas físicas o jurídicas, públicas o privadas, la obligación o el deber de reconocer la eficacia del documento nacional de identidad electrónico para acreditar la identidad y los demás datos personales del titular que consten en el mismo, y para acreditar

la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos.

En cuanto a los requisitos y características del documento nacional de identidad electrónico, el artículo 16 LFE se limita a señalar que los órganos competentes del Ministerio del Interior para la expedición del documento nacional de identidad electrónico cumplirán las obligaciones que la presente Ley impone a los prestadores de servicios de certificación que expidan certificados reconocidos con excepción de la relativa a la constitución de la garantía de los 3.000.000 de Euros a la que se refiere el apartado 2 del artículo 20, así como que la Administración General del Estado empleará, en la medida de lo posible, sistemas que garanticen la compatibilidad de los instrumentos de firma electrónica incluidos en el documento nacional de identidad electrónico con los distintos dispositivos y productos de firma electrónica generalmente aceptados. Como puede observarse, la Ley se limita a fijar el marco normativo básico del nuevo DNI electrónico poniendo de manifiesto sus dos notas más características -acredita la identidad de su titular en cualquier procedimiento administrativo y permite la firma electrónica de documentos- remitiéndose a la normativa específica en cuanto a las particularidades de su régimen jurídico.

LA FIRMA ELECTRÓNICA DE LAS PERSONAS JURÍDICAS

Concluiremos esta revisión de los aspectos más destacados de la Ley 59/2003 con un tema que merece un tratamiento singular, como es el establecimiento en la Ley del régimen aplicable a la actuación de personas jurídicas como firmantes ya que en Argentina existe un vacio legal en este sentido. España se va así más allá del Real Decreto-ley de1999, que sólo permitía a las personas jurídicas ser titulares de certificados electrónicos en el ámbito de la gestión de los tributos. Precisamente, la enorme expansión que han tenido estos certificados en dicho ámbito en los últimos años, sin que ello haya representado aumento alguno de la litigiosidad ni de inseguridad jurídica en las transacciones, aconsejan la generalización de la titularidad de

certificados por personas morales. En todo caso, los certificados electrónicos de personas jurídicas no alteran la legislación civil y mercantil en cuanto a la figura del representante orgánico o voluntario y no sustituyen a los certificados electrónicos que se expidan a personas físicas en los que se reflejen dichas relaciones de representación. Como resortes de seguridad jurídica, la Ley exige, por un lado, una especial legitimación para que las personas físicas soliciten la expedición de certificados; por otro lado, obliga a los solicitantes a responsabilizarse de la custodia de los datos de creación de firma electrónica asociados a dichos certificados, todo ello sin perjuicio de que puedan ser utilizados por otras personas físicas vinculadas a la entidad. Por último, de cara a terceros, limita el uso de estos certificados a los actos que integren la relación entre la persona jurídica y las Administraciones públicas y a las cosas o servicios que constituyen el giro o tráfico ordinario de la entidad, sin perjuicio de los posibles límites cuantitativos o cualitativos que puedan añadirse. Se trata de conjugar el dinamismo que debe presidir el uso de estos certificados en el tráfico con las necesarias dosis de prudencia y seguridad para evitar que puedan nacer obligaciones incontrolables frente a terceros debido a un uso inadecuado de los datos de creación de firma. El equilibrio entre uno y otro principio se ha establecido sobre las cosas y servicios que constituyen el giro o tráfico ordinario de la empresa de modo paralelo a cómo nuestro más que centenario Código de Comercio regula la vinculación frente a terceros de los actos de comercio realizados por el factor del establecimiento. Adicionalmente, se añade un régimen especial para la expedición de certificados electrónicos a entidades sin personalidad jurídica a las que se refiere el artículo 33 de la Ley General Tributaria, a los solos efectos de su utilización en el ámbito tributario, en los términos que establezca el Ministerio de Hacienda. Sin embargo, el régimen jurídico de firma electrónica de las personas jurídicas responsabiliza del uso indebido de la firma electrónica a la persona física que la solicitó y a quien se le concedió y, además, si dicha persona física deja de formar parte de la persona jurídica obliga a to-

mar las medidas de pertinentes, que avocarán, por criterios de seguridad, a la extinción del certificado.

Quizá, con la firma electrónica de las personas jurídicas, se ha querido llevar al mundo comercial una realidad que ha funcionado con eficacia en las relaciones entre las personas jurídicas y la Administración (como ocurre con el pago del impuesto de sociedades), pero el problema estriba en el carácter más dinámico que tiene la representación de las personas jurídicas en el tráfico y la posibilidad de revocación o cese de tal representación, y, en ese sentido, creo que no se justifica la existencia de este certificado de firma electrónica a favor de personas jurídica y que se debía de haber optado por el mismo sistema de actuación que se emplea fuera de línea, en el que los representantes (personas física) de la persona jurídica puedan actuar en su nombre, máxime si se tiene en cuenta que el desarrollo tecnológico experimentado en los Registros Españoles permite solucionar la cuestión de la representación de las personas jurídicas de forma sencilla, segura y eficaz, ya que con una conexión telemática en línea (es decir, en tiempo real) con el Registro Mercantil permite comprobar con total fiabilidad la realidad y vigencia de la representación. Será la práctica, en definitiva, la que ponga de manifiesto el acierto y la utilidad de la firma electrónica de las personas jurídicas.

VIII. Implementación de experiencia de timbrado digital

A) Selección final de la experiencia de timbrado digital

En función del estudio de investigación realizado e informado en el Tercer Informe Parcial, sobre las distintas alternativas de circuitos administrativos que resultaran adecuados para la aplicación de la tecnología de timbrado digital, se distinguieron dos aplicaciones cuyo diseño se abordó con mayor detalle, por resultar en ese momento y según las conclusiones oportunamente documentadas, las de mayor factibilidad según los criterios de evaluación propuestos. En particular, se detalló el diseño de las siguientes experiencias:

1. Procedimiento de solicitud y emisión de Certificado de Buena Conducta emitido por la Policía Científica de Mendoza.
2. Procedimiento de solicitud y emisión de Certificado de Servicios y Remuneraciones requerido por la ANSES.

No obstante esto, se aclaró oportunamente que la implementación efectiva de dichos diseños estaba sujeta a decisiones de carácter político que debían ser tomadas con posterioridad y que los cambios u alteraciones que derivasen de estas decisiones serían plasmados en informes subsiguientes. Dado que la toma de estas decisiones se postergó en el tiempo y que el contexto político y operativo no acompañó a la implementación efectiva de alguno de estos circuitos, la presente consultoría decidió abordar la implementación de una tercera alternativa cuya concreción efectiva resultaba más segura en términos del interés manifestado por los organismos usuarios. Nos referimos en particular al circuito de emisión de la Tarjeta Única Migratoria (TUM) emitido por la Dirección Nacional de Migraciones, a través de la Guía de Trámites de la provincia de Mendoza, a los ciudadanos argen-

tinos o extranjeros que deseen cruzar al vecino país de Chile por el paso fronterizo Horcones.

Cabe en esta instancia, por tanto, documentar el diseño que debió realizarse, como tarea previa al desarrollo e implementación de la experiencia.

B) Diseño de experiencia

Procedimiento de Solicitud y Emisión de la Tarjeta Única Migratoria (TUM) emitido por la Dirección Nacional de Migraciones

1. **Tipo de Circuito**:

Este procedimiento tiene como producto final la impresión en soporte papel de la ***TUM*** o ***Visa*** que permite a ciudadanos argentinos o extranjeros realizar el trámite migratorio en el paso fronterizo Horcones/Libertadores en el cruce a Chile.

En la actualidad, los ciudadanos pueden obtener esta TUM por triplicado en forma on-line desde la Guía Orientadora de Trámites del Gobierno de la Provincia de Mendoza http://www.tramite.mendoza.gov.ar y presentarla luego en el paso fronterizo para concretar su salida y posterior ingreso al país. No obstante la efectividad y sencillez del sistema actual, los formularios emitidos por el mismo carecen de mecanismos de seguridad que garanticen su originalidad y procedencia, lo que justifica la aplicación de timbre digital a la TUM para asegurar la autenticidad y verificabilidad de dicho documento migratorio.

2. Carácter gratuito:

Este procedimiento cumple también la condición de no exigir retribución monetaria por parte de los ciudadanos usuarios. Tal condición, como

expresáramos previamente, facilita considerablemente cuestiones de índole operativa en pos de la implementación inicial rápida y con plena funcionalidad en términos de utilidad para el ciudadano, siempre que este no necesita trasladarse personalmente, ni hacer colas para de realizar el trámite.

3. Sistematización de la información:

Atendiendo a cuestiones que mejoran calidad de la implementación en términos de resultados en el tiempo, este procedimiento es sumamente simple por cuanto no maneja información de bases de datos. Además cuenta con una alta repitencia, sobre todo en temporada estival en que se incrementa el volumen de personas que viajan a Chile por vacaciones.

4. Estrategia multicanal:

Este criterio, fundamental para la posterior digitalización completa del circuito, es una base esencial para la elección del procedimiento. Se trata de utilizar al timbre como forma de bajar la firma digital al papel, es decir las TUM firmadas digitalmente no necesitarán, en un futuro, ser impresos para presentarlos en los cruces de frontera, sino que se podrán chequear directamente desde un repositorio digital accesible vía web.

5. Utilidad para el usuario:

Este factor es muy importante siempre que tengamos 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 este sentido, la obtención on-line de la TUM aportó en su momento al ***ahorro de tiempos y disminución de colas***, por cuanto agilizó significativamente la realización del trámite, ya que el usuario no debe realizar ningún tipo de cola ni para iniciar el trámite ni para retirarlo, lo que redunda en un considerable ahorro de su tiempo. Por otra parte al tratarse de un trámite a nivel nacional tiene un alto ***grado de distribución geográfica*** de ciudadanos usuarios; es aquí donde la aplicación de estas tecnologías

determina un gran ahorro en términos de costos y tiempo de traslado hasta la dependencia en dónde se realiza ya que los suprime de plano. Aportar hoy, seguridad y verificabilidad a la TUM emitida por el sistema on-line, a través de timbre digital, resulta un aspecto fundamental para ***generar la confianza*** que los usuarios necesitan depositar en este sistema en vías a masificar su uso.

c) Diseño de la implementación

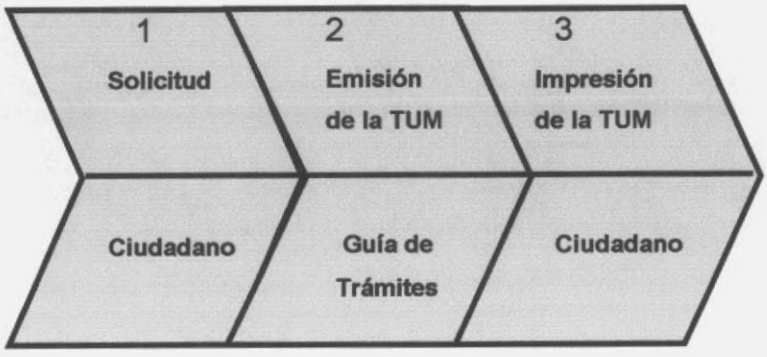
Procedimiento de Solicitud y Emisión de la Tarjeta Única Migratoria (TUM) emitido por la Dirección Nacional de Migraciones

El presente procedimiento describe el conjunto de pasos a realizar por los ciudadanos/usuarios que requieran la TUM.

Secuencia Sintética del Proceso

(Arrow chart)

Etapas



Principal sector interviniente

Objetivo:

A través de la redacción de este procedimiento se busca formalizar las tareas que lo conforman y fortalecer el diseño administrativo con la im-

plementación de tecnología de firma y timbre digital en el mismo. Además, se busca asegurar garantías de autenticidad e integridad de los documentos entregados.

Alcance:

Este trámite se facilita a todos los ciudadanos argentinos o extranjeros que deseen cruzar a Chile por el paso fronterizo Horcones, ubicado sobre la Ruta Nacional N° 7.

Definición de Roles

Responsable del Procedimiento: Hebe Gazzola
Oficina: Dirección Nacional de Migraciones

Descripción del Procedimiento:

4. ***Ciudadano/Solicitante:*** ingresa al Sitio Web de la Guía de Trámites, en e-trámite por Internet http://www.tramite.mendoza.gov.ar/ y elige la opción TUM (Tarjeta Única Migratoria). A continuación, completa y envía el formulario de solicitud web con los datos completos que el mismo requiere.
5. ***Guía de Trámites***: Una vez completado el formulario de solicitud el sistema generará automáticamente un documento PDF con la TUM, la cual se emite por cuadruplicado, timbrada digitalmente.

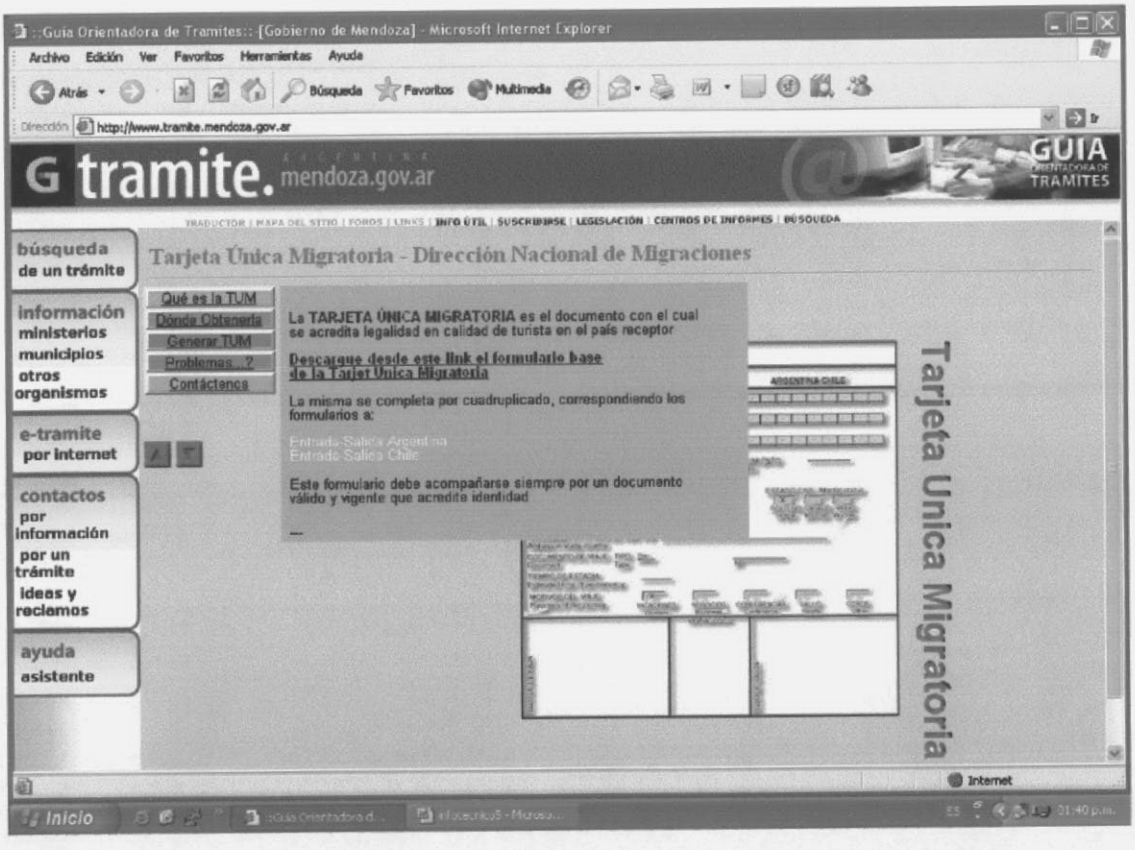
6. ***Ciudadano:*** Imprime las cuatro copias de la TUM timbrada, generada por el sistema y las presenta al momento de su viaje en el Control Aduanero Argentino realizado por la Oficina Nacional de Migraciones en el puesto fronterizo.

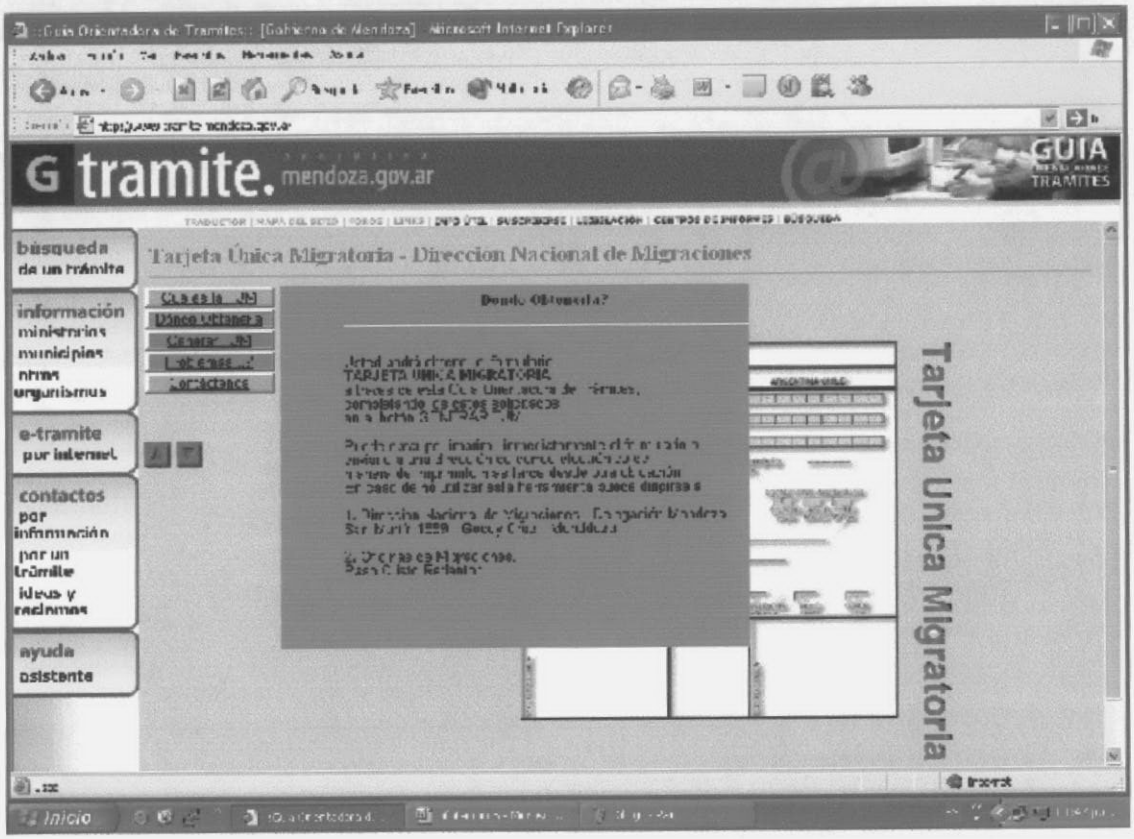
7. ***Oficina Nacional de Migraciones:*** Revisa, sella y retiene el comprobante de salida del país, al ser presentado por el ciudadano/viajero, verifi-

cando el timbre digital correspondiente y aprobando o no la salida de la persona. Los duplicados de la TUM generados por el sistema serán luego requeridos por la Policía Chilena y el Control de Migraciones de dicho país al momento de ingresar y salir del mismo.

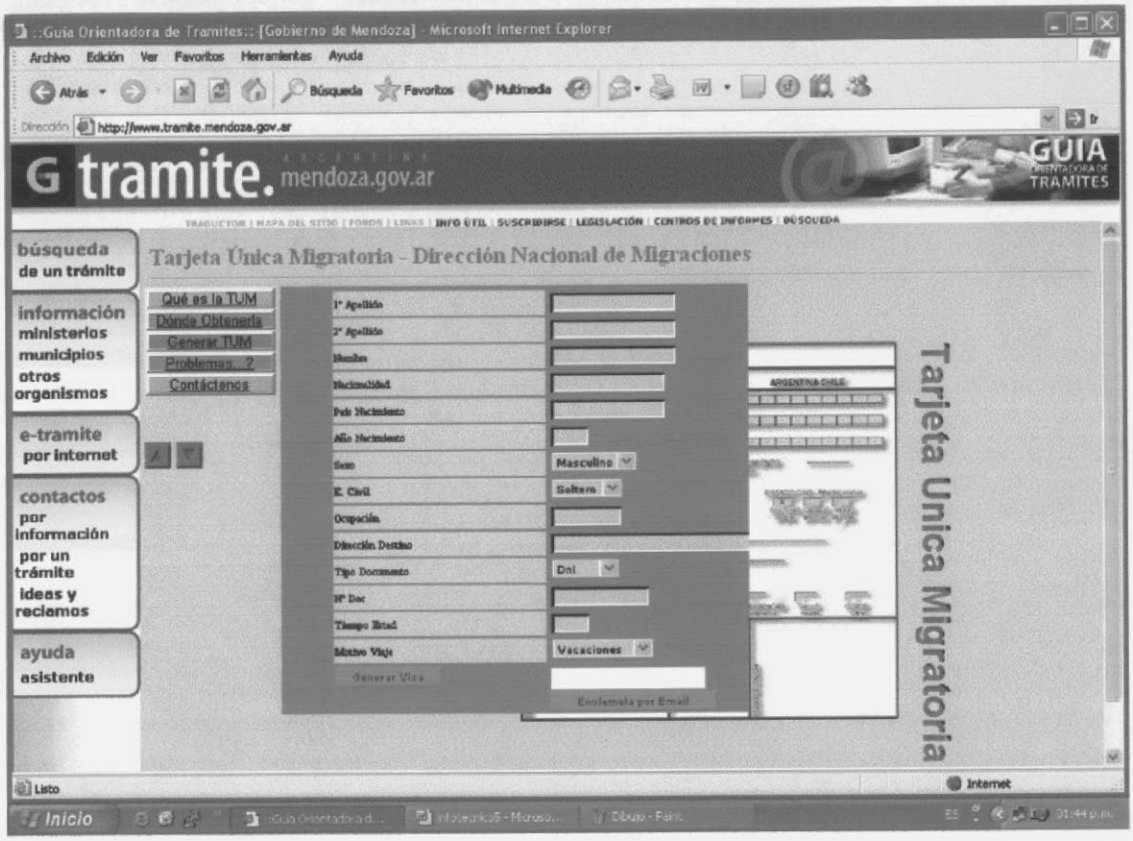
Adjuntos

Ayuda on-line a usuarios





Formulario de solicitud web de TUM



TUM expedida por el Sistema

Tarjeta Unica Migratoria

Sr. Viajero

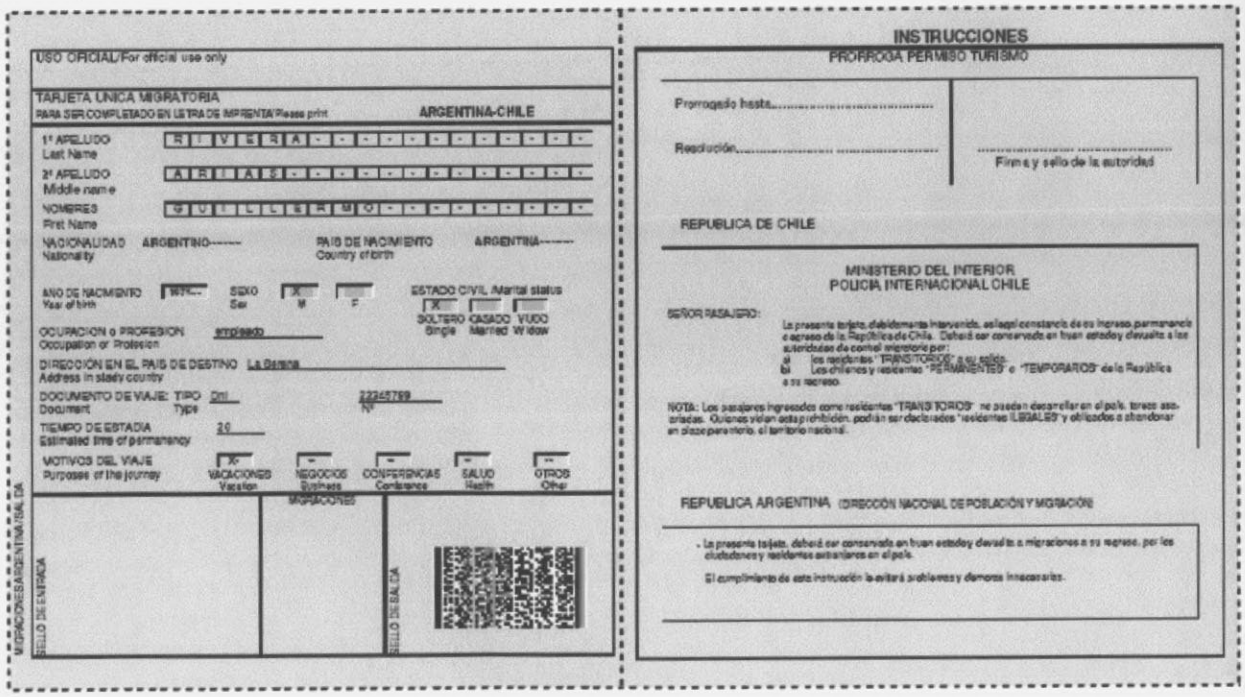
A continuación serán impresos 4 formularios (**TARJETA UNICA MIGRATORIA**) de **23,8cm x 19.9cm** cada uno. Recorte a lo largo de la línea punteada cada uno de ellos.

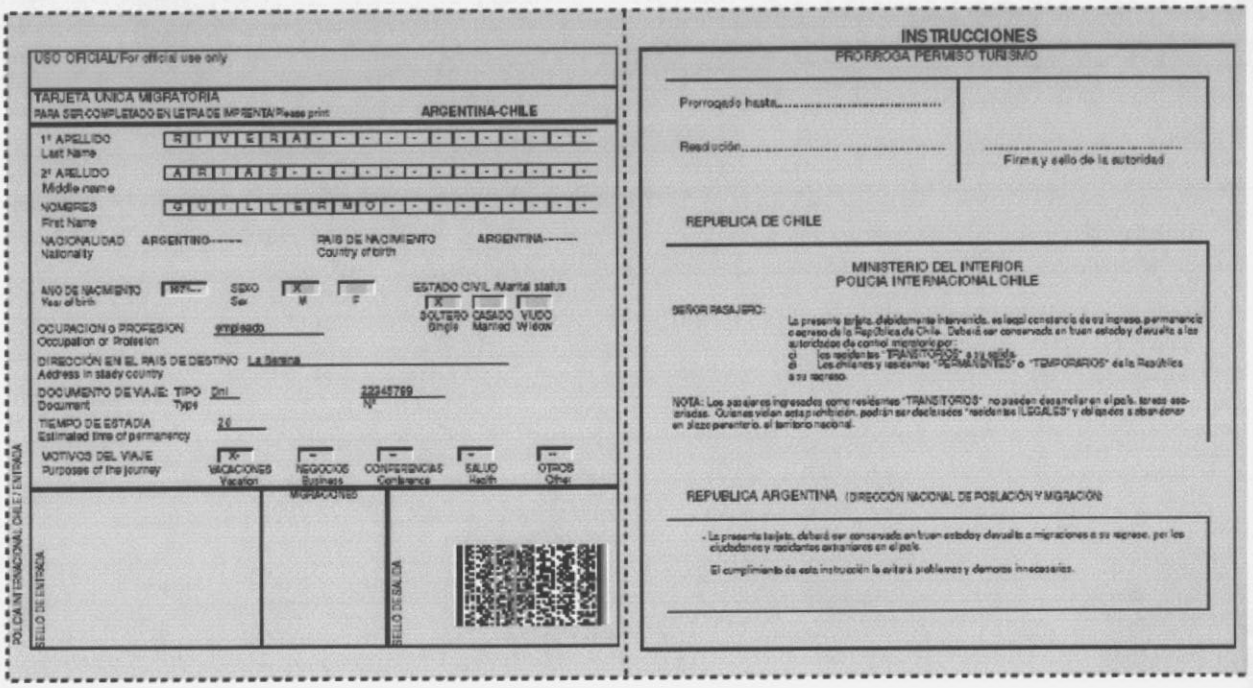
El primero (color gris) será retenido en el **CONTROL ADUANERO ARGENTINO.**.

El segundo será retenido por la **POLICIA CHILENA** en el puesto de control policial chileno.

Conserve cuidadosamente los dos formularios restantes, puesto que estos representan el principal documento de identificación en la República de Chile.

Si observa algún problema con la impresión de los cuatro formularios (tamaño desproporcionado, datos ilegibles, etc.) por favor consulte con el agente autorizado para la gestión de dichos documentos.





USO OFICIAL/For official use only

TARJETA UNICA MIGRATORIA
PARA SER COMPLETADO EN LETRA DE IMPRENTA/Please print — ARGENTINA-CHILE

1º APELLIDO / Last Name: RIVERA
2º APELLIDO / Middle name: ARIAS
NOMBRES / First Name: GUILLERMO
NACIONALIDAD / Nationality: ARGENTINO
PAIS DE NACIMIENTO / Country of birth: ARGENTINA
AÑO DE NACIMIENTO / Year of birth: 1971
SEXO / Sex: M X — F
ESTADO CIVIL / Marital status: SOLTERO / Single X — CASADO / Married — VIUDO / Widow
OCUPACION o PROFESION / Occupation or Profesion: empleado
DIRECCIÓN EN EL PAIS DE DESTINO / Address in study country: La Serena
DOCUMENTO DE VIAJE: TIPO / Document Type: Dni — Nº 22345789
TIEMPO DE ESTADIA / Estimated time of permanency: 20
MOTIVOS DEL VIAJE / Purposes of the journey: VACACIONES / Vacation X — NEGOCIOS / Business — CONFERENCIAS / Conference — SALUD / Health — OTROS / Other

POLICIA INTERNACIONAL DE CHILE
SELLO DE ENTRADA / MIGRACIONES / SELLO DE SALIDA

INSTRUCCIONES
PRORROGA PERMISO TURISMO

Prorrogado hasta.....
Resolución.....
Firma y sello de la autoridad

REPUBLICA DE CHILE

MINISTERIO DEL INTERIOR
POLICIA INTERNACIONAL CHILE

SEÑOR PASAJERO:

La presente tarjeta, debidamente intervenida, es legal constancia de su ingreso, permanencia o egreso de la República de Chile. Deberá ser conservada en buen estado y devuelta a las autoridades de control migratorio por:
a) los residentes "TRANSITORIOS" a su salida
b) Los chilenos y residentes "PERMANENTES" o "TEMPORARIOS" de la República a su regreso.

NOTA: Los pasajeros ingresados como residentes "TRANSITORIOS" no pueden desarrollar en el país, tareas asociadas. Quienes violen esta prohibición, podrán ser declarados "residentes ILEGALES" y obligados a abandonar en plazo perentorio, el territorio nacional.

REPUBLICA ARGENTINA (DIRECCIÓN NACIONAL DE POBLACIÓN Y MIGRACIÓN)

- La presente tarjeta, deberá ser conservada en buen estado y devuelta a migraciones a su regreso, por los ciudadanos y residentes extranjeros en el país.

El cumplimiento de esta instrucción le evitará problemas y demoras innecesarias.

USO OFICIAL/For official use only

TARJETA UNICA MIGRATORIA
PARA SER COMPLETADO EN LETRA DE IMPRENTA/Please print — ARGENTINA-CHILE

1º APELLIDO / Last Name: RIVERA
2º APELLIDO / Middle name: ARIAS
NOMBRES / First Name: GUILLERMO
NACIONALIDAD / Nationality: ARGENTINO
PAIS DE NACIMIENTO / Country of birth: ARGENTINA
AÑO DE NACIMIENTO / Year of birth: 1971
SEXO / Sex: M X — F
ESTADO CIVIL / Marital status: SOLTERO / Single X — CASADO / Married — VIUDO / Widow
OCUPACION o PROFESION / Occupation or Profesion: empleado
DIRECCIÓN EN EL PAIS DE DESTINO / Address in study country: La Serena
DOCUMENTO DE VIAJE: TIPO / Document Type: Dni — Nº 22345789
TIEMPO DE ESTADIA / Estimated time of permanency: 20
MOTIVOS DEL VIAJE / Purposes of the journey: VACACIONES / Vacation X — NEGOCIOS / Business — CONFERENCIAS / Conference — SALUD / Health — OTROS / Other

POLICIA INTERNACIONAL DE CHILE
SELLO DE ENTRADA / MIGRACIONES / SELLO DE SALIDA

INSTRUCCIONES
PRORROGA PERMISO TURISMO

Prorrogado hasta.....
Resolución.....
Firma y sello de la autoridad

REPUBLICA DE CHILE

MINISTERIO DEL INTERIOR
POLICIA INTERNACIONAL CHILE

SEÑOR PASAJERO:

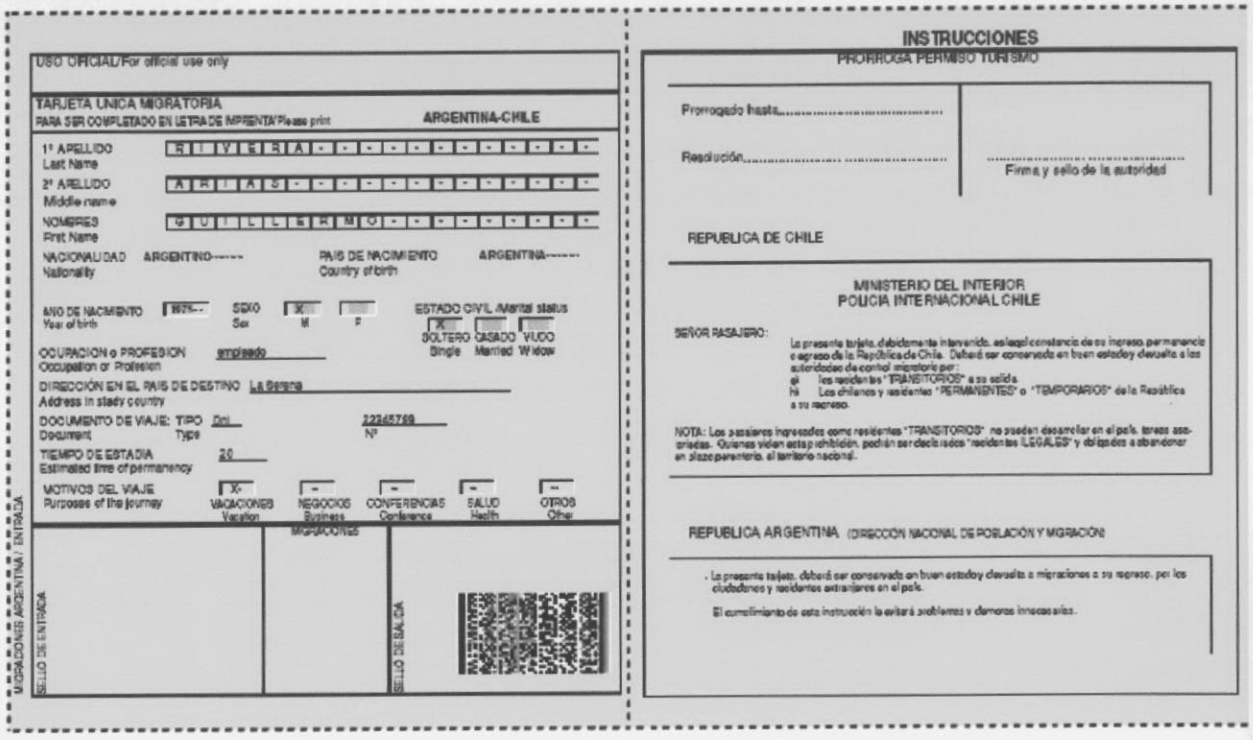
La presente tarjeta, debidamente intervenida, es legal constancia de su ingreso, permanencia o egreso de la República de Chile. Deberá ser conservada en buen estado y devuelta a las autoridades de control migratorio por:
a) los residentes "TRANSITORIOS" a su salida
b) Los chilenos y residentes "PERMANENTES" o "TEMPORARIOS" de la República a su regreso.

NOTA: Los pasajeros ingresados como residentes "TRANSITORIOS" no pueden desarrollar en el país, tareas asociadas. Quienes violen esta prohibición, podrán ser declarados "residentes ILEGALES" y obligados a abandonar en plazo perentorio, el territorio nacional.

REPUBLICA ARGENTINA (DIRECCIÓN NACIONAL DE POBLACIÓN Y MIGRACIÓN)

- La presente tarjeta, deberá ser conservada en buen estado y devuelta a migraciones a su regreso, por los ciudadanos y residentes extranjeros en el país.

El cumplimiento de esta instrucción le evitará problemas y demoras innecesarias.



USO OFICIAL/For official use only

TARJETA UNICA MIGRATORIA
PARA SER COMPLETADO EN LETRA DE IMPRENTA/Please print — ARGENTINA-CHILE

1º APELLIDO / Last Name: R I V E R A
2º APELLIDO / Middle name: A R I A S
NOMBRES / First Name: G U I L L E R M O
NACIONALIDAD / Nationality: ARGENTINO------
PAIS DE NACIMIENTO / Country of birth: ARGENTINA------
AÑO DE NACIMIENTO / Year of birth: 1975--
SEXO / Sex: M X F
ESTADO CIVIL / Marital status: SOLTERO / Single X; CASADO / Married; VIUDO / Widow
OCUPACION o PROFESION / Occupation or Profesion: empleado
DIRECCIÓN EN EL PAIS DE DESTINO / Address in study country: La Serena
DOCUMENTO DE VIAJE: TIPO / Document Type: Dni — Nº: 12345789
TIEMPO DE ESTADIA / Estimated time of permanency: 20
MOTIVOS DEL VIAJE / Purposes of the journey: VACACIONES / Vacation X-; NEGOCIOS / Business -; CONFERENCIAS / Conference -; SALUD / Health -; OTROS / Other --

MIGRACIONES ARGENTINA / ENTRADA
SELLO DE ENTRADA
MIGRACIONES
SELLO DE SALIDA

INSTRUCCIONES
PRORROGA PERMISO TURISMO

Prorrogado hasta.....
Resolución.....
Firma y sello de la autoridad

REPUBLICA DE CHILE

MINISTERIO DEL INTERIOR
POLICIA INTERNACIONAL CHILE

SEÑOR PASAJERO:

La presente tarjeta, debidamente intervenida, es legal constancia de su ingreso, permanencia o egreso de la República de Chile. Deberá ser conservada en buen estado y devuelta a las autoridades de control migratorio por:
a) los residentes "TRANSITORIOS" a su salida.
b) Los chilenos y residentes "PERMANENTES" o "TEMPORARIOS" de la República a su regreso.

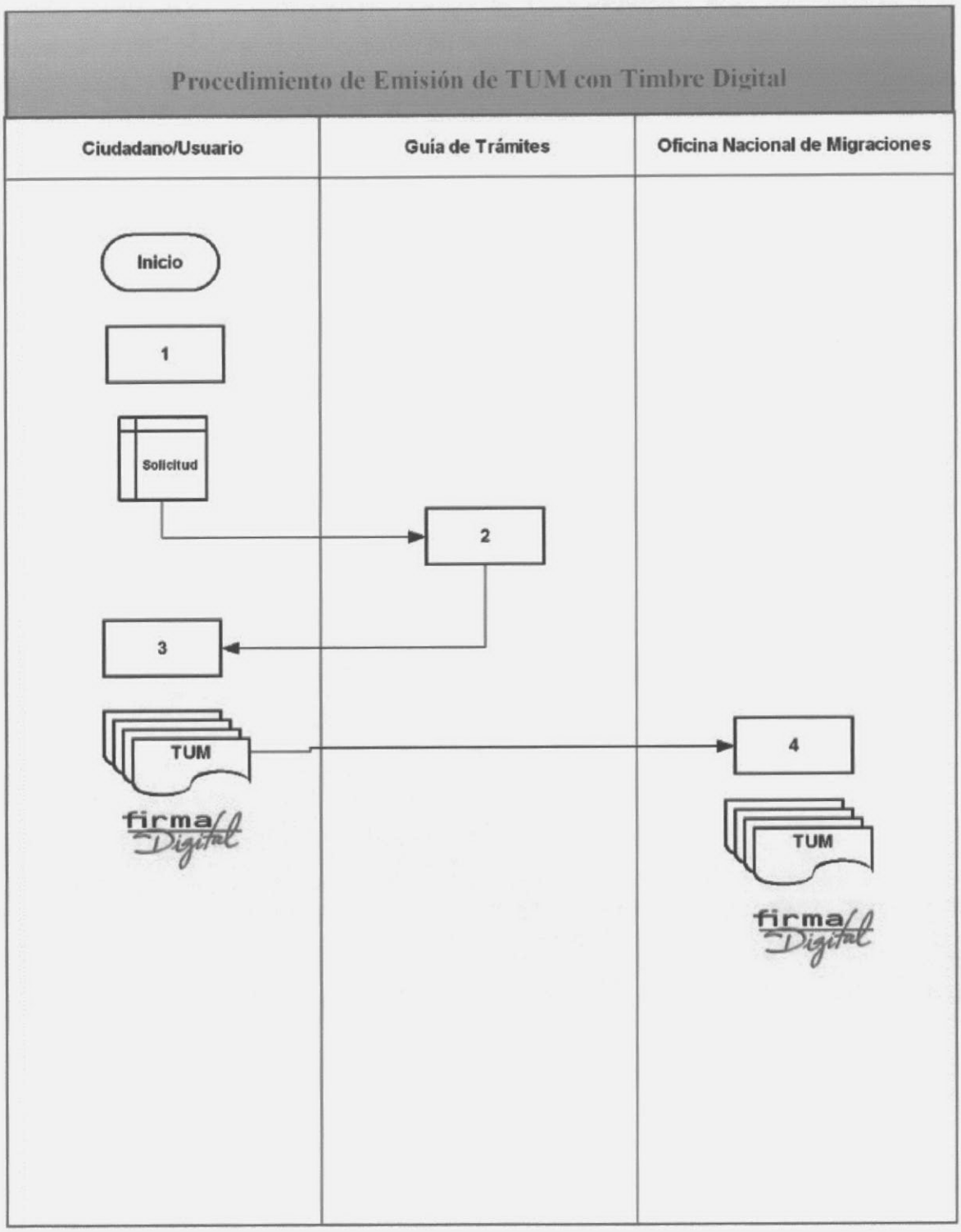
NOTA: Los pasajeros ingresados como residentes "TRANSITORIOS" no pueden desarrollar en el país, tareas asociadas. Quienes violen esta prohibición, podrán ser declarados "residentes ILEGALES" y obligados a abandonar en plazo perentorio, el territorio nacional.

REPUBLICA ARGENTINA (DIRECCION NACIONAL DE POBLACIÓN Y MIGRACIÓN)

- La presente tarjeta, deberá ser conservada en buen estado y devuelta a migraciones a su regreso, por los ciudadanos y residentes extranjeros en el país.

El cumplimiento de esta instrucción le evitará problemas y demoras innecesarias.

Diagrama del Procedimiento



D) Desarrollo de aplicaciones

Se han completado en esta etapa las tareas de desarrollo del trámite de emisión on-line de la TUM con Timbre Digital en función de las especificaciones de diseño documentadas en la sección anterior.

Cabe aclarar que la implementación de timbre digital requirió cambios en la plataforma tecnológica donde anteriormente se realizaba el trámite, por lo que fue necesario reescribir el código de generación del documento PDF de la TUM, previo a encarar el desarrollo del timbrado propiamente dicho.

Documentamos la estructura de las aplicaciones de timbrado y verificación y las tareas realizadas en pos de su desarrollo.

ESTRUCTURA DEL DESARROLLO

El desarrollo contempla dos aplicaciones bien diferenciadas:

1-El servlet de generación y timbrado de la TUM

2-La aplicación de validación del timbre

1. Servlet de generación y timbrado de la TUM

Esta aplicación, que corre del lado del servidor, es la encargada de tomar como parámetros posteados los datos ingresados por el solicitante en el formulario html y, a partir de ellos, producir on-line el documento .pdf con el contenido de la TUM y su timbre digital.

La aplicación fue desarrollada con Java (TM) Servlet Technology, incorporando un único servlet que hace invocación de clases auxiliares de firma y codificación de datos.

Un ***Servlet*** es una clase especial que sirve para generar páginas Web dinámicas. Este servlet o clase se hospeda en el servidor de aplicaciones y se invoca desde un browser enviándole una serie de parámetros conocidos

como el Request (en nuestro caso estos parámetros son los datos ingresados por el usuario en el formulario de generación de la TUM). La clase los procesa y envía una respuesta en código HTML, conocido como Response (en nuestro caso el response es un documento pdf con el contenido de la TUM y el timbre digital, generado dinámicamente).

2. Aplicación de validación de Timbre Digital

Esta aplicación standalone, se ejecuta en los desktop de los funcionarios de la Oficina Nacional de Migraciones que reciben la TUM impresa en el puesto fronterizo y deben verificar la validez e integridad 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 la TUM presentada.

PRINCIPALES TAREAS y DECISIONES DE DESARROLLO

Describimos a continuación las tareas realizadas durante el desarrollo de las dos aplicaciones descriptas en el apartado anterior, detallando las principales decisiones y condiciones funcionales que se priorizaron en el desarrollo:

1. Selección y configuración de la Plataforma Tecnológica

El desarrollo preexistente de generación de la TUM estaba formulado sobre un script en php, ejecutado del lado del servidor, que generaba una serie de cadenas postscript con la información introducida por el usuario en el formulario .html, produciendo en línea, el documento .pdf con la información de la TUM.

De cara a la introducción del timbrado digital, se evaluaron dos alternativas de desarrollo para incorporar el timbre al documento .pdf:

<table>
<tr><td colspan="2">Alternativa 1: Timbrar los datos introducidos por el usuario en el formulario html. A continuación, tomar el documento pdf generado por el script php, abrirlo nuevamente y agregarle el código de barras obtenido del proceso de timbrado.</td></tr>
<tr><td>Ventajas</td><td>Desventajas</td></tr>
<tr><td>No se requiere modificar el desarrollo preexistente</td><td>el proceso se vuelve significativamente más lento, por cuanto se necesita la reapertura, modificación y cierre del documento .pdf generado para el agregado del timbre
se requiere mantener copias auxiliares de los documentos .pdf generados en el servidor
dado que el proceso de timbrado y generación del codebar PDF 417, se genera con librerías Java, mantener el desarrollo anterior exigiría la convivencia en el servidor de una multiplicidad de plataformas (servidor apache con php, servidor de aplicaciones java, etc.)</td></tr>
<tr><td colspan="2">Alternativa 2: Reescribir el código de generación del documento .pdf a fin de que en un mismo paso se genere el formato gráfico de la TUM y se agregue el timbre digital.</td></tr>
<tr><td>Ventajas</td><td>Desventajas</td></tr>
<tr><td>mayor eficacia en el proceso de generación de la TUM (no se requiere</td><td>aumento del tiempo y complejidad de desarrollo</td></tr>
</table>

doble apertura de archivos ni copias auxiliares) mejores condiciones de mantenimiento futuro, al existir un solo desarrollo integrado y no agregados realizados en distintos lenguajes. mayor portabilidad y flexibilidad en la plataforma (portabilidad de Java) menor dispersión tecnológica	

De la lectura del análisis comparativo anterior resulta clara la elección de la segunda alternativa.

Tomada la decisión anterior, se configuró la siguiente plataforma de desarrollo:

Configuración del servidor: del lado del servidor se requiere la plataforma J2SDK 1.4 o superior y cualquier servidor de aplicaciones web que interprete Servlets Java. En particular se ha utilizado para el desarrollo el *Application Server Jakarta-Tomcat 4.1.* embebido en *JBOSS,* pero cualquier otro que cumpla los requisitos es aceptable.

Para la generación del documento .pdf y el codebar PDF417, se utiliza la API java iText, instalada en el classpath de la aplicación. Alternativamente, para contemplar la posibilidad de generación de objetos de firma PKCS#7 se ha incorporado en el servidor el paquete BouncyCastle (http://www.bouncycastle.org).

Configuración del cliente: el cliente sólo necesita un browser de Internet y Adobe Acrobat Reader 6.0 o superior.

Configuración de clientes que validan timbre digital: en las oficinas de migraciones, encargadas de validar y aceptar la TUM se necesita

además de las características del cliente, un scanner de código de barras Metrologic MS9544 con capacidad para interpretar PDF417 en el modo de procedimiento MacroPDF417 (u otro con características similares), y la aplicación de validación de timbre provista por la Unidad de Reforma y Modernización del Estado.

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

2. Selección del formato de los documentos Digitales

El desarrollo, tal como se trabajara previamente, genera la TUM en formato pdf, 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.

3. Selección de los lenguajes de desarrollo

La programación hace uso de los siguientes lenguajes:

- Servlets y Clases: *Java (J2EE)*
- Interface web: *Javascript, HTML*

4. Librerías y paquetes de clases utilizadas

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 desarrollo de la TUM con timbre digital utilizó las siguientes librerías (APIs Java), cuyo propósito y características principales describimos a continuación:

API iText : iText es un proyecto Sourceforge mantenido por una comunidad abierta de desarrolladores de software libre encabezada por Bruno Lowagie y Paulo Soarez. 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, nuestro desarrollo utiliza clases de 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 de la TUM. Esta firma es luego codificada en codebar MacroPDF417 constituyendo así el timbre digital.

5. Determinación de niveles de Seguridad y Acceso al Sistema

El servlet de generación de la TUM es de acceso público a cualquier usuario de Internet a través de la interfase web provista por la Guía de Trámites. La seguridad en la generación de la TUM se implementa mediante la generación del timbre.

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 de migraciones en la frontera con Chile, es de acceso exclusivo a usuarios con privilegios de administración u operación sobre el sistema, validados mediante esquemas de login-password.

6. 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.)* se gestionan 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 online 24x7x365.

7. 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, en el desarrollo se contemplaron las siguientes condiciones:
  1. Se excluyó la posibilidad de representar la firma como un objeto PKCS#7[PKC93] debido a que el conjunto de bytes generados es demasiado grandes (3 Kbytes aprox.).
  2. 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, se representa entonces la firma digital 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.

3. La clave pública, contenida en la firma se representa por un identificador del algoritmo en un código ASCII, seguido de los parámetros del algoritmo en un orden predefinido separados por el carácter ASCII "-".
4. El resto de datos incluidos en el timbre, se representan por código ASCII de una manera legible al ser humano.
5. Para ampliar la capacidad de codificación y no sufrir excepciones de desbordamiento por el tamaño máximo de datos se emplea el procedimiento MACRO PDF417. No se debe utilizar el procedimiento denominado Truncated PDF417, para garantizar la lectura de las marcas gráficas generadas.

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

   <<Cadena de Datos firmados>> *+ <<primer apellido ingresado como parámetro>> + "-" + <<segundo apellido ingresado como parámetro>> + "-" + <<Nombres ingresados como parámetro>> + "-" + <<Tipo de documento ingresado como parámetro>> + "-" + <<Nro. documento ingresado como parámetro>> + "-" + <<Nacionalidad ingresada como parámetro>> + "-" + <<Tiempo de estadía ingresado como parámetro>> + "-" + <<Motivo del viaje ingresado como parámetro>> +* ***<<Cadena de firma codificada en CodeBase64 (PKCS#1)>> + <<Clave pública>>***

6. La imagen del timbre generado cumple con las siguientes condiciones:
   - aspect ratio: 1:3 (relación de aspecto)
   - quiet zone: 1 cmt. (perímetro blanco)

E) Ejecución del Plan de Pruebas

Se documentan a continuación la ejecución de los casos de prueba propuestos en el Plan de Pruebas diseñado para la experiencia de Timbre Digital y documentado en el tercer informe parcial. En particular se abordaron las pruebas propuestas para las ***Fases de diseño y desarrollo*** y para la ***Fase de Implementación***. Describimos para cada una de estas fases la tabla de resultados obtenidos.

Fase de diseño y desarrollo

La ejecución de esta fase de pruebas tenía por objetivo:

- Comprobar el correcto funcionamiento de los módulos de timbrado y verificación según los requerimientos técnicos y funcionales establecidos.
- Comprobar la correcta integración modular del sistema.
- Documentar condiciones de fallo del sistema y la plataforma de hardware asociada.
- Obtener conclusiones de calidad y confiabilidad del desarrollo.

En función de ellos se realización pruebas unitarias y de integración, tanto de caja blanca como de caja negra, que permitieron verificar si el sistema cumple, tanto modularmente como en forma integrada, con las especificaciones funcionales, de compatibilidad, portabilidad, interoperabilidad y fundamentalmente de seguridad e integridad pertinentes. Se evaluaron aquí las respuestas del sistema ante casos de prueba con datos válidos e inválidos, se comprobó su funcionamiento con distintos Certificados y distintos paquetes de datos a timbrar, se realizaron comprobaciones sobre timbres válidos e inválidos, sobre timbres dañados y sobre variantes en la codificación PDF417.

Presentamos a continuación la síntesis de resultados obtenidos para las distintas corridas de casos de prueba ejecutadas.

Caso de Prueba	***Objetivo particular del testing***	***Caracterización de los conjuntos de datos de prueba***	***Resultados***
Pruebas funcionales	Testear el cumplimiento de las especificaciones funcionales de cada módulo y de la integración de los mismos.	Conjuntos de datos de entrada válidos e inválidos, tomando como parámetros correctos: Cadenas de texto en claro de 60 a 300 caracteres. Certificados de firma X.509 v3 • Certificados ONTI • Certificados AC-URME	Si bien la cadena de texto en claro a timbrar oscila entre los 100 y 150 caracteres de acuerdo a los datos ingresados en el formulario en el formulario de la TUM más parámetros especiales. Se amplio el intervalo de prueba a un rango de 60 a 300 caracteres. En todos los casos el timbrado del texto en claro se obtuvo sin problemas y no se registraron excepciones de desbordamiento. El timbre pudo ser adecuadamente generado y validado tanto con Certificados ONTI como con Certificados AC-URME a igual conjunto de extensiones de certificado configuradas.

Pruebas de compatibilidad e interoperabilidad	Evaluar compatibilidad del desarrollo con distintos tipos de TBS de certificados, distintas plataformas de ejecución, distintos modos y hardware de impresión, etc.	Generación de timbres utilizando: • Certificados ONTI • Certificados AC-URME con distintas configuraciones de restricciones críticas. • Entorno Linux, Windows 98, XP. • Keystores: PKCS11, JKS, PKCS12 • Impresión en impresoras Láser estándar, chorro de tinta.	Se comprobó la generación de Timbres con distintos tipos de TBS de certificados. En principio se detectaron algunos errores producidos por la activación de extensiones críticas en algunas configuraciones de Certificados AC-URME que deben ser consideradas a la hora de generar Certificados con finalidad de timbrado. No obstante, todo el desarrollo funcionó adecuadamente con la configuración prevista en los Certificados ONTI que son los requeridos en la puesta en producción real del entorno de timbrado. Se generaron TUMs timbradas desde distintos browser corriendo en entornos Windows 98, XP y Linux, con readers Acrobat Reader 6.0 y 7.0. En todos los casos el documento fue

			correctamente generado y el timbre debidamente validado. Como era esperable según la documentación del estándar PDF417 y pruebas realizadas en la fase de investigación preliminar, la impresión de TUMs timbrada en distintos modelos de impresora con tecnologías Laser y Chorro de Tinta operó correctamente y no se identificaron problemas al momento del reconocimiento del codebar PDF417
Pruebas de carga de trabajo	Evaluar el comportamiento del módulo frente a distintos niveles de carga de trabajo	Generación de timbres por lote: • 0 a 2 transacciones por minuto • 2 a 4 transacciones por minuto • 5 a 7 transacciones por minuto • 7 a 10 transacciones • más de 10 transacciones por minuto	Si bien no es esperable por datos históricos de volúmenes de transacciones de pedido de TUMs on-line la concurrencia de transacciones. Se evaluó la capacidad de respuesta del servidor con altos niveles de concurrencia hasta más de 10 transacciones por minuto.

		Datos a timbrar: estándar de aplicación. Cadena de 153 bytes ISO 8002 Certificado X509 v3. – ONTI Algoritmo de firma: sha1withrsa	En todos los casos, los tiempos de respuesta del servidor fueron satisfactorios (manteniéndose dentro de los 10 segundos sin contemplar latencia por comunicaciones o apertura del reader), no manifestándose excepciones por concurrencia transaccional.
Pruebas lingüísticas	Evaluar el correcto timbrado y verificación de conjuntos de datos con caracteres propios del idioma español-latinoamericano.	Generación de timbres sobre conjuntos de datos que incluyan caracteres especiales tales como letra ñ, signos de interrogación y admiración, barras, diéresis, etc.	En base a las pruebas realizadas se identificó la configuración adecuada del conjunto de parámetros del scanner que permite la correcta decodificación de caracteres especiales del idioma castellano, tales como letra ñ y demás.
Pruebas de seguridad e integridad	Testear la inviolabilidad del timbre	• Timbres alterados en su conjunto de texto en claro • Timbres rotos • Timbres copiados • Timbres con firma adulterada • Timbres con clave pública adulterada • Timbres con certi-	El algoritmo de verificación detectó correctamente todos los casos en que se alteró alguno de los datos incluidos en el timbre: texto en claro, clave pública, certificados o firma. Las pruebas de recu-

		ficados no válidos, revocados, o autoafirmados.	peración de timbres dañados (imagen codebar PDF417 dañada) no resultaron satisfactorias. No obstante, se decidió tolerar este nivel de fallas en pos de no tener que elevar el Nivel de Corrección de Errores a 5 y degradar significativamente por ello la capacidad de codificación de información en el timbre.

Fase de implementación

Esta fase acompañó la etapa de implementación y puesta a punto del circuito de manera integral; y tuvo por objetivo lograr la aceptación final del desarrollo por parte del organismo usuario. Se realizaron en esta instancia pruebas de usabilidad y de sistemas, de caja negra en el entorno de producción, para verificar su correcta utilización por parte de los usuarios y la correcta respuesta del desarrollo ante situaciones de uso no previstas en las fases previas.

Caso de Prueba	***Objetivo particular del testing***	***Caracterización de los conjuntos de datos de prueba***	***Resultados***
Pruebas funcionales	Testear el cumplimiento de las especificaciones funciona-	Conjuntos de datos de entrada válidos e inválidos, tomando	En todos los casos el timbrado del texto en claro se obtuvo

	les del desarrollo.	como parámetros correctos: • Cadenas de texto en claro en simbología ASCII en longitudes de 100 a 150 caracteres. • Certificados de firma X.509 v3 - Certificados ONTI	sin problemas y no se registraron excepciones de desbordamiento, ni por errores de lingüística. El timbre pudo ser adecuadamente generado y validado tanto con Certificados ONTI.
Pruebas de compatibilidad e interoperabilidad	Evaluar el funcionamiento del sistema en distintas plataformas de ejecución.	Generación de timbres utilizando: •Certificados ONTI •Entorno Linux y Windows 98, XP. •Browser IE 5.0 o superior, Mozila, Netscape Communicator. •Keystores: PKCS12 •Representación de certificados .pfx, •Impresión en impresoras	Se generaron TUMs timbradas desde los distintos browsers corriendo en entornos Windows 98, XP y Linux, con readers Acrobat Reader 6.0 y 7.0. En todos los casos el documento fue correctamente generado y el timbre debidamente validado. Los Certificados tomados desde un Keystore PKCS12 operan correctamente en el entorno de producción.

		Láser estándar, chorro de tinta.	
Pruebas lingüísticas	Evaluar el correcto timbrado y verificación de conjuntos de datos con caracteres propios del idioma español-latinoamericano.	Generación de timbres sobre conjuntos de datos que incluyan caracteres especiales tales como letra ñ, signos de interrogación y admiración, barras, diéresis, etc.	Con la configuración adecuada del conjunto de parámetros del scanner identificada en la fase de desarrollo no se detectaron problemas de decodificación de caracteres especiales del idioma castellano, tales como letra ñ y demás.
Pruebas de seguridad e integridad	Testear la inviolabilidad del timbre	• Timbres alterados • Timbres rotos • Timbres copiados	Se demostró ante los usuarios las adecuadas características de seguridad del sello.
Pruebas de accesibilidad e interfase	Comprobar la facilidad de uso de la interfase de usuario.	Conjuntos de datos válidos e inválidos que permitan probar todos los cursos de acción e interacción con el usuario del sistema. •Ventanas de opción •Ventanas de información •Eventos asocia-	Como resultado de esta etapa se obtuvo una serie de recomendaciones de mejora sugeridas por los funcionarios de la Oficina Nacional de Migraciones que atienden fundamentalmente a cambios en la documentación del usuario y en la visibilidad de la firma

		dos a botones •Mensajes de confirmación •Mensajes de alerta y error •Otros.	y datos firmados al momento de la validación del timbre. La factibilidad de incorporación de dichas mejoras serán evaluadas por esta Consultoría de acuerdo a los tiempos previstos para el mantenimiento del desarrollo.

El resultado de estas comprobaciones y mediciones debe condujo a la conclusión final de que el sistema cumple con niveles de calidad y confiabilidad aceptables en términos de identificación de errores, tolerancia a fallos y vulnerabilidades.

F) Implementación

Concretada la etapa de pruebas se emprendió la implementación efectiva del sistema de emisión on-line de la TUM con Timbre Digital en el ámbito de la Oficina Nacional de Migraciones.

Implementar un sistema, no implica únicamente instalar el software y capacitar al personal, sino adecuar la estructura organizacional, los procesos administrativos y operativos, los controles, las políticas, los procedimientos y hasta la propia aplicación informática a los cambios que la introducción del nuevo sistema acarrea.

Teniendo en cuenta lo dicho y dadas las características de experiencia piloto que este desarrollo posee, es importante definir los objetivos y alcances de la implantación, por cuanto aportará a la comprensión de las actividades realizadas y su proyección futura.

Objetivo: Iniciar el funcionamiento del trámite on-line de emisión de la TUM con Timbre Digital desde la Guía de Trámites del Gobierno de la Provincia de Mendoza.

Alcance: La implementación inicial aspira a la puesta en marcha de la dinámica de sistemas, logrando el mejor impacto sobre las personas y procesos involucrados.

En esta instancia se realizaron las siguientes actividades:

1-Selección del modelo de implementación

Dado que la introducción de timbre a la TUM constituye un agregado adicional a los mecanismos de seguridad implementados en el trámite anterior y que no afecta las características del mismo, se decidió que la implementación actual reemplazara por completo a la implementación previa. Se hicieron no obstante, las consideraciones pertinentes con respecto a los alcances legales de los certificados de firma digital involucrados en el proceso (Certificados emitidos por la ONTI) y la característica de experiencia preliminar de la implementación de timbre.

2-Asignación de recursos y responsables

Se designaron 2 empleados de la Oficina Nacional de Migraciones, que se desempeñan en el puesto fronterizo, como responsables de la operación inicial del sistema. Estas personas se desempeñaron durante la etapa de implementación, con el soporte permanente del equipo de desarrollo y bajo el control de la responsable de la Guía de Trámites, Ing. Flavia Videla.

Para el proceso de implantación inicial se dispuso de los siguientes recursos, además del servidor donde corre la aplicación.

- 1 PC con sistema operativo Windows XP.
- 1 Scanner Metrologic MS9544
- Certificado Digital de timbrado.

Salvo el Scanner que fue provisto en préstamo por la Unidad de Reforma, el resto del equipamiento fue provisto por la Oficina Nacional de Migraciones.

3-Provisión del Certificado de firma digital para la generación del Timbre

A través de la Autoridad de Registro de la ONTI, constituida en la Unidad de Reforma y Modernización del Estado, se proveyó de un Certificado Digital de servidor con capacidades de firma digital a nombre de la Oficina Nacional de Migraciones. Este certificado fue instalado en el servidor de timbrado para la generación del timbre. La clave pública correspondiente al mismo fue incluida en la aplicación de validación de timbre y distribuida a los usuarios con la misma.

4-Capacitación de responsables

Se realizó un entrenamiento intensivo de los responsables 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 la Oficina de la Unidad de Reforma y Modernización del Estado durante media jornada. Por la simplicidad operativa de la aplicación de validación de timbre, no requirió documentación específica, distinta de la ayuda incluida en la aplicación.

5-Puesta en marcha del proceso emisión de TUMs, Timbrado y Validación

Una vez capacitados los responsables se inició el proceso de instalación y configuración preliminar del sistema. La aplicación de generación de TUMs timbradas fue instalada en el servidor de producción y se vinculó a los accesos previstos en la Guía de Trámites. En la Oficina Nacional de Migraciones (puesto fronterizo) se instaló la aplicación de validación y se configuraron los parámetros del Scanner por parte de los Técnicos de la Unidad de Reforma y Modernización del Estado. Se ejecutaron en esta etapa las pruebas previstas para la Fase de Implementación, cuyos resultados se documentaron en la sección anterior.

6-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, la interacción permanente de los expertos del proyecto de firma digital con los responsables designados para la tarea, aportó a identificar necesarios ajustes sobre el desarrollo de la herramienta informática y el circuito operativo.

G) Evaluación de la Experiencia

Describimos a continuación el sistema de evaluación de resultados que se aplicará al e-trámite de emisión de la TUM con timbre digital. 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.

Es importante señalar que el diseño respeta el enfoque del modelo general de evaluación de resultados, propuesto para el proyecto de firma digital y la infraestructura PKI, con un 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 piloto TUM 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 la Oficina Nacional de Migraciones – 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 TUM emitidas válidas / Total de TUMs emitidas mensuales
- Nro. de TUMs emitidas rechazadas / Total de TUMs 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 TUMs emitidas mensuales
- Cant. de verificaciones de certificación mensuales
- % de utilización de servicios (sobre el total de actores involucrados)

Calificación ponderada final

.....