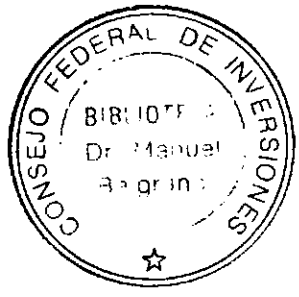
GOBIERNO DE MENDOZA
SECRETARÍA ADMINISTRATIVA LEGAL Y TÉCNICA
UNIDAD DE REFORMA DEL ESTADO

e-firma/mza

"Análisis de factibilidad para la implementación de Firma Digital"

Primer Informe de Etapa



Consejo Federal de Inversiones

CONSULTOR: LIC. PABLO GUILLERMO LIOY

INDICE

Primer Informe de Etapa

e-firma/mza

"Análisis de factibilidad para la implementación de Firma Digital"

Introducción

En el marco del proyecto e-firma/mza y de acuerdo con el Plan de Actividades propuesto, se presentan a continuación, como Primer Informe de Etapa, el desarrollo de las siguientes actividades:

1. **Realizar un estudio general de factibilidad** para introducir la firma digital en el ámbito del Gobierno de la Provincia de Mendoza.
    - Análisis de Factibilidad Operativa
    - Análisis de Factibilidad Económica-Financiera
    - Análisis de Factibilidad Legal

2. **Determinación de estructuras técnicas aplicables** de soporte para la PKI (*Public Key Infrastructure)*
    - Análisis de Factibilidad Técnica
    - Definición de la Arquitectura de Soporte
    - Definición de necesidades a cubrir por la PKI
    - Presupuesto Estimado
    - Determinación de la arquitectura más adecuada a la vista del análisis de requerimientos

Idea Guía

Crear las condiciones necesarias para introducir las tecnologías criptográficas pertinentes para el soporte de la Firma Electrónica y sus servicios asociados. Con ello, a futuro, se espera poder facilitar el camino del desarrollo de proyectos reales de teleadministración y de proyectos que agilicen multitud de tramitaciones internas de la Administración Pública de la Provincia de Mendoza, llegando a disponer de sus propios servicios de Autoridad de Certificación y de Registro, con una estructura de certificación coherente.

Objetivo General

Estudio de factibilidad y Diseño de Infraestructura (PKI) tendiente a instrumentar la firma digital en el ámbito del Gobierno de la Provincia de Mendoza.

Objetivos Específicos:

- Determinar factibilidad para la implementación de tecnologías de firma digital que fomenten el ahorro y la celeridad en los procedimientos públicos provinciales.

- Diseñar una PKI de propósito general, para la emisión y gestión de certificados digitales que permitan la generación de firmas digitales y el cifrado en procesos internos, y que permitan a los ciudadanos y las empresas relacionarse con la Administración a través de Internet, en un entorno seguro.

- Proponer un marco regulatorio compatible pero adecuado a las circunstancias particulares de la provincia.

- Identificar ámbitos de aplicación de acuerdo con la demanda ciudadana local.

Alcance

El ámbito de los procesos susceptibles de generar ahorros, mayor efectividad operativa y acercamiento al ciudadano a través de la utilización de tecnologías de firma digital dentro de la Administración Pública Provincial.

Conceptos Básicos[1]

SIGLAS

PKI: Public Key Infraestructure – Infraestructura de Clave Pública

AC / CA / ACL: Autoridad de Certificación Licenciada.

CL: Certificador Licenciado

CRL: Lista de Certificados Revocados.

CVC: Ciclo de vida de certificados

HSM: Módulo criptográfico en hardware

[1] Ley Nacional de Firma Digital N°25.506

Decreto Reglamentario N°2628/2002 Reglamentación de la Ley N° 25.506

J2EE: Java 2 Enterprise Edition

DBA: Administrador de Base de Datos

ODBC: Open DataBase Client.

Firma Electrónica: Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizados por el signatario como su medio de identificación, que carezca de algunos de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez (artículo 5°, Ley N° 25.506).

Firma digital: 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 ésta 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.

Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes (artículo 2°, Ley N° 25.506).

Documento Digital o Electrónico: Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte: utilizado para su fijación, almacenamiento archivo. Un documento digital también satisface el requerimiento de escritura (artículo 6°, Ley N° 25.506).

Infraestructura de clave pública (PKI): una infraestructura de clave pública o PKI (de *Public Key Infrastructure*) es el conjunto de elementos de seguri-

dad y sistemas criptográficos que permiten el establecimiento de los más altos niveles de seguridad de una forma flexible y con un coste de gestión razonablemente bajo. Gestionando claves y certificados a través de una PKI, una organización posibilita la utilización de servicios de firma electrónica y cifrado en una amplia variedad de aplicaciones y establece y mantiene un entorno de red seguro.

Certificado Digital: Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular (artículo 13, Ley N° 25.506).

Certificador Licenciado: Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante.

La actividad de los certificadores licenciados no pertenecientes al sector público se prestará en régimen de competencia. El arancel de los servicios prestados por los certificadores licenciados será establecido libremente por éstos (artículo 17, Ley N° 25.506).

Política de Certificación: Conjunto de criterios que indican la aplicabilidad de un certificado a un grupo de usuarios en particular o a un conjunto de aplicaciones con similares requerimientos de seguridad. En inglés Certification Policy (CP).

Manual de Procedimientos: Conjunto de prácticas utilizadas por el certificador licenciado en la remisión y administración de los certificados. En inglés Certification Practice Statement (CPS).

Plan de Seguridad: Conjunto de políticas, prácticas y procedimientos destinados a la protección; de los recursos del certificador licenciado.

Plan de Cese de Actividades: conjunto de actividades a desarrollar por el certificador licenciado en caso de finalizar la prestación de sus servicios.

Plan de Contingencias: Conjunto de procedimientos a seguir por el certificador licenciado ante situaciones de ocurrencia no previstas que comprometan la continuidad de sus operaciones.

Lista de certificados revocados: Lista de certificados que han sido dejados sin efecto en forma permanente por el Certificador Licenciado, la cual ha sido firmada digitalmente y publicada por el mismo.

En inglés Certificate Revocation List (CRL).

Certificación digital de fecha y hora: Indicación de la fecha y hora cierta, asignada a un documento o registro electrónico por una tercera parte confiable y firmada digitalmente por ella.

Terceras partes confiables: Entidades independientes que otorgan seguridad y confiabilidad al manejo de la información.

Proveedor de servicios de certificación digital: Entidad que provee el servicio de emisión y administración de certificados digitales.

Homologación de dispositivos de creación y verificación de firmas digitales: Proceso de comprobación efectuado para establecer la adecuación de los dispositivos a requerimientos mínimos establecidos.

Certificación de sistemas que utilizan firma digital: Proceso de comprobación efectuado para establecer la adecuación de un sistema o aplicación a requerimientos mínimos establecidos.

Suscriptor o Titular de certificado digital: Persona a cuyo nombre se emite un certificado y posee una clave privada que se corresponde con la clave pública contenida en el mismo.

Procedimiento de verificación: proceso utilizado para determinar la validez de una firma digital. Dicho proceso debe considerar al menos:

- que dicha firma digital ha sido creada durante el período de validez del certificado digital del firmante;
- que dicha firma digital ha sido creada utilizando los datos de creación de firma digital correspondientes a los datos de verificación de firma digital indicados en el certificado del firmante
- la verificación de la autenticidad y la validez de los certificados involucrados.

Datos de creación de firma digital: datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear su firma digital.

Datos de verificación de firma digital: datos únicos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma digital, la integridad del documento digital y la identidad del firmante.

Dispositivo de creación de firma digital: dispositivo de hardware o software técnicamente confiable que permite firmar digitalmente.

Dispositivo de verificación de firma digital: dispositivo de hardware o software técnicamente confiable que permite verificar la integridad del documento digital y la identidad del firmante.

Técnicamente confiable: cualidad del conjunto de equipos de computación, software, protocolos de comunicación y de seguridad y procedimientos administrativos relacionados que cumplan los siguientes requisitos:

Clave criptográfica privada: En un criptosistema asimétrico es aquella que se utiliza para firmar digitalmente.

Clave criptográfica pública: En un criptosistema asimétrico es aquella que se utiliza para verificar una firma digital.

Integridad: Condición que permite verificar que una información no ha sido alterada por medios desconocidos o no autorizados.

Criptosistema asimétrico: Algoritmo que utiliza un par de claves, una clave privada para firmar digitalmente y su correspondiente clave pública para verificar dicha firma digital.

Antecedentes

Las redes abiertas como Internet revisten cada vez mayor importancia para la comunicación mundial. Esas redes permiten una comunicación interactiva entre interlocutores que no necesariamente han entablado previamente relación alguna. Además, ofrecen nuevas posibilidades empresariales, creando herramientas que mejoran la productividad y reducen los costos, así como nuevas formas de llegar al cliente. Las redes están siendo utilizadas por empresas que desean aprovechar los nuevos tipos de actividad y nuevas formas de trabajo, como el teletrabajo y los entornos virtuales compartidos. También las administraciones públicas las utilizan en su gestión interna y en su interacción con empresas y ciudadanos. El comercio electrónico brinda al país una excelente oportunidad para avanzar en su integración económica con las naciones del resto del mundo.

Para aprovechar todas estas posibilidades es necesario disponer de un entorno seguro en relación con la autenticación digital. En la práctica existen diversos métodos para firmar documentos digitalmente, que van desde algunos muy sencillos (por ejemplo, insertar la imagen escaneada de una firma manuscrita en un documento creado con un procesador de texto) que no permiten otorgarle validez jurídica a la firma, a otros muy avanzados (por ejemplo, la firma digital que utiliza la "criptografía de clave pública"), que sí lo permiten. Para tener validez jurídica, las firmas digitales deben permitir verificar tanto la identidad del autor de los datos (*autenticación de autoría*), como comprobar que dichos datos no han sufrido alteración desde que fueron firmados (*integridad*).

La explosión del comercio electrónico va de la mano con normas legales de seguridad, confiabilidad y protección al consumidor. En este sentido el uso de la firma digital es uno de los pilares sobre los que se asienta el sistema propuesto.

Al facilitar la autenticación a distancia entre partes que no necesariamente se conocen previamente, la firma digital constituye el mecanismo esencial para proveer seguridad y desarrollar la confianza en las redes abiertas. Esto le otorga un rol estratégico en el desarrollo del comercio electrónico en Internet.

El comercio electrónico no es el único beneficiario de la firma digital. Actualmente las empresas y los organismos públicos de nuestro país están atorados de grandes cantidades de documentos en soporte papel que ocupan un significativo y costoso espacio de archivo en sus oficinas y que dificultan su informatización, lo que da como resultado un acceso a la información más lento y costoso. La implementación de modernos sistemas informáticos nos permitiría acceder a documentos a distancia y a la información en forma inmediata, dando lugar por ejemplo a nuevas modalidades de desempeño laboral como ser el tele-trabajo ("tele-commuting").

Y es aquí donde se produce el mayor beneficio de la utilización de la firma digital: tanto estas nuevas modalidades de trabajo como el incremento en la velocidad de circulación de la información que permite hacer factible el documento digital para que las organizaciones ofrezcan un mejor nivel de servicios a sus clientes y simultáneamente reduzcan sus costos. Es indudable que el Estado tiene un rol de liderazgo que cumplir en la incorporación de la cultura digital en la sociedad Argentina.

Fundamentos Tecnológicos.

Los avances en disciplinas del campo de las Tecnologías de la Información y de las Comunicaciones se han complementado y potenciado, tanto en sus capacidades técnicas estructurales como en los contenidos que constituyen su objeto.

En cuanto a las capacidades técnicas estructurales, las posibilidades físicas para la conservación y procesamiento de información revelan un avan-

ce en apariencia ilimitado, tanto en los volúmenes como en la velocidad de los procesos.

Los sistemas operativos y los programas de aplicación a su vez han incrementado su eficiencia en forma equivalente, facilitando la administración de cada vez mayores volúmenes de datos a velocidades aptas para obtener resultados en tiempo útil.

Podemos observar un ejemplo de esta cooperación entre los dispositivos físicos y lógicos de un sistema informático, en los desarrollos de software que permiten el almacenamiento de mayores volúmenes de información reduciendo el espacio físico requerido para igual cantidad de datos, mediante algoritmos de compactación que hoy son de aplicación común para cualquier usuario.

Sin embargo, el salto cualitativo en orden a la significación social, económica, política y jurídica de estas tecnologías se produce cuando las computadoras abandonan su estado de relativo aislamiento, de disposición de los datos almacenados en su propia memoria, y son conectadas a una red global de comunicación que les permite acceder y procesar información contenida virtualmente en cualquier otra computadora ubicada en un lugar remoto del planeta.

En este punto cualitativo, el contenido de las tecnologías de información han pasado de los usos restringidos para los que se originaron, a contener casi todo el conocimiento adquirido en todas las actividades desarrolladas por el hombre.

Estos enunciados son conocidos ampliamente. Pero se insiste en ellos, por que debemos comprender la magnitud de estos cambios y el impacto que están y van a seguir generando en nuestra organización social, en nuestra forma de vida, en nuestra capacidad para trabajar y producir, para contratar y también esta llamado a tener un fuerte impacto en nuestras libertades individuales.

Compatibilización

Es imprescindible que el marco legal y técnico que adopte el país para el desarrollo de la firma digital sea compatible con el que ya existe en otros países. La aplicación de criterios legales diferentes a los aplicables en otros países en cuanto a los efectos legales de la firma digital, y cualquier diferencia en los aspectos técnicos en virtud de los cuales las firmas digitales son consideradas seguras, resultará perjudicial para el desarrollo futuro del comercio electrónico nacional y, por consiguiente, para el crecimiento económico del país y su incorporación a los mercados internacionales, cada vez más globalizados.

El tema puede enfocarse en primer análisis, desde dos puntos de vista:

a) En el derecho público, en nuestras relaciones con el estado y en el funcionamiento mismo de las instituciones estatales, y
b) En el derecho privado, en las contrataciones telemáticas en general y particularmente en el comercio electrónico que ha alcanzado volúmenes tan importantes económicamente, como significativos en la seguridad jurídica de que carecen.

En el sector público, la necesidad de administrar las cantidades enormes y crecientes de presentaciones administrativas, expedientes, autorizaciones estatales y los más diversos trámites necesarios, -a veces-, para el funcionamiento institucional y social, han llevado a la informatización gradual de los procesos administrativos.

En la legislación comparada se observa que los países en general han comenzado el proceso de utilización de la firma digital, mediante normativas orientadas al sector público, generando la infraestructura estatal de firma digital. La finalidad es expresada gráficamente en los decretos emitidos, diciendo que este proceso deberá conducir a la despapelización de la administración pública.

Anexo I

e-firma/mza

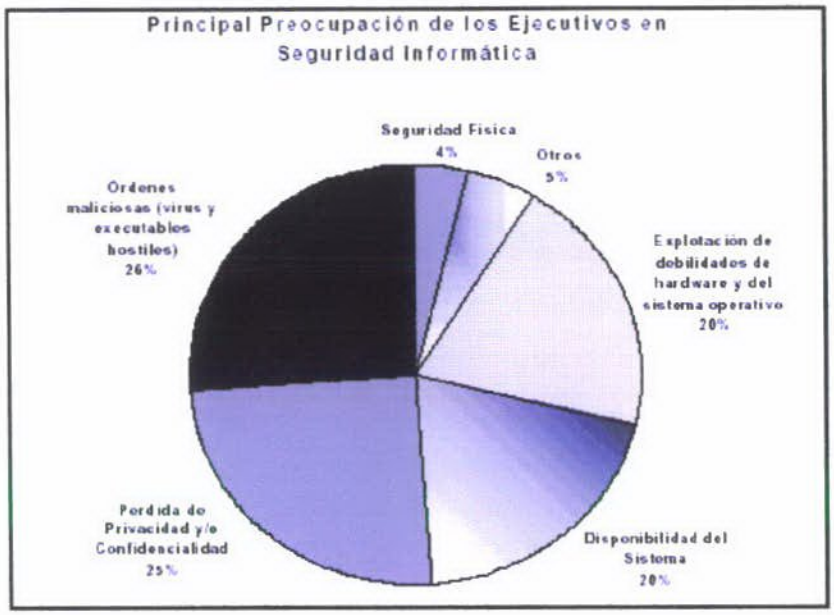
Análisis de Factibilidad Operativa

En este subestudio es preciso analizar si la Administración Pública provincial se encuentra en condiciones de convivir con una infraestructura de firma Digital y sus servicios asociados, es decir, de qué forma planeamos que su organización y su personal se adapten satisfactoriamente a los cambios necesarios para que el nuevo sistema funcione con éxito. Por otro lado resulta importante plantear las condiciones que deben cumplirse y las acciones que deben desarrollarse para lograr con alto grado de seguridad la funcionalidad u operatividad del modelo a plantear. En tal sentido a continuación se presenta una enumeración de factores que son considerados importantes para la consecución efectiva de los objetivos fijados.

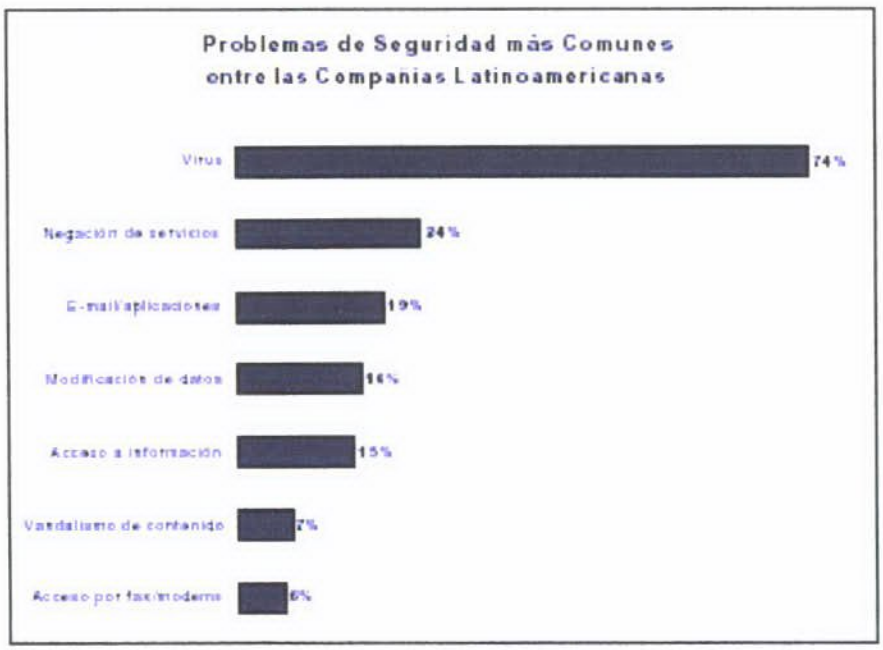
1. Cambio, Seguridad y Garantías

Es cada vez mayor la preocupación sobre los niveles de seguridad a los que deben llegar los sistemas informáticos de empresas, administración gubernamental y personas naturales. Si bien estos problemas no son nuevos, hasta ahora sus riesgos se encontraban medianamente controlados. Debemos tener en cuanta aquí que *"la seguridad no es un bien en sí mismo, pero que su carencia se paga caro"*

Con el movimiento global generado por internet el conjunto de riesgos en materia de seguridad aumentó considerablemente a través de nuevas formas y profundizó las ya existentes. En tal sentido las preocupaciones de los niveles gerenciales han sido:



Fuente: Infosecurity



Dentro del espectro de problemas relacionados con la seguridad son los virus los que ocupan el primer lugar, pero en segundo lugar se encuentra la propia negación de servicios que otro sentido también resulta muy desfavorable y nociva.

Para menguar las consecuencias de estos riesgos, las instituciones y empresas han puesto en práctica una serie de herramientas y aplicaciones de seguridad buscando prevenir los daños potenciales a sus actividades B2C (Business to Commerce) y B2B (Business to Business). Dichas medidas están orientadas principalmente a garantizar el funcionamiento seguro de las distintas partes de los sistemas informáticos (identidad de usuarios, seguridad de canales de conexión, etc)

Otro tanto ha ocurrido con el desarrollo evolutivo de los sistemas de información y de las TIC´s, este ha determinado un cambio en la concepción de las relaciones entre los individuos y las organizaciones en todo el mundo. Una sustentable aplicación de las nuevas tecnologías necesariamente implica un cambio de mentalidad con argumentos firmes que venzan la resistencia.

Concretamente, cuando hablamos de tecnologías de Firma Digital, no solo consideramos nuevas formas de prestar servicios; también consideramos la posibilidad de crear nuevos servicios. La diferencia que introduce este cambio impacta directamente en la relación administrativa y de prestación de servicios y viene dada principalmente por la sustitución del soporte tradicional por soportes electrónicos.

Dicho cambio, presenta matices tales como la superposición de algunos mecanismos de garantías que son necesarios para corregir correctamente las relaciones nuevas con las ya existentes. Proverbialmente los documentos necesitan garantías de no falsificación y privacidad, así como también contienen fechas y firmas.

Dentro del espectro de problemas relacionados con la seguridad son los virus los que ocupan el primer lugar, pero en segundo lugar se encuentra la propia negación de servicios que otro sentido también resulta muy desfavorable y nociva.

Para menguar las consecuencias de estos riesgos, las instituciones y empresas han puesto en práctica una serie de herramientas y aplicaciones de seguridad buscando prevenir los daños potenciales a sus actividades B2C (Business to Commerce) y B2B (Business to Business). Dichas medidas están orientadas principalmente a garantizar el funcionamiento seguro de las distintas partes de los sistemas informáticos (identidad de usuarios, seguridad de canales de conexión, etc)

Otro tanto ha ocurrido con el desarrollo evolutivo de los sistemas de información y de las TIC´s, este ha determinado un cambio en la concepción de las relaciones entre los individuos y las organizaciones en todo el mundo. Una sustentable aplicación de las nuevas tecnologías necesariamente implica un cambio de mentalidad con argumentos firmes que venzan la resistencia.

Concretamente, cuando hablamos de tecnologías de Firma Digital, no solo consideramos nuevas formas de prestar servicios; también consideramos la posibilidad de crear nuevos servicios. La diferencia que introduce este cambio impacta directamente en la relación administrativa y de prestación de servicios y viene dada principalmente por la sustitución del soporte tradicional por soportes electrónicos.

Dicho cambio, presenta matices tales como la superposición de algunos mecanismos de garantías que son necesarios para corregir correctamente las relaciones nuevas con las ya existentes. Proverbialmente los documentos necesitan garantías de no falsificación y privacidad, así como también contienen fechas y firmas.

Tales garantías, son función del contexto organizacional de la Administración pública y de la información involucrada:

- **Autenticación/Control de acceso:** debemos asegurar que las partes implicadas son quienes dicen ser.
- **Información Íntegra:** la misma información que se está recibiendo debe ser la que se envió.
- **Información Confidencial:** sólo podrá ser vista por las personas que tengan autorización.
- **No repudio:** imposibilidad de negar que la información ha sido enviada por el remitente y recibida por el destinatario.
- **Auditabilidad:** identificación y rastreo del historial de acciones realizadas por un usuario dentro de un sistema informático con acceso a través de certificados, en especial al incorporar el estampillado de tiempo, que añade la fecha y hora de las acciones realizadas en forma confiable.
- **Acuerdo de claves secretas:** asegura la confidencialidad de la información que se intercambia entre las partes, esté firmada o no, como las realizadas a través de sitio seguro.

Resulta difícil ignorar el valor que en la actualidad s e da a la disponibilidad de información fidedigna y oportuna. Las ventajas comparativas de tenerla son inigualables. Toda vez que las garantías anteriores se cumplan, podremos transponer viejos procedimientos y concepciones hacia un modelo de servicio público más eficiente y enfocado en el ciudadano. Para lograrlo es necesario comprender la necesidad de una apropiada estandarización e identificación de personas y organizaciones por medios electrónicos. Es preciso estar atentos a los avances tecnológicos y adecuar las estructuras orgánicas involucradas para que funcionen aprovechando para beneficio propio y común todas sus ventajas.

2. Condiciones de Certificación Digital

En Latinoamérica la introducción de la tecnología de certificación ha sido lenta; el incremento de la penetración de internet no ha desarrollado hasta el momento, la cantidad de transacciones suficientes como para demandar el uso masivo de certificados digitales. De la masa crítica de usuarios conectados a la red, sólo un porcentaje menor realiza transacciones comerciales. Si bien el motivo de esta conducta es esencialmente un tema de falta de confianza, también se encuentran involucrados factores culturales de hábitos y costumbres.

Por otro lado, los riesgos reales involucrados no son de conocimiento popular, generalmente las personas están concientes del fraude por robo del número de tarjeta de crédito; pero ignoran peligros latentes como por ejemplo son la suplantación de identidades y la violación de correos electrónicos, la Provincia de Mendoza no es ajena a esta situación.

De manera de superar los problemas que genera la ausencia del conjunto de garantías, que hemos definido como necesarias para la exitosa introducción de la tecnología de firma Digital, debemos recurrir a los mecanismos criptográficos. Dichos mecanismos utilizan funciones matemáticas que permiten cifrar y descifrar la información.

Los métodos actuales de criptografía disponibles no sustentan la seguridad buscada para este tipo de procedimientos en el secreto del algoritmo criptográfico que se emplee, sino en un parámetro de dicho algoritmo llamado clave que se utiliza para cifrar, descifrar o para ambas cosas.

Es necesario determinar un mecanismo que garantice que una clave pública pertenece realmente a quién se supone que pertenece. Tal problema, encuentra su solución con la implementación de certificados digitales. Además, a través del espectro de la certificación digital se cumple con los cuatro tipos de garantías buscadas Autenticación/Control de acceso, Integridad, Confidencialidad, No repudio, Auditabilidad y Acuerdo de claves secretas.

En su expresión más simple un certificado digital es el equivalente electrónico de un carnet de identidad, que da la posibilidad de identificar al suscriptor propietario. Es un fichero digital intransferible y no modificable, emitido por una tercera parte de confianza, que asocia a una persona o entidad a una clave pública.

De acuerdo con el standard X509v3 debe contener la siguiente información:

- Identificación del titular del certificado
- Clave pública del titular de certificado
- Fecha de validez
- Número de serie
- Identificación del emisor del certificado

Entonces, la misión de los certificados digitales consiste en permitir la comprobación de que la clave pública de un usuario, pertenece realmente a ese usuario, ya que así consta en el certificado emitido por una autoridad.

Usos:

Los certificados permiten realizar una gran cantidad de acciones a sus titulares, se identifican seis modalidades de uso frecuente:

- **Identificación:** control de accesos a sitios web o servicios en línea restringidos. Desarrollo de comunidades cerradas, intranets corporativas. Control de acceso físico de tarjetas inteligentes. Firma de software para su uso en internet de manera que se puedan realizar acciones en el navegador del usuario que de otro modo le serían negadas.
- **Transacciones electrónicas:** como por ejemplo los movimientos en una cuenta corriente o las transacciones comerciales seguras.

- **Trámites fiscales:** como por ejemplo declaraciones juradas de impuestos, pago on-line de tributos.
- **Seguridad en servidores web:** se trata de tener la certeza de que se está en el verdadero sitio y no en una copia, permitiendo realizar interacciones seguras.
- **Documentos electrónicos:** da la posibilidad de firmar contratos, órdenes de compra o cualquier otro documento de uso público o privado en forma digital con los mismos efectos que los celebrados por escrito y en soporte de papel. Así mismo, se puede asegurar la confidencialidad en procesos administrativos o consultas de información de importancia en servidores de la Administración.
- **Correo Seguro:** permite enviar correo electrónico cifrado y firmado de manera de proteger este canal identificando a quién emite, a quién recibe y además encriptando el contenido del mensaje.

Clases:

Existen varias clases de certificados dependiendo fundamentalmente de quién y en qué ámbitos se emitan

- Certificados de clave pública, que contienen la clave pública determinada de un individuo asociando dicha clave una persona en concreto
- Certificados de Atributos, que identifican a su titular y al par de claves, pero agregan algún tipo de información de carácter adicional y permiten su uso fuera o dentro de la organización
- Certificados transaccionales, emitidos para ser utilizados en una transacción específica con la finalidad de limitar el riesgo

tanto para el titular del certificado como para la autoridad de certificación

Una de las características más importantes de los certificados es su temporalidad, tienen un plazo de duración dentro del cual mantienen vigencia. Su expiración puede darse en forma ordinaria o extraordinaria, el primer caso hace referencia a la culminación del periodo de vigencia del mismo, el segundo se da por causales imprevistas como puede ser el eventual compromiso de la clave privada del titular.

3. Infraestructura de clave pública

Resulta primordial ahora, una vez que hemos tenido en cuenta las condiciones de seguridad y de Certificación Digital, otorgar a todo ello un enfoque sistémico que relacione y de idea de conjunto. Tales propiedades las cumpliría eficientemente la definición de una adecuada Infraestructura de Clave Pública (PKI) que posibilite la utilización de servicios de firma digital en una amplia variedad de aplicaciones y mantenga un entorno de red seguro.

Su misión debe ser la de securizar las transacciones electrónicas de la Administración Pública provincial con su entorno proveyendo claves y gestionando eficientemente certificados confiables, para lograr las mencionadas garantías de autenticación, confidencialidad y no repudiación.

Su implementación funcional debería permitirnos proporcionar como mínimo los siguientes **servicios**:

- Servicios de Certificación: Garantías de autenticidad, confidencialidad e integridad de los datos a través de una plataforma de certificación, gestión de usuarios, control de revocados, etc

- Servicios de certificación temporal y timbre digital

- Disponer de un conjunto homogéneo y compatible de soluciones criptográficas

- Asesoramiento y apoyo en cuanto a soluciones disponibles ante problemas que surjan en la implementación de otros proyectos tanto del sector público como del privado.

3.1 Principales componentes de PKI

En este apartado se describen las principales características de los distintos elementos que se deben interrelacionar correctamente para lograr una organización coherente de los sistemas de clave pública, ellos son:

- Una Autoridad de Certificación
- Certificados Digitales y listas de Revocación
- Pares de claves matemáticamente relacionadas, disponiendo en cada par de una clave privada y una clave pública

Tales elementos se desarrollan dentro de una estructura formal determinada por:

- Políticas de Certificación
- Manuales de Procedimientos

Una **Autoridad de Certificación** representa al usuario que ha sido reconocido por el resto en un determinado entorno como certificador de las identidades digitales de todos. Es el órgano responsable de la emisión de los certificados, luego de una correcta verificación por los métodos que considere en la políti-

ca de certificación. Es el principal proveedor de la tecnología de criptografía asimétrica. Debe contar con medidas de seguridad que infundan la total confianza requerida para considerara a su gestión seria y exitosa y ostentar altos niveles de calidad en la prestación y disponibilidad de sus servicios.

La función básica de una AC reside en verificar la identidad de los solicitantes de certificados, crear los certificados y publicar listas de revocación cuando éstos son inutilizados.

Posibles maneras de identificar autoridades certificantes pueden ser:

- **Por organización**: la autoridad certificante emite certificados a individuos afiliados a una organización.
- **Por residencia**: emite certificados a individuos basándose en una dirección geográfica. Desde el punto de vista gubernamental podría decirse que asumen la responsabilidad por estos certificados en debido estado.
- **Por persona**: es un caso especial donde la certificación no reclama la inserción de su nombre en el certificado con una persona física o entidad. Está establecido par acomodar a usuarios que desean encubrir su identidad cuando hacen uso de las facilidades de seguridad.

Una Autoridad de Certificación puede valerse en su desempeño de **Autoridades de Registro** cuya misión es realizar meticulosamente la verificación de las personas (validación de identidad) que requieren la emisión de un certificado y realizar la solicitud formal pertinente(Registro de presentaciones). Gracias a esta descentralización se agiliza el proceso de certificación y se aumenta la eficacia en la gestión de solicitudes.

Las **Políticas de Certificación** y los **Manuales de Procedimiento** rigen el funcionamiento general de la PKI definiendo cuestiones tan esenciales como el tipo de certificado a emitir por la Autoridad de Certificación, el alcance de la información almacenada en el certificado, los procedimientos de registro, el tipo

y alcance del compromiso de la Autoridad de Certificación con los usuarios y viceversa, las restricciones en el uso del certificado, etc. Además, en todo momento debe considerarse que su confección debe ser de total conformidad con lo estipulado en la legislación vigente sobre el tema. El valor legal de una firma digital validada con un certificado calificado dependerá fuertemente de la política que gobierna el uso de la clave privada asociada

La Publicación de **certificados y de las listas de revocación** de los mismos deben ser publicadas en un directorio, los usuarios de la PKI deben tener acceso para la comprobación de firmas. Además, se le debe prestar atención a la no publicación de datos sensibles. Muchas veces puede convertirse en un elemento crítico si no se le presta la debida atención.

Dentro del espectro de la Ley de Firma Digital, una robusta implementación de una infraestructura de clave pública considera y distingue los siguientes componentes

- **Organismo Licenciante**: Es la Autoridad Certificante Raíz que emite certificados de clave pública a favor de aquellos organismos o dependencias que deseen actuar como Autoridades Certificantes Licenciadas, es decir como emisores de certificados de clave pública para sus funcionarios y agentes.

- **Organismos Auditantes**: Es el órgano de control, tanto para el Organismo Licenciante como para las Autoridades Certificantes Licenciadas.
- **Autoridades Certificantes Licenciadas**: Son aquellos organismos o dependencias que soliciten y obtengan la autorización, por parte del Organismo Licenciante, para actuar como Autoridades Certificantes de sus propios agentes.

- **Suscriptores de certificados:** Pueden serlo todos aquellos funcionarios y agentes dependientes de los organismos que soliciten y obtengan un certificado de clave pública emitido por un organismo que haya obtenido su licencia para actuar como Autoridad Certificante.

3.2 Aplicaciones posibles de la pki de propósitos generales

Es importante resaltar aquí que son justamente las aplicaciones que usan los certificados las que darán, en última instancia el verdadero valor de la PKI. Las que le darán sentido y justificaran su implementación.

Tipo de aplicaciones:

Se prevé implementar las siguientes prestaciones:

- **Correo electrónico seguro/secure messaging, firma digital y no repudio.** La naturaleza distribuida del correo electrónico y la necesidad de almacenar y reenviar información a muchos destinatarios encuentran en la criptografía de clave pública las capacidades de firma digital de mensajes y cifrado masivo sin establecimiento previo de claves secretas compartidas.

- **Autenticación de identidad:**

  de Servidores (sitio seguro), para que los usuarios puedan comprobar el servidor con el que se comunican.

  de clientes (control de acceso) para que los servidores puedan comprobar la identidad del cliente y en función de ésta tomar decisiones de control de acceso

- **Canal Seguro (SSL):** Confidencialidad en la transferencia de datos a través de enlaces públicos de Internet mediante protocolos de la capa de transporte.

- **Secure Desktop:** Cifrado de archivos (acuerdo de clave privada mediante clave pública) y cifrado masivo de datos (sin establecimiento previo de claves secretas compartidas).

- **Secure e-forms:** firma digital y seguridad para formularios basados en web.

- **Encripción de bases de datos**

En conclusión, nuestra PKI podrá incluir una o varias autoridades de registro para certificar la identidad de los usuarios, una o varias autoridades de certificación que emitan los certificados de clave pública, un repositorio de certificados; accesible vía web u otro medio, donde se almacenen los certificados; las listas de revocación de certificados (CRL), donde se listan los certificados suspendidos o revocados; y los propios certificados.

Muchas de las precisiones que quedan aquí planteadas serán efectivamente realizadas a lo largo del proyecto cuando a partir de las recomendaciones realizadas en los diferentes estudios de factibilidad, se le dé forma legal, técnica, operativa y funcional a la infraestructura de Clave Pública para la provincia de Mendoza a través de la redacción de sus políticas y procedimientos y de la propuesta de normativa legal prevista en el Plan de Trabajo.

4. Tecnología y regulación legal

La especial importancia que revisten en sí mismos estos temas genera un desarrollo más profundo que ha sido contemplado en la metodología de

trabajo propuesta para el proyecto. Sin embargo, desde la perspectiva de la factibilidad operativa, resulta importante destacar que el estado de la tecnología actual y la regulación legal de la que ésta ha sido objeto en nuestro país, aportan al escenario actual inmejorables condiciones para el desarrollo de aplicaciones destinadas a mejorar los procedimientos administrativos internos y a ofrecer nuevos servicios al ciudadano o mejorar los ya existentes. *(Ver Anexos III y IV)*

Cabe aclarar que cumplir estrictamente con las pautas estructurales plasmadas en la Ley 25.506 nos deja indefectiblemente sujetos al grado de desarrollo nacional que se dé en la materia, sin perjuicio de las implementaciones bajo la figura de "pruebas piloto" que se puedan ir desarrollando en la provincia.

5. Promoción y formación

Utilizando una interfaz de persuasión y motivación creemos muy conveniente encarar acciones de sensibilización y difusión (y en una etapa posterior de capacitación) de las tecnologías asociadas a la firma digital y sus aplicaciones más funcionales en el ámbito de la Administración Pública.

El objetivo: lograr la toma de conciencia de los beneficios de esta tecnología, a fin de acelerar su adopción por parte de los funcionarios y personal público.

Hemos dividido la tarea teniendo en cuenta los siguientes ámbitos:

- Ámbito Legislativo
- Ámbito Ejecutivo
- Ámbito Judicial
- Personal Administrativo Público en general

En tal sentido, se han iniciado las tareas de sensibilización con la planificación de un taller específico sobre Firma Digital dentro del Marco del Coloquio "Hacia el gobierno Digital" programado para el mes de junio del corriente

año. En dicho taller se espera contar con personalidades versadas en el tema y de reconocido prestigio en el medio.

6. Escenario Provincial

Existen en el medio local una serie de factores y condiciones que, a nuestro entender, constituyen un escenario favorable para la instauración de una Infraestructura de Clave Pública y el consiguiente desarrollo de aplicaciones de firma digital sobre su base.

A saber:

- **Convenio Consejo Federal De La Función Pública / Convenio De Cooperación Y Asistencia Técnica:** considera dentro de sus premisas la política de reformar y modernizar el Estado, a fin de avanzar hacía un país capaz de recuperar su potencial de crecimiento y desarrollo y responder a las necesidades de la ciudadanía con servicios efectivos y de calidad, requiere la acción conjunta del Estado Nacional y los Estados provinciales para llevar a cabo políticas concertadas de reforma básica y de modernización de las respectivas administraciones públicas, promoviendo asimismo la adhesión participativa de los otros poderes de gobierno y de los municipios. Por este convenio la Provincia reafirma su compromiso prioritario con el proceso de reforma y modernización de la Administración Pública para fortalecer las estructuras provinciales, y establece con esos fines relaciones de cooperación y asistencia técnica con la NACIÓN.

Además en su **ACTA COMPLEMENTARIA N° 1** el Señor Jefe De Gabinete De Ministros, D. Alfredo Néstor Atanasof y el Señor Gobernador De La Provincia De Mendoza, Ing. D. Roberto Raúl Iglesias, acuerdan entre otros puntos:

- OBJETIVOS DE LAS ACCIONES DE COOPERACIÓN: Comenzar la puesta en marcha de acciones centradas en el aseguramiento y modernización de los procesos básicos de gestión y administración de recursos, incorporando tecnologías que contribuyan a gestionar con efectividad, calidad y transparencia la administración gubernamental, a fin de facilitar el acceso de la población a los servicios del estado provincial.

- PROYECTO DE COOPERACIÓN: El primer proyecto de cooperación tendrá como objetivo la implementación de tecnología de firma digital en diversos trámites de gobierno. Para ello se definirá un trámite en particular a partir del cual desarrollar una prueba piloto con certificados emitidos por la Subsecretaría de la Gestión Pública de la Jefatura de Gabinete de Ministros. Con posterioridad se trabajará en la definición y la habilitación de alguna instancia del gobierno provincial como Autoridad de Registro y, con posterioridad, como Autoridad Certificante.

La propuesta plasmada en este convenio marcaría un punto de partida muy importante en cuanto al apoyo técnico que podría recibir la Provincia con relación al proyecto e-firma/mza y aumentaría considerablemente la viabilidad política del proyecto.

✔ **Guía orientadora de trámites:** este exitoso proyecto desarrollado por la Unidad de Reforma del Estado y financiado íntegramente por el CFI, ha llevado a cabo considerables avances en términos de informatización de trámites. Este hecho, constituye un antecedente y una base potable de procedimientos administrativos que podrán servir de materia prima para la implementación de diferentes aplicaciones de firma digital, a saber:

- Firma y/o cifrado de Correo Electrónico, tanto interno como externo.

- Firma y/o cifrado de Documentos (Pericias, Dictámenes, Publicaciones en el Boletín Oficial, Planos, Software, Políticas, Procedimientos, Normativas, Expedientes, etc.)
- Identificación de personas ante Sistemas internos en redes locales y abiertas (Intranets). Sitios Web (sin necesidad de registrar datos). Determinación implícita del Perfil del Usuario. Identificación de sistemas ante el usuario.
- Auditoría de transacciones
- Seguridad al operar con pagos on-line, recaudación de impuestos.
- Identificación de los componentes físicos de una red.
- Fidelización de documentos digitalizados
- Recibos de pago
- Adjudicaciones
- Certificados varios
- Circulares internas o externas

✔ **Financiamiento CFI:** es importante señalar el constante apoyo de tipo no sólo financiero, sino también técnico desde el Consejo Federal de Inversiones que posee una larga trayectoria de asistencia en proyectos de e-Government en la provincia de Mendoza.

✔ **Plan Provincial:** el proyecto e-firma/mza no es una iniciativa aislada sino que forma parte del Plan Provincial "Hacia el Gobierno Digital" cuyos objetivos son:

- Mejorar la calidad en la atención al público, a través de la incorporación de alternativas que promuevan la rapidez en el inicio y/o gestión de tramitaciones.

- Promover la eficiencia en la gestión a través de la estandarización de los procedimientos y formularios utilizados para los trámites administrativos que tienen similares características.

- Propiciar la disminución de costos en que debe incurrir la población al tener que trasladarse hasta una dependencia específica para realizar tramitaciones.

Dentro del marco de este plan el proyecto e-firma forma parte del Programa de **Incorporación de NTIC´s a la Gestión de Gobierno** el cual busca ampliar los servicios tecnológicos de contacto con la ciudadanía; a través de la introducción de nuevas formas y procesos internos en la administración del Estado, que permitan la integración de los sistemas de los diferentes servicios, compartir recursos y mejorar la Gestión interna de los mismos. Procurando que la calidad de los servicios prestados a través de esta nueva modalidad sea superior a la recibida en forma presencial en las dependencias públicas.

7. Conclusiones

Sólo una completa y adaptada implementación de una Infraestructura de Clave Pública (con un determinado sistema de hardware, de software, de políticas y de personas) hace factible proporcionar el conjunto de seguridades informáticas que la Administración Pública Provincial necesita. En tal sentido, es muy importante realizar una fina valorización de ciertos factores que pueden entorpecer el desarrollo de nuestro proyecto pero que, correctamente tratados, pueden fortalecer su implementación, a saber:

El grado de interoperabilidad

El hecho de adherir a las especificaciones del estándar X.509.v3 no garantiza necesariamente que dos certificados generados por dos sistemas desarrollados por firmas distintas sean mutuamente compatibles. Pueden darse, y de hecho han ocurrido, ciertos inconvenientes en estas certificaciones cruzadas ya que existen problemas de confianza entre las Autoridades de Certificación de distintas organizaciones, que puede imposibilitar el éxito en la verificación de las cadenas de certificación cuya AC raíz sea desconocida o no confiable, invalidando todo el conjunto. Cabe destacar que este problema no es esencialmente de orden técnico como tampoco del estado de desarrollo del espectro tecnológico actual.

Los costos

Cada empresa prestadora de servicios de clave pública tarifa en función de una diversidad amplia de criterios (por certificado, por uso de certificado, por servidores instalados, etc) al no existir aún un mercado totalmente desarrollado, los honorarios que se cobran también resultan dispares, de tal forma que la inversión en una PKI como respuesta a las necesidades de seguridad y accesibilidad puede resultar en algunos casos inesperadamente elevada. Muchas veces

la respuesta estará en planificar una infraestructura escalable que comience con aplicaciones acotadas.

La escalabilidad

Si no se considera criteriosamente las posibilidades de expansión de una PKI, cuando la cantidad de certificados crece, pueden surgir situaciones conflictivas. Esto puede afectar, por ejemplo, a la gestión relacionada a las listas de revocación ya que deben ser consultadas en cada operación que involucre certificados y firmas digitales en las aplicaciones más serias del entorno de la PKI.

Complejidad tecnológica frente a usuarios finales no capacitados y participación activa

La tecnología PKI se torna un tanto lejana para el usuario final que no termina de entender toda la jerga relacionada. La costumbre de autenticarse sin más que introducir su nombre y contraseña, lo hace sentir rebasado por la complejidad tecnológica de las firmas digitales y la criptografía de clave pública. En este sentido la introducción de la tecnología sin niveles adecuados de capacitación se torna casi inviable.

La seguridad y almacenamiento de la clave privada

Ninguna solución de PKI es más fuerte de lo que lo es su eslabón más débil. En otras palabras, si no protege correctamente las claves privadas que forman el núcleo de la PKI, se estará comprometiendo la seguridad de la infraestructura de confianza y, en último término, de su organización.

No hay nada más crítico para la seguridad de una PKI que la integridad y el carácter secreto de la clave privada de la autoridad de certificación. En las PKI basadas en software, las claves son vulnerables, al ser creadas, almacenadas o gestionadas en servidores con arquitecturas y sistemas operativos abiertos. Cada vez que el sistema utiliza una clave, ésta queda expuesta a posibles

ataques. Una vez que una clave ha sido robada, la integridad de todo el sistema puede quedar expuesta al riesgo de emisión de certificados falsos, expedidos por quien ha atacado el sistema, que pueden poner en peligro la validez de todas las identidades digitales expedidas con esa clave de CA.

Identificación de circuitos administrativos

Casi cualquier número de transacciones electrónicas puede requerir los niveles de seguridad que provee una PKI, sin embargo es importante hacer una adecuada elección del alcance y los ámbitos de aplicación de los servicios de criptografía asimétrica para lograr ahorros y no incurrir en sobrecostos de implementación

Criterios de selección de circuitos administrativos

-Trámites con alta frecuencia de repetición a cargo de la misma oficina, ente o persona.
-Circuitos que requieren autenticación de las partes involucradas
-Circuitos administrativos que enlazan importantes distancias geográficas
-Circuitos basados en gran cantidad de papeleo
-Circuitos administrativos de transferencia de información con exigencias de oportunidad

Criterios de selección de transacciones aptas para ser firmadas digitalmente

-Aquellas que requieren efectiva autenticación de personas o entes involucrados en la transacción
-Aquellas que implican traslado de fondos

-Aquellas que autorizan subsidios o prestaciones sociales de ayuda

-Aquellas que se definan en las políticas y manuales de procedimientos de la Autoridad Certificante

Criterios de selección de transacciones aptas para ser encryptadas

-Aquellas que contengan información estrictamente confidencial

-Aquellas que contengan información que no debe estar disponible públicamente sin filtros previos

Métodos de Retención de Archivos y Riesgos

Las prácticas basadas en criptografía de clave pública protegen a los gobiernos de los riegos de fraude y del repudio de transacciones asociadas a archivos firmados digitalmente, determinar correctamente la cobertura de riesgo que se desea asumir junto con la valoración de costo beneficio nos permite elegir una estrategia de retención de archivos adecuada a las necesidades de la Provincia.

Ejemplos de Niveles de Riesgos, Tipos de E-firma, Métodos y Prácticas

Cobertura de Riesgo	**Ejemplo de E-firma**	***Métodos y Prácticas***
Baja	User ID/password o PIN	• Copia de seguridad de archivos, software de aplicación, identificación de ingreso a base de datos, identificación de ingreso a base de datos con referencia de fecha y hora.

		• Procedimientos de prueba de identidad en transacciones de recepción de certificados o documentos personales.
Media	Protección de Contraseña Firma digital	• Copia de seguridad de archivos, software de aplicación, identificación de ingreso a base de datos, identificación de ingreso a base de datos con referencia de fecha y hora. • Procedimientos de prueba de identidad en transacciones de recepción de certificados o documentos personales. • Copia de certificados digitales o registro de firmas digitales • Prueba de validación del certificado digital al momento de la transacción, archivo de listas de certificados revocados o chequeo on-line del estado del certificado.
Alta	Firma digital protegida por tarjetas inteligentes o por técnicas biométricas	• Copia de seguridad de archivos, software de aplicación, identificación de ingreso a base de datos, identificación de ingreso a base de datos con referencia de fecha y hora. • Procedimientos de prueba de identidad en

		transacciones de recepción de certificados o documentos personales. • Copia de certificados digitales o registro de firmas digitales • Prueba de validación del certificado digital al momento de la transacción, archivo de listas de certificados revocados o chequeo on-line del estado del certificado. • Prueba de que la realización de una transacción o que de un procedimiento de firma a ocurrido en un momento específico (time stamping) • Archivo de Instrucciones para aplicaciones y recuperación de archivos para un sistema de transacciones • Archivo del vínculo de acceso a las listas de revocación para validación de firmas digitales en tiempo real. • Sistema de escritura única para archivos

Muy alta	Firma digital protegida por tarjetas inteligentes o por técnicas biométricas	Copia de seguridad de archivos, software de aplicación, identificación de ingreso a base de datos, identificación de ingreso a base de datos con referencia de fecha y hora. • Procedimientos de prueba de identidad en transacciones de recepción de certificados o documentos personales. • Copia de certificados digitales o registro de firmas digitales • Prueba de validación del certificado digital al momento de la transacción, archivo de listas de certificados revocados o chequeo on-line del estado del certificado. • Prueba de que la realización de una transacción o que de un procedimiento de firma a ocurrido en un momento específico (time stamping) • Archivo de Instrucciones para aplicaciones y recuperación de archivos para un sistema de transacciones • Archivo del vínculo de acceso a las listas de revocación para validación de firmas

		digitales en tiempo real. • Sistema de escritura única para archivos • Hardware de almacenamiento capaz de ofrecer los archivos on-line necesarios a las aplicaciones de firma digital que lo requieran

Fuente: Gartner Research

8. Estrategias y Propuestas

Por último, hemos intentado aquí resumir las acciones estratégicas principales que se desprenden de este subestudio de factibilidad operativa y que son consecuencia de los desarrollos plasmados en su contenido.

- Considerar la Palnificación de la PKI de propósito general como un elemento realmente estratégico, que le de coherencia y unidad a las aplicaciones aisladas que se desarrollen en la Provincia.

- Generar Políticas, Normas y Procedimientos de alcance general para apoyar y realizar aplicaciones basadas en la tecnología de Firma digital en el ámbito administrativo y de prestación de servicios de la Administración Pública Provincial.

- Identificar aplicaciones a través de un diseño adecuado y coherente de una Infraestructura de Clave Pública

- Desarrollar actividades de sensibilización, capacitación y difusión de la tecnología asociada

- Cumplir ampliamente con los requisitos legales establecidos por la Ley 25506 y su Decreto Reglamentario

- Emplear tecnología estándar y certificada

- Transmitir seguridad, solidez y confiabilidad a través de la estructura funcional, procedimientos operativos, y políticas de registro y certificación.

- Estudiar ampliamente la aplicabilidad funcional de los certificados digitales.

- Mantener cierta flexibilidad y apertura operativa.

- Procurar una escalabilidad adecuada al entorno provincial planteando una Infraestructura de Clave Pública por etapas de crecimiento.

- Comenzar con aplicaciones piloto para luego escalar.

- Prestar asesoramiento y apoyo a proyectos relacionados con la tecnología de firma digital

- Como fin último desarrollar ampliamente los servicios prestados sobre la infraestructura planteada, ya que es lo que esencialmente determina su valor real

Anexo II

e-firma/mza

Factibilidad Económica-Financiera

Las nuevas tecnologías, se aplican cada día más en los ámbitos particulares como en el de las organizaciones, tanto de manera interna como externa. Y tienden fundamentalmente a la asistencia para el incremento de la eficiencia, la eficacia, mejorar las relaciones internas y externas, el confort y al incesante ahorro de Costos.

Es innegable que el contar con información fidedigna y precisa al momento de cualquier decisión, la diferencia competitiva es inigualable.

Es así que, como históricamente para cada enfermedad siempre surgió, sin considerar el costo, el remedio, hoy para adecuar el bajo costo de comunicación con el consiguiente grado de confianza surge un nuevo paradigma. La criptografía es el remedio a la incertidumbre de que la información que tratamos en un medio que no nos permite determinar que la información de quién dice ser, simplemente es.

Analizaremos ahora una proyección del mercado de las PKI sustentada en los beneficios de cúmulo que nos traería su desarrollo en el sector productivo y desde una perspectiva amplia de costo/beneficio la factibilidad económico-financiera de la implementación de una PKI y sus servicios, desglosando las dos grandes dimensiones que implica ésta relación.

1. Nociones de mercado y Tendencias

El mercado de esta tecnología se descompone en dos segmentos principales: Productos y Servicios.

Se denomina como "productos" de las PKI a los software diseñados para registrar, emitir y administrar las claves públicas y privadas relacionadas con los certificados digitales durante todo su ciclo de vida.

Los ingresos en este segmento incluyen, en general, licencias de software y su mantenimiento.

Se denomina "servicios" a la emisión, registro y administración de certificados emitidos por una autoridad certificadora.

Existen además servicios adicionales que pueden o no incluirse dentro de este último segmento, entre los que están los servicios profesionales (consultorías, entrenamiento, planeamiento y implementación de una PKI), mantenimiento e integración de sistemas.

Dado su reciente desarrollo, a finales de 1999 la mayoría de las PKI del mundo todavía no se encontraba en estado de régimen. La gran mayoría se encontraba en etapas previas, y solo el 30% estaba en la etapa de despliegue.

Si bien es cierto que el número de autoridades certificadoras ha ido creciendo sostenidamente, la industria en su conjunto se encuentra aún en una fase preliminar, aunque se espera una expansión continua a partir de los próximos años, en tanto esta infraestructura es reconocida como uno de los grandes facilitadores del comercio electrónico.

Las proyecciones de ingresos por ventas varían fuertemente según la fuente de origen.

Sin embargo, todas ellas apuntan a sugerir que los ingresos crecerán progresivamente durante los próximos años, en particular en las áreas de las aplicaciones y servicios.

Se proyecta un incremento de los ingresos desde U$S 281 millones de 1999 a U$S 3.010 millones al año 2004, sólo por concepto de Productos y Servicios, con una intensificación en los ingresos por servicios por sobre los productos.

Finalmente, Frost & Sullivan pronostica ingresos fuertemente expansivos durante los próximos años, estimándose para 2004 ingresos por U$S 3.200 millones, más de veinte veces superiores a los registrados en 1999.

PROYECCIONES DE INGRESOS DE LAS PKI
(Millones de US$)

	1999	2004	CAGR (*)
INGRESOS	281	3,010	60.7%
PARTICIPACIÓN			
Productos	66.9%	40.8%	
Servicios de las AC	33.1%	59.2%	

Fuente: IDC

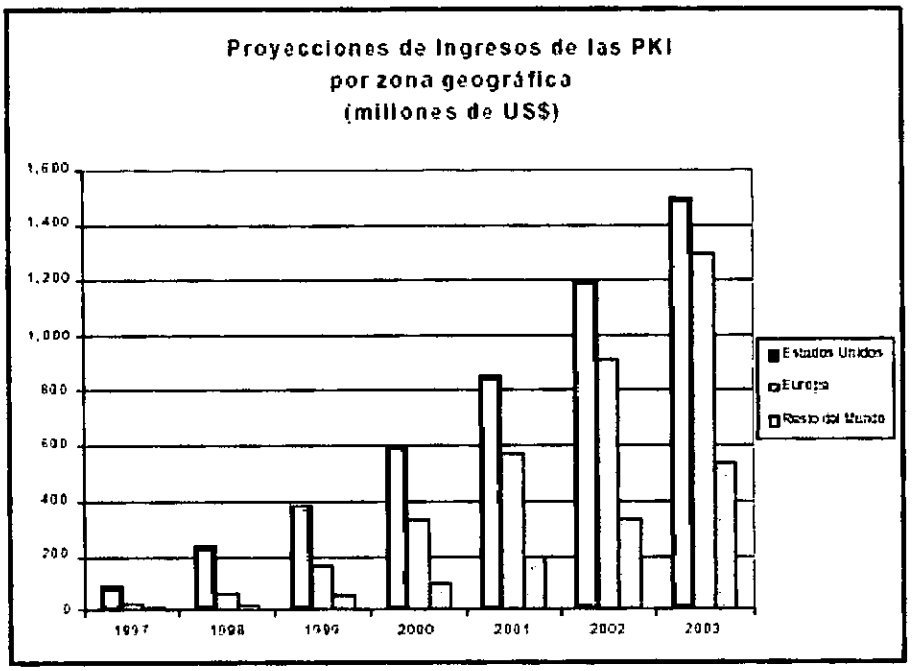
(*) Tasa de Crecimiento Anual Compuesta

En general, se estima que las PKI tendrán un crecimiento fuerte y estable por los años, al mismo tiempo que esta tecnología se transforma crecientemente en un mecanismo de confianza para el comercio electrónico.

El crecimiento sistemático se dará como resultado de la adopción masiva de tecnologías PKI como soluciones para la autenticación, autorización, encriptación y administración por parte de empresas, agencias de gobierno y otras instituciones. Con el tiempo, un mayor número de aplicaciones sustentarán a las PKI. A medida que más aplicaciones de PKI se desarrollen, los servicios de las ACs serán llevados progresivamente a la emisión de certificados, en lugar de que una empresa los emita por sí misma. A medida que el mercado madure, los servicios representarán una mayor proporción del mercado.

En términos regionales, durante esta primera fase de actividad, los ingresos por ventas han sido explicados casi exclusivamente por el comporta-

miento de Estados Unidos y Europa. No obstante, se proyecta que esta concentración tenderá a decrecer una vez que se vayan promulgando los proyectos de firma digital y se desarrollen las PKI para ir generando una mayor demanda en los demás países del globo, especialmente en el continente asiático y Sudamérica, que son los que presentan un mayor desfase.



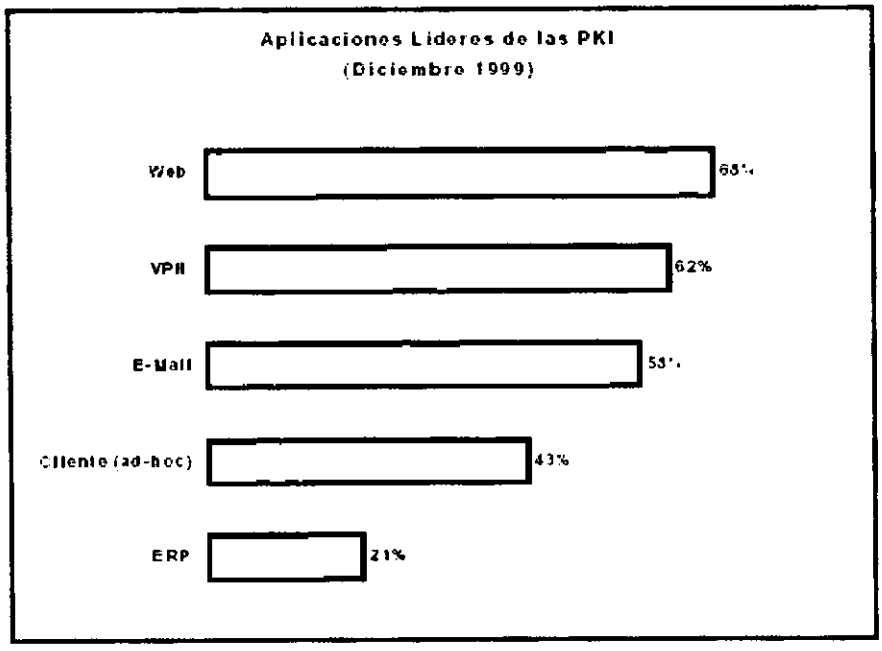
Fuente: Datamonitor

Para el año 2003 se estima que aunque las ventas seguirán creciendo fuertemente en todo el mundo, la participación en los ingresos de Estados Unidos decrecerá al 45% mientras que la de Europa se incrementará a 39%. El resto del mundo incrementará sus ventas por sobre el promedio para alcanzar el 16% del total.

Históricamente, el principal tipo aplicación asociada a las PKI fue aquella destinada a otorgar seguridad en la Web. Otro tipo de aplicación que destacó fuertemente fueron las VPN3 intensivamente utilizadas por las empresas que realizan transacciones B2B, y que por tanto demandan altos estándares de seguridad. Ésta tecnología protege las transacciones entre los host que pertenecen a

una red privada, generalmente los proveedores y demandantes de un marketplace.

Con casi igual importancia, destacaron los programas para otorgar seguridad a los e-mail que requieren operar bajo normas confidenciales. Luego, con un poco menor relevancia que las anteriores pero con una todavía fuerte participación, destacaron las soluciones a la medida, diseñadas para satisfacer demandas de clientes específicos. Finalmente, más atrás se ubicaron los ERP 4.



Fuente: Aberdeen Group. PKI Multi-Client Study.

2. *Costos*

Encarar un proyecto de implementación de aplicaciones basadas en la teoría de firma digital en la Administración Pública Provincial es una tarea laboriosa, por cuanto se deben considerar los costos que implica la adopción de

este nuevo estilo de trabajo, no solo por los cambios tecnológicos sino por los cambios culturales que implica.

Entre los aspectos más destacados en cuanto costos resaltamos:

- Estratégicos, o aquellos costos que insume el tiempo invertido en el planeamiento de todo lo que tenga que ver con el diseño e implementación de una Infraestructura de Clave Pública.

- La inversión en el establecimiento y operación efectiva de autoridades certificadoras, depósitos de claves públicas y todos los servicios necesarios para el funcionamiento de estos procesos.

- Educación, este aspecto incluye tanto el entrenamiento del personal interno para redefinir y asumir nuevas responsabilidades en un ambiente de Firma Digital, como así también la educación de los usuarios externos que eventualmente queden implicados en una aplicación de ésta tecnología.

- Implementación, incluye el costo del personal del área de Sistemas de Información que asegura la compatibilidad de las aplicaciones internas con los sistemas.

- Intercambios, gasto en comunicaciones y el mantenimiento de todos los elementos que permitan el óptimo funcionamiento de la PKI.

- Desarrollo, adquisición de programas, desarrollo y programación de las interfaces de aplicación, mejoramiento del software de aplicación interno para aprovechar todas las ventajas de una PKI y las pruebas necesarias para la óptima implementación de la nueva Tecnología.

- Requerimientos de soft y Hardware definidos en el estudio de factibilidad técnica (Ver Anexo IV).

3. Beneficios

El despliegue de una PKI y la utilización de certificados digitales posee, desde varios puntos de vista un costo relativo más que eficiente debido al elevado nivel de seguridad que otorga. No resulta fuera de lo común que en los países más avanzados se haya utilizado la tecnología de certificación digital y que goce de perspectivas firmes de expansión. Cabe señalar también, que en la actualidad es una tecnología que por sus características no posee sustitutos.

Entre los aspectos más destacados en cuanto a beneficios resaltamos:

- Disminución de costos materiales en papel, correo, cartuchos de impresora, horas hombre y principalmente en tiempo,

- Transparencia de información, ya sea en trámites internos o externos, lo que redunda en una mayor eficiencia y rapidez en los procesos internos o en la prestación de servicios al ciudadano.

- Potencialidad para dotar al sistema de una mayor transparencia y obtener la consecuente reducción del gasto público y restablecer la credibilidad en las instituciones democráticas.

- Ahorros de costos de transacción y almacenamiento

- Mayor agilidad y eficiencia en los procesos que involucran papeles y documentos oficiales.

- Creación de nuevos mercados, generará redes productivas más ágiles entre diversas empresas e introducirá mayor eficiencia en sectores público y privado, produciendo significativos avances en materias de productividad.

- Eliminación de trabas burocráticas.

- Trabajo cooperativo, educación a distancia, servicios de la administración pública como los trámites y el pago de impuestos.

- El mayor grado de seguridad que puede obtenerse de un documento firmado digitalmente.

- Amplio abanico de servicios de seguridad

- Facilidad de búsqueda y de acceso, liberación de espacio físico, limpieza, seguridad

Concretamente nos trae enormes beneficios en la relación:

Administración ⟶ Administrado

Tales como:

- La presencia segura de la administración en la red
- La consulta de información personal desde internet
- La realización de trámites varios en internet como pago de tributos u obtención de certificaciones.
- Acceso a aplicaciones informáticas de gestión
- Comunicación entre dependencias de la administración pública
- Integración de información al ciudadano desde distintas administraciones
- Aplicaciones de democracia electrónica tales como el plebiscito o el sufragio.

Por tanto dichas modalidades de trabajo, el incremento de la velocidad de circulación de la información a través de los documentos digitales y el notable incremento de la seguridad del entorno hará que se ofrezcan más y mejores servicios al ciudadano y simultáneamente se logren ahorros de tiempo y costos.

Beneficios concretos de la despapelización

En función de la enorme cantidad de tiempo y dinero que el Gobierno Provincial destina al papeleo, los potenciales beneficios de procesar tal cantidad de información por medios digitales son considerables.
Dicha afirmación es posible sustentarla en las siguientes reducciones:

Reducción de costos

Los llamados formularios digitales seguros pueden producir economías de hasta un 90% por sobre el procesamiento manual usado actualmente en el gobierno y en la prestación de servicios a los ciudadanos.

Costo unitario por formulario	De papel	Digital	Ahorro
Impresión y almacenamiento	U$S15	U$S1	U$S14
Llenado, procesado y codificado	U$S145*	U$S5**	U$S140
Costo por formulario completo	U$S160	U$S6	U$S154

E-Government Solutions-Secure e-forms-www.entrust.com

* Incluye el tiempo empleado en el llenado a mano, envío del formulario completo para su aprobación, envío al usuario final, el tecleo manual en la aplicación, el costo de formularios perdidos y los errores de tipeo.

** Incluye llenado del formulario, remisión del formulario, procesamiento de los datos del formulario en la base de datos o en aplicaciones de oficina.

Las fuentes de reducción de costos a partir del uso de herramientas digitales de despapelización son múltiples:

- Eliminación o reducción al mínimo de los costos de impresión.
- La eliminación de duplicaciones de entrada de información y errores de transcripción puede reducir los costos operativos.
- Las reglas automáticas para recolección de datos precisos reducen la necesidad de intervención manual y tiempo de procesamiento para corregir errores.

- La automatización de los procesos habilitada por los formularios digitales seguros, puede reducir los costos operativos que insume su procesamiento efectivo.
- Los servicios de distribución basados en aplicaciones Web son generalmente más económicos que los servicios de distribución manuales.

Reducción de errores

El procesamiento de errores puede reducirse drásticamente a través del uso de formularios digitales seguros. Cuando formulario digital se diseña, cada campo puede enmascararse para aceptar sólo un tipo de caracter o un formato de datos definido. Esto simplifica el trabajo de la persona que completa el formulario al incluir la información apropiada en el formato requerido. Si un usuario completa un campo con información errónea, un formulario electrónico seguro puede devolver el formulario inmediatamente al usuario para la corrección antes de que empiece a ser procesado, reduciendo tiempo y costo de gestión manual.

Reducción de los tiempos de procesamiento

Habilitando el uso de los formularios digitales seguros en línea, se puede disminuir significativamente el tiempo de proceso, ya que los datos no tienen que ser transferido manualmente del formulario de papel a una base de datos u otro sistema de procesamiento electrónico. Este re-tecleo de información, consume tiempo, dinero e incrementos en la tasa de error.

Cuando se controlan los errores durante la recolección de datos, el tiempo del proceso aumentado que es el resultado de los formularios incompletos o incorrectos se minimiza, produciendo la realización más rápida de la actividad.

Cuando los datos se procesan electrónicamente, la distribución de la información es casi instantánea. Usando los servicios estándar de mensajería sólo se agregan días que suman tiempo de proceso. Para los formularios de uso interno, el tiempo

adicional se pierde con los movimientos de papeleo entre oficinas para lograr las firmas de la aprobación correspondiente. Cuando los formularios digitales seguros utilizan las tecnologías relacionadas con la firma digital, las firmas digitales pueden agregarse rápidamente y con la misma confianza depositada en las firmas manuscritas.

Finalmente, cuando pueden accederse a los formularios digitales a través de un portal gubernamental, la disponibilidad de acceso a toda hora permite a los ciudadanos completar y enviar los formularios a su conveniencia.

Los beneficios de usar los formularios digitales seguros para el gobierno se traducen en aplicaciones virtuales útiles de gobierno a ciudadano (G2C), de gobierno a empresas (G2B), de gobierno a gobierno (G2G) y en los procesos internos de gobierno.

El daño hecho a la confianza pública y a la seguridad por las brechas de seguridad electrónicas puede ser muy perjudicial para los gobiernos. Mientras que los beneficios de la despapelización son tremendos, los gobiernos deben focalizarse en la seguridad, a priori los requerimientos de privacidad y de firma digital deben tenerse en cuenta para llevar a cabo las soluciones gubernamentales electrónicas.

4. Conclusiones

Hemos plasmado aquí un boceto de las características del sector en el que se desenvuelven las Infraestructuras de Clave Pública, así como también hemos determinado que tipos de costos deberemos de absorber en la implementación y de que tipo de beneficios disfrutaremos una vez alcanzados los objetivos.

En función de la naturaleza de la propuesta sustentada en la Factibilidad Operativa *(Anexo I)* y en la Factibilidad Técnica *(Anexo IV)* en la que se hace mención a una estrategia de crecimiento escalable de la PKI, dejaremos para

la propuesta de implementación final del presente proyecto la determinación estricta y con bases presupuestales de los costos/beneficios medidos en términos de las aplicaciones que iremos desarrollando y los recursos que éstas demanden de la infraestructura global.

Anexo III

e-firma/mza

Análisis de Factibilidad Legal

Si bien se considera que las manifestaciones de voluntad, los contratos privados y las actuaciones administrativas ante y por el estado a través de medios electrónicos y telemáticos, no difieren "sustancialmente" o en su contenido de los actos contractuales y administrativos realizados sobre la base del soporte en papel, resulta necesario dotar de seguridad jurídica a las declaraciones de voluntad emitidas digitalmente, atendiendo a las características especiales del proceso de formación de la voluntad y su manifestación digital.

Ante el impulso de la realidad y la significación de las contrataciones digitales, esta dificultad legal debió ser superada, llenando el vacío legislativo existente en una materia de reciente data, pero de una inusitada gravitación en la vida jurídica de las personas y las instituciones.

De tal manera se concibió la estructura técnica y jurídica de la firma digital, como sustituto válido y seguro en los documentos digitales, de la firma ológrafa prevista por el codificador, en el siglo 19 para los instrumentos privados escritos en soporte papel.

1. Antecedentes INTERNACIONALES

En el plano internacional tienen lugar actualmente múltiples actividades y debates en torno a los aspectos legales de la firma digital:

- La Comisión Europea ha redactado su borrador final de Directiva de Firma Digital ("Propuesta de Directiva del Parlamento Europeo y el Consejo sobre un Marco Común Para las Firmas Electrónicas") del 13 de mayo de 1998, publicado en el Diario Oficial de las Comunidades Europeas del 23 de octubre de 1998, que establece las pautas para la utilización de la firma digital por los Estados miembros.

- La Comisión de las Naciones Unidas para el Derecho Comercial Internacional (UNCITRAL) ha aprobado una Ley-Modelo sobre Comercio Electrónico y ha comenzado a trabajar en la preparación de normas uniformes en materia de firma digital.

- Ley Modelo de la Comisión de las Naciones unidas para el derecho mercantil internacional (CNUDMI) sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno.

- La Organización de Cooperación y Desarrollo Económico (OCDE) prosigue sus trabajos en este ámbito, a modo de continuación de sus pautas de política criptográfica de 1997.

- Otras organizaciones internacionales, como la Organización Mundial del Comercio (OMC), han empezado también a interesarse en el tema.

- El Comité de Seguridad de la Información de la Sección de Ciencia y Tecnología de la American Bar Association ("ABA" – Asociación de Abogados de los EE.UU.) redactó su Normativa de Firma Digital en 1996, en la que participaron casi ochenta profesionales de las disciplinas del derecho, la informática y la criptografía de los sectores público y privado, en la que especifica un mecanismo de firma digital a base a criptografía asimétrica, los certificados de clave pública y los certificadores de clave pública.

- Directiva 99/93 de la Unión Europea que tiene por finalidad facilitar el uso de la firma electrónica y contribuir a su reconocimiento jurídico. Crea un marco jurídico para la firma electrónica y para determinados servicios de certificación con el fin de garantizar el correcto funcionamiento del mercado interior. No regula otros aspectos relacionados con la celebración y validez de los contratos u otras obligaciones legales cuando existan requisitos de forma establecidos en las legislaciones nacionales o comunitaria, ni afectan

a las normas y límites, contenidos en las legislaciones nacionales o comunitaria, que rigen el uso de documentos.

A su vez se han recopilado los siguientes documentos internacionales que denotan el grado de desarrollo en materia legal, de los cuales es objeto la tecnología de firma digital en los distintos países del mundo:

País	Actividad legislativa de firma digital
Alemania	Ley y decreto promulgados en materia de firma digital, estableciendo las condiciones para considerar segura una firma digital; acreditación voluntaria de proveedores de servicios de certificación. Elaboración de un catálogo de medidas de seguridad adecuadas Consulta pública en curso sobre los aspectos jurídicos de la firma digital y de los documentos firmados digitalmente.
Australia	Estrategia para la creación de una infraestructura de firma digital que asegure la integridad y autenticidad de las transacciones efectuadas en el ámbito gubernamental y en su relación con el sector privado. Prevé la creación de una autoridad pública que administre dicha infraestructura y acredite a los certificadores de clave pública (Proyecto "Gatekeeper").
Austria	Las bases legales de la Firma Digital austríaca se encuentran en la Ley Federal de Firma digital (Federal Electronic Signature Act), BGBl I 1999/190.
Bélgica	Ley de telecomunicaciones: Régimen voluntario de declaración previa para los certificadores de clave pública. Proyecto de ley de certificadores de clave pública relacionados con la firma digital. Proyecto de ley de modificación del Código Civil en materia de prueba digital. Proyecto de ley sobre la utilización de la firma digital en los ámbitos de la seguridad social y la salud pública.

Brasil	Proyecto de ley sobre creación, archivo y utilización de documentos electrónicos.
Canadá	Bill 88 2000 Un Acto para promover el uso de tecnología de información en el anuncio y otras transacciones resolviéndose las incertidumbres legales y quitando las barreras estatutarias que afectan la comunicación electrónica En junio del 2000, Manitoba introdujo el Comercio Electrónico. En el año 2000, Quebec publicó el proyecto (Bill 161) Ley Ejemplar en el E-comercio. Bill No. 24 Ley de Evidencia electrónica. Bill No. 25 Ley de Comercio electrónico. Bill No. 70 Ley de Transacciones electrónicas.
Colombia	Ley 527 de 1999 por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Ley 588 del 2000 por medio de la cual se reglamenta el ejercicio de la actividad notarial.
Chile	Ley No. 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de Dicha Firma. Decreto Supremo No. 81 que regula el uso de la firma digital y los documentos electrónicos en la administración del Estado en Chile.

Dinamarca	Proyecto de ley de utilización segura y eficaz de la comunicación digital.
EE.UU.	Iniciativas del Gobierno Federal: Iniciativa sobre la creación de una infraestructura de clave pública para el comercio electrónico. Ley de Firma digital y Comercio Nacional Electronic Signatures in Global and National Commerce Act . June 8, 2000 . Ley que autoriza la utilización de documentación electrónica en la comunicación entre las agencias gubernamentales y los ciudadanos, otorgando a la firma digital igual validez que la firma manuscrita. (Ley Gubernamental de Reducción de la Utilización de Papel - "Government Paperwork Elimination Act"). Ley que promueve la utilización de documentación electrónica para la remisión de declaraciones del impuesto a las ganancias. Proyecto piloto del IRS (Dirección de Rentas - "Internal Revenue Service") para promover la utilización de la firma digital en las declaraciones impositivas. Proyecto de ley de Firma Digital y Autenticación Electrónica para facilitar el uso de tecnologías de autenticación electrónica por instituciones financieras. Proyecto de ley que promueve el reconocimiento de técnicas de autenticación electrónica como alternativa válida en toda comunicación electrónica en el ámbito público o privado. Resolución de la Reserva Federal regulando las transferencias electrónicas de fondos. Resolución de la FDA (Administración de Alimentos y Medicamentos - "Food and Drug Administration") reconociendo la validez de la utilización de la firma electrónica como equivalente a

	la firma manuscrita. Iniciativa del Departamento de Salud proponiendo la utilización de la firma digital en la transmisión electrónica de datos en su jurisdicción. Iniciativa del Departamento del Tesoro aceptando la recepción de solicitudes de compra de bonos del gobierno firmadas digitalmente. Iniciativas de los Gobiernos Estatales: Casi todos los estados tienen legislación, aprobada o en proyecto, referida a la firma digital. En algunos casos, las regulaciones se extienden a cualquier comunicación electrónica pública o privada. En otros, se limitan a algunos actos internos de la administración estatal o a algunas comunicaciones con los ciudadanos. Se destaca la Ley de Firma Digital del Estado de Utah, que fue el primer estado en legislar el uso comercial de la firma digital. Regula la utilización de criptografía asimétrica y fue diseñada para ser compatible con varios estándares internacionales. Prevé la creación de certificadores de clave pública licenciados por el Departamento de Comercio del Estado. Además, protege la propiedad exclusiva de la clave privada del suscriptor del certificado, por lo que su uso no autorizado queda sujeto a responsabilidades civiles y criminales.

Ecuador	Proposed Law Covering Electronic Commerce, Electronic Signatures And Data Messages
España	Circulares de la dirección de Aduanas sobre utilización de la firma digital. Resolución en el ámbito de la seguridad social que regula la utilización de medios digitales. Leyes y circulares en materia de hipotecas, fiscalidad, servicios financieros y registro de empresas que autorizan el uso de procedimientos digitales. Ley de presupuestos de 1998, por la que la Casa de la Moneda actuará como certificador de clave pública. El Ministerio de Ciencia y Tecnología de España, en estrecha colaboración con los Ministerios de Administraciones Públicas, Economía, Interior, Justicia y la participación de la Agencia Tributaria, ha elaborado un segundo borrador de Anteproyecto de Ley de firma electrónica, que reemplazará al Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica. Este nuevo texto es el resultado de una amplia consulta pública en la que han participado más de cincuenta entidades del sector, la Agencia de Protección de Datos, la Comisión del Mercado de las Telecomunicaciones, el Consejo de Consumidores y Usuarios, el Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información, el Colegio de Registradores de la Propiedad y Mercantiles de España y el Consejo General del Notariado, constatándose un gran interés por esta iniciativa.
Finlandia	Proyecto de ley de intercambio electrónico de datos en la administración y los procedimientos judiciales administrativos; Proyecto de ley por la que la Oficina del Censo actuará como certificador de clave pública.
Francia	Ley de telecomunicaciones (decretos de autorizaciones y exenciones): suministro de productos de firma digital sujeto a procedimiento de información, libertad de uso, importación y exporta-

	ción de productos y servicios de firma digital Normativa sobre utilización de la firma digital en los ámbitos de la seguridad social y la sanidad pública. Ley de firma digital
Italia	Ley general de reforma de los servicios públicos y simplificación administrativa promulgada: Principio del reconocimiento legal de los documentos digitales. Decreto de creación, archivo y transmisión de documentos y contratos digitales. Decreto regulador de productos y servicios, en preparación. Decreto sobre las obligaciones fiscales derivadas de los documentos digitales, en preparación.
Japón	Ley de Firmas Electrónicas y Certificaciones: Outline of Law Concerning Electronic Signatures and Certification Services
Malasia	Ley de firma digital, aprobada y pendiente de promulgación, que otorga efecto legal a su utilización y regula el licenciamiento de los certificadores de clave pública. Proyecto piloto de desarrollo de infraestructura de firma digital.
Países Bajos	Régimen voluntario de acreditación para los certificadores de clave pública, en preparación. Normativa fiscal que prevé la presentación digital de la declaración de ingresos. Proyecto de ley de modificación del Código Civil, en preparación.
Panamá	Ley 43 que regula los documentos y firmas electrónicas y las entidades de certificación en el comercio electrónico, y el intercambio de documentos electrónicos.

Perú	Ley de Firmas y Certificados Digitales Ley que regula la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.
Puerto Rico	Ley de Firma Digital Puerto Rico. S.B. 423 (No. 188). Aprobada el 7 de Agosto, 1998.
Reino Unido	Proyectos legislativos en materia de concesión de licencias voluntarias a los certificadores de clave pública y reconocimiento legal de la firma digital.
Singapur	Ley de Transacciones electrónicas
Venezuela	Ley sobre mensajes de datos y firmas electrónicas de Venezuela, con el objeto de otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.

2. Antecedentes NACIONALES

Una recopilación de este tipo de normativa en la República Argentina arrojó los siguientes resultados:

1. **Resolución MTSS N° 555/97 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL - Normas y Procedimientos para la Incorporación de Documentos y Firma Digital.** Define el documento digital, la fir-

ma digital, el certificador de clave pública, el certificado, la clave privada, la clave pública y establece que los documentos digitales se considerarán válidos y eficaces, surtiendo todos los efectos legales y probatorios cuando estén firmados digitalmente.

2. **Resolución SAFJP Nº 293/97 SUPERINTENDENCIA DE ADMINISTRADORAS DE FONDOS DE JUBILACION Y PENSIONES - Incorporación del Correo Electrónico con Firma Digital.** Establece que los CD-ROMs remitidos por las Administradoras de Fondos de Jubilaciones y Pensiones, debidamente identificados por el Sistema, serán válidos y eficaces, surtiendo todos los efectos legales y probatorios, a partir de la fecha y hora en que queden disponibles en las bandejas de entrada y que la firma electrónica o clave de seguridad habilitante para acceder al sistema poseerá el mismo valor legal que la firma manuscrita.

3. **Resolución SFP Nº 45/97 SECRETARIA DE LA FUNCION PUBLICA - Incorporación de Tecnología de Firma Digital a los Procesos de Información del Sector Público.** La SECRETARIA DE LA FUNCION PUBLICA adhiere y hace suyos los conceptos vertidos por el Sub-Comité de Criptografía y Firma Digital del CUPI en el documento "Pautas Técnicas en la Materia de Normativa de Firma Digital" y autoriza el empleo de ésta tecnología para la promoción y difusión del documento y la firma digitales en el ámbito de la Administración Pública Nacional.

4. **Resolución SFP Nº 212/98 SECRETARIA DE LA FUNCION PUBLICA -** Políticas de Certificación para el Licenciamiento de Autoridades Certificantes. La SECRETARIA DE LA FUNCION PUBLICA dicta los estándares de licenciamiento y operación de las autoridades certificantes de la Administración Pública Nacional.

5. **Decreto Nº 427/98 del PODER EJECUTIVO - Firmas Digitales para la Administración Pública Nacional.** Autoriza el empleo de la firma digital

en la instrumentación de los actos internos del Sector Público Nacional, que no produzcan efectos jurídicos individuales en forma directa. El Decreto fue redactado por el Sub-Comité de Firma Digital del CUPI ("Comité de Usuarios de Procesamiento de Imágenes"), convocado por el BANCO CENTRAL DE LA REPUBLICA ARGENTINA y del que participaron representantes de distintos organismos estatales.

6. **Resolución SFP N° 194/98 SECRETARIA DE LA FUNCION PUBLICA** - Estándares Aplicables a la Infraestructura de Firma Digital para el Sector Público Nacional del Decreto N° 427/98. La SECRETARIA DE LA FUNCION PUBLICA dicta los estándares de homologación de algoritmos criptográficos para la Infraestructura de Clave Pública de la Administración Pública Nacional.

7. **Resolución General CNV N° 345/99:** Incorpora al libro VIII otras disposiciones de las Normas (T.O. 1997) el Capítulo 23 Autopista de la Información Financiera.

8. **Decreto 1347/99:** regula sobre el Servicio de Conciliación Laboral Obligatoria (SECLO) del Ministerio de Trabajo y Seguridad Social.

9. **El proyecto enviado por el PEN** el 18 de agosto de 1999, el trabajo realizado los Doctores Horacio Lynch y Mauricio Devoto publicado por el CENIT (Centro de Investigaciones en Information Technology)

10. **Decreto N° 1023/2001:** permite a través de su artículo 21 la realización de las contrataciones comprendidas en el régimen en formato digital firmado digitalmente.

11. **Decreto N° 889/2001:** aprueba la estructura organizativa de la Secretaría para la modernización del Estado en el ámbito de la subsecretaría de la Gestión Pública, creando la Oficina nacional de Tecnologías de la Información y otorgándole competencias en materia de firma digital.

12. **Decreto N° 677/2001:** otorga a los documentos digitales firmados digitalmente remitidos a la Comisión Nacional de Valores de acuerdo con las reglamentaciones dictadas por ese organismo, similar validez y eficacia que los firmados en soporte de papel.

13. **Decreto N° 673/2001:** Crea la Secretaría para la Modernización del Estado en el ámbito de la Jefatura de Gabinete de Ministros, asignándole competencia para actuar como Autoridad de Aplicación del régimen normativo que establece la infraestructura de Firma Digital para el Sector Público Nacional y para la aplicación de nuevas tecnologías informáticas.

14. **Ley N° 25237:** a través del artículo 61 establece que la Sindicatura General de la Nación ejercerá las funciones de Organismo Auditante en el régimen de empleo de la firma digital en la instrumentación de los actos internos de la Administración Pública Nacional.

15. **La Ley de Firma Digital:** el proyecto de Ley de Firma Digital en la Argentina, recibió sanción definitiva con fuerza de ley por el Congreso Nacional con fecha 14 de Noviembre de 2001. La Ley N° 25.506 ha sido publicada en el Boletín Oficial N° 29.796 del 14 de diciembre de 2001. El Poder Ejecutivo Nacional reglamentará la nueva norma en un plazo de 180 días a partir de dicha publicación.

Está organizada en XI Capítulos y un Anexo en que se encuentran previstos los principios y fundamentos que hemos comentado en esta exposición. La Ley argentina de Firma Digital, en el Capitulo I, denominado de **Consideraciones Generales**, establece las principales definiciones en cuanto al objeto, alcances, validez y presunciones legales referidas a la firma digital.

Este proyecto de ley impone al Sector Público Nacional - Poder Ejecutivo, Poder Judicial y Poder Legislativo nacional – la obligación de digitalizar los documentos y la utilización de la firma digital. De manera tal que en un plazo no mayor a cinco años por lo menos el cincuenta por ciento de los expedientes

estén digitalizados y el cien por cien de los Decretos, Resoluciones, Sentencias, Leyes etc. se firmen digitalmente.

16. **Proyecto de Simplificación e Informatización de Procedimientos Administrativos *(PROSIPA)*:** en el contexto del Plan Nacional de Modernización, la Decisión Administrativa N° 118/2001 de Jefatura de Gabinete de Ministros implementa el proyecto mencionado en forma obligatoria para toda la Administración Pública Nacional. Sus objetivos contemplan el diseño e implementación de un nuevo modelo de gestión administrativa con soporte de firma digital y la adecuación de la normativa vigente en materia de tramitación administrativa a las nuevas tecnologías de gestión. La Secretaría para la Modernización del Estado es la Autoridad de Aplicación de la nueva norma.

17. **Decreto Reglamentario 2628/2002:** el Decreto, publicado en el Boletín Oficial del 20 de diciembre de 2002 establece para el ámbito federal lo que se da en llamar una Infraestructura de Firma Digital para ofrecer la autenticación y garantía de integridad para los documentos digitales o electrónicos y constituir de esa forma la base tecnológica que permita otorgarles validez jurídica, regulando el funcionamiento de los certificadores licenciados de manera de garantizar la adecuada prestación de los servicios de certificación. A tal fin crea un Ente Administrador de Firma Digital, encargado de otorgar las licencias a los certificadores, supervisar su actividad y dictar las normas tendientes a asegurar el régimen de libre competencia en el mercado de los prestadores y protección de los usuarios de Firma Digital, supliendo de esa forma una falencia que tenía la Ley 25.506

Por su parte, en su articulado regula la conformación de una Comisión Asesora para la Infraestructura de Firma Digital, con un equipo multidisciplinario de especialistas en la materia, con el fin de asesorar y recomendar a la Autoridad de Aplicación estándares tecnológicos, y otros aspectos que hacen al funcionamiento de

la mencionada Infraestructura, designando al efecto a la Jefatura de Gabinete de Ministros.

18. **La Resolución 176/2002 de Jefatura de Gabinete de Ministros** habilita el Sistema de Tramitación Electrónica para la recepción, emisión y archivo de documentación digital firmada digitalmente. Este sistema, que funcionará en el Departamento de Mesa de Entradas y Despacho de la Subsecretaría de la Gestión Pública, permitirá el ingreso y despacho de documentos vía correo electrónico firmado digitalmente, emitiendo los correspondientes acuses de recepción fechados y firmados en formato electrónico. Publicada en el Boletín Oficial del 15 de Abril del 2002.

19. **La Resolución 17/2002 de la Subsecretaría de la Gestión Pública** regula el procedimiento para tramitar la certificación exigida al Registro del Personal acogido al Sistema de Retiro Voluntario, habilitando la modalidad de tramitación mediante el empleo de documentación digital firmada digitalmente, en lo que constituye la digitalización de un trámite interno de la Administración Pública con el empleo de la tecnología de firma digital. Publicada en el Boletín Oficial del 15 de Abril del 2002.

20. **Decreto N°78/2002:** faculta a la Subsecretaría de la Gestión Pública a actuar como autoridad de aplicación del Régimen Normativo que establece la Infraestructura de Firma Digital para el Sector Público Nacional, como así también en las funciones de organismo licenciante en la materia.

Además exhorta a la Oficina Nacional De Tecnologías De Información a promover la utilización de Firma Digital en los organismos del Sector Público Nacional actuando como autoridad certificante y a:

- Entender en la elaboración del marco regulatorio del régimen relativo a la validez legal del documento y firma digital, así como intervenir en aquellos aspectos vinculados con la incorporación de

estos últimos a los circuitos de información del sector público y con su archivo en medios alternativos al papel.

- Ejercer las funciones de Organismo Licenciante de la Infraestructura de Firma Digital para el Sector Público Nacional.

21. **Decreto 283/2003:** que autoriza con carácter transitorio a la Oficina Nacional de Tecnologías Informáticas a proveer certificados digitales para su utilización en aquellos circuitos de la Administración Pública Nacional que requieran firma digital, de acuerdo a la política de certificación vigente.

3. Antecedentes PROVINCIALES (Mendoza)

- Con la aplicación de **la Resolución N° 54 / 99 y del Decreto – Acuerdo N° 1806 del 5 de octubre de 1999**, el Gobierno de la Provincia de Mendoza, a través del Comité de Información Pública (COM.I.P.) órgano dependiente de la Unidad de Reforma del Estado, adopta para el ámbito del Poder Ejecutivo Provincial el uso del **COBIT** (Objetivos de Control para la Información y Tecnología Relacionadas y sus posteriores actualizaciones), se adoptan además el uso de los **Estándares Tecnológicos de la Administración Pública Nacional** (E.T.A.P. y sus posteriores modificaciones) desarrollados por la Subsecretaría de Tecnologías para el Sector Público, dependiente de la Secretaría Administrativa – Legal y Técnica de la Gobernación de la Jefatura de Gabinete de Ministros y las **Normas de Seguridad de Sistemas de Información**, sus posteriores modificaciones y agregados.

- **Consejo Federal De La Función Pública / Convenio De Cooperación Y Asistencia Técnica:** considera dentro de sus premisas la política de reformar y modernizar el Estado, a fin de avanzar hacía un país capaz de recuperar su potencial de crecimiento y desarrollo y responder a las nece-

sidades de la ciudadanía con servicios efectivos y de calidad, requiere la acción conjunta del Estado Nacional y los Estados provinciales para llevar a cabo políticas concertadas de reforma básica y de modernización de las respectivas administraciones públicas, promoviendo asimismo la adhesión participativa de los otros poderes de gobierno y de los municipios. Por este convenio la Provincia reafirma su compromiso prioritario con el proceso de reforma y modernización de la Administración Pública para fortalecer las estructuras provinciales, y establece con esos fines relaciones de cooperación y asistencia técnica con la NACIÓN.

Además en su **ACTA COMPLEMENTARIA N° 1** el Señor Jefe De Gabinete De Ministros, D. Alfredo Néstor Atanasof y el Señor Gobernador De La Provincia De Mendoza, Ing. D. Roberto Raúl Iglesias, acuerdan entre otros puntos:

- OBJETIVOS DE LAS ACCIONES DE COOPERACIÓN: Comenzar la puesta en marcha de acciones centradas en el aseguramiento y modernización de los procesos básicos de gestión y administración de recursos, incorporando tecnologías que contribuyan a gestionar con efectividad, calidad y transparencia la administración gubernamental, a fin de facilitar el acceso de la población a los servicios del estado provincial.

- PROYECTO DE COOPERACIÓN: El primer proyecto de cooperación tendrá como objetivo la implementación de tecnología de firma digital en diversos trámites de gobierno. Para ello se definirá un trámite en particular a partir del cual desarrollar una prueba piloto con certificados emitidos por la Subsecretaría de la Gestión Pública de la Jefatura de Gabinete de Ministros. Con posterioridad se trabajará en la definición y la habilitación de alguna instancia del gobierno provincial como Autoridad de Registro y, con posterioridad, como Autoridad Certificante.

Los desarrollos legales anteriormente citados se encuentran en proceso de análisis y serán reconocidos como antecedentes en la propuesta de normativa legal contemplada en el Plan de Actividades del proyecto e-firma/mza.

4. Conclusiones y Propuestas

Ley de Adhesión.

Como primera medida, se estima conveniente emitir la norma legal fundante del resto del andamiaje jurídico sobre la materia, engarzando en la posibilidad que contempla la legislación nacional vigente, ley 25.506, art. 50, que expresamente dispone: "*Invitación. Invítase a las jurisdicciones provinciales a instrumentar los instrumentos legales pertinentes para adherir a la presente ley.*".

Así las cosas, la provincia debe contar con la ley de adhesión, la cual no reviste mayores dificultades técnicas, sin perjuicio de las variables políticas que correspondan ser evaluadas, atento al alto nivel de innovación que implica la implementación de la materia *sub examine*.

La mencionada ley 25.506, si bien es de alcance nacional (regula materia contemplada por el C.C.) y por lo tanto en sentido estricto no necesita de adhesión, siendo obligatoria; deja abierta la posibilidad de adhesión a los fines de su instrumentalización.

Ello por cuanto la materia de fondo constituye facultades delegadas al gobierno nacional (art. 75 inc. 12), pero la materia administrativa es de competencia local.

Decreto Reglamentario.

Así las cosas, el gobierno provincial debe proceder a emitir la norma correspondiente –decreto reglamentario de la ley de adhesión- a fin hacer operativa la norma básica.

Contenido básico del decreto reglamentario local.

Como dijimos, el dictado del decreto implica la instrumentalización concreta en el orden local de la legislación nacional referida.

Siendo competencia del Poder Ejecutivo (art. 128 inc. 2 CPr.), será éste quien deberá por lo tanto tomar las decisiones concretas que, plasmadas en el decreto, permitirán incorporar el producto elaborado.

Dicho decreto se estima deberá contener disposiciones mínimas referidas a los siguientes aspectos:

Determinación de la Autoridad de Aplicación.

En el orden nacional, la Autoridad de Aplicación es la Jefatura de Gabinete de Ministros. Sin embargo, su competencia queda restringida al ámbito de la Administración Pública Nacional (art. 100 CN), por lo cual no tiene atribuciones sobre las administraciones locales autónomas (cfr. Art. 5, 75 inc. 12, 121 ss y cc de la CN).

Por lo tanto, resulta de vital importancia la determinación de la autoridad de aplicación local, encargada entre otras cosas, de:

- determinar las normas y procedimientos técnicos para la generación, comunicación, archivo y conservación del documento digital o electrónico, según lo previsto por los arts. 11 y 12 de la ley 25.506.

- establecer los estándares tecnológicos y de seguridad aplicables en consonancia con estándares internacionales, los procedimientos de firma y verificación en consonancia con los estándares tecnológicos definidos conforme el inciso precedente, las condiciones mínimas de emisión de certificados digitales, los mecanismos que garantizarán la validez y autoría de las listas de certificados revocados, los procedimientos mínimos de revocación de certificados digitales cualquiera

que sea la fuente de emisión, y los procedimientos mínimos de conservación de la documentación de respaldo de la operatoria de los certificadores licenciados, en el caso que éstos cesen su actividad, el sistema de auditoría, las condiciones y procedimientos para el otorgamiento y revocación de las licencias, las normas y procedimientos para la homologación de los dispositivos de creación y verificación de firmas digitales, el procedimiento de instrucción sumarial y la gradación de sanciones previstas en la Ley N° 25.506, en virtud de reincidencia y/u oportunidad. los contenidos mínimos de las políticas de certificación de acuerdo con los estándares nacionales e internacionales y las condiciones mínimas que deberán cumplirse en el caso de cese de actividades de un certificador licenciado; etc.

Creación de un Comité Asesor.

Es recomendable la creación por vía decreto, de un organismo provincial con funciones de asesoramiento y consulta, en el ámbito de la autoridad de aplicación, legislando sobre su integración, funciones, etc.

Determinación de un organismo Administrador.

Dependerá de la Autoridad de Aplicación. Se trata de un ente técnico- administrativo encargado de otorgar las licencias a los certificadores y de supervisar su actividad, según las exigencias instituidas por la reglamentación y de dictar las normas tendientes a asegurar el régimen de libre competencia, equilibrio de participación en el mercado de los prestadores y protección de los usuarios. Deberá reglamentarse entre otras cosas, lo referido a su constitución, autoridades, funciones, recursos, etc.

Implementación de un Sistema de Auditoría.

Causales de revocación de certificados digitales.

Obtención de licencias por los certificadores.

Así también lo referido a Seguros, responsabilidad, recursos, servicios de terceros, etc.

Contenido mínimo de políticas de certificación.

Dictado de otras normas reglamentarias.

Tales las exigidas por la Autoridad de Aplicación, referidas especialmente a su funcionamiento interno.

Anexo IV

e-firma/mza

Análisis de Factibilidad Técnica

1. Introducción

En este anexo se informa sobre los resultados de la investigación y pruebas preliminares realizadas para ***determinar la factibilidad técnica*** de implantación de una Infraestructura de Clave Pública (PKI) diseñada para implementar y difundir el uso de los Certificados Digitales y la firma digital en el ámbito del Gobierno de Mendoza, a los fines de brindar los siguientes servicios:

- Correo electrónico seguro, firma digital y no repudio.
- Autenticación de identidad: de Servidores (sitio seguro) y de clientes (control de acceso).
- Canal Seguro (SSL).
- Secure Desktop – Cifrado de archivos (acuerdo de clave privada mediante clave pública).
- Secure e-forms: firma digital y seguridad para formularios basados en web.
- Encripción de bases de datos.
- Seguridad de aplicaciones sobre intranets y extranets.

El cuerpo del informe está dividido en tres bloques. El primero de ellos especifica las dimensiones y localización óptima propuestas para una primera instancia de implantación de la PKI en términos técnicos. El segundo bloque, resume esquemáticamente la ingeniería de proyecto. En dicho estudio, se intenta describir un diseño preliminar para la infraestructura y se proponen distintos escenarios de plataforma tecnológica alternativos para la implementación real de cada propuesta. Finalmente, se presenta un breve análisis de los recursos humanos necesarios para la administración y mantenimiento de la tecnología de soporte a la PKI y se resumen las principales conclusiones y sugerencias del estudio, las cuáles emiten una recomendación final sobre el camino a seguir para un diseño detallado e implementación real del proyecto.

2. Objetivos del estudio

El presente estudio tiene por objetivo, sugerir un modelo de arquitectura PKI, un plataforma tecnológica y una estructura de soporte técnico adecuadas para implantar una infraestructura de clave pública operativa en el ámbito de la Administración Pública de la provincia de Mendoza, constituyendo un sistema técnicamente confiable, ajustado a los estándares tecnológicos y operativos propuestos en el marco regulatorio de la actividad (Res. 194/98); por la Autoridad de Aplicación (Jefatura de Gabinete de Ministros); y a los estándares internacionales, de modo tal de:

- Garantizar la confiabilidad, confidencialidad, integridad y disponibilidad permanente de los datos. En particular:
    - garantizar la seguridad en el mantenimiento de la confidencialidad de los datos de creación de una firma digital, el par de claves y los documentos digitales que así lo requieran
    - garantizar la disponibilidad permanente de la información de carácter público que la infraestructura debe proveer: Lista de Certificados Revocados (CRLs), Políticas de Certificación, Información de Auditoría, Manual de Procedimiento, otros.
- Garantizar la interoperabilidad de los sistemas y sus posibilidades de integración a la mayor cantidad de aplicaciones y plataformas posibles
- Garantizar la escalabilidad de la PKI.

3. Tamaño Óptimo

El parámetro fundamental desde el cual se parte habitualmente para dimensionar tecnológicamente una infraestructura de clave pública es el ***volumen de certificados*** que la misma va a administrar.

Definiendo claramente este parámetro, junto a otros como los ***tipos de aplicaciones*** o servicios PKI que se van a soportar y el ***tipo de usuarios*** (personas y equipos), a los cuales la misma está destinada; es factible definir claramente un diseño acabado para la infraestructura; determinando puntualmente la capacidad de los servidores, unidades de almacenamiento, tecnologías de bases de datos, dispositivos de comunicaciones, y toda la tecnología asociada.

Los alcances definidos en el presente proyecto contemplan una ***PKI de propósito general*** que brinde los servicios de la criptografía de clave pública y la firma digital a la Administración Pública de la Provincia de Mendoza. En este contexto, sería erróneo dimensionar, para una primera experiencia de implantación, una infraestructura tecnológica que soporte el volumen final de certificados que potencialmente se gestionarían en el transcurso del tiempo en el Gobierno de Mendoza. Un planteo de este tipo, además de ser ineficiente en términos de la inversión económica necesaria, sería inviable también en términos de obsolescencia tecnológica, de capacidades de recursos humanos capacitados, de capacidades de conectividad y otra gran cantidad de factores que condicionan la búsqueda de otros mecanismos de dimensionamiento.

Por lo expuesto, consideramos que la mejor alternativa es definir una infraestructura de clave pública de ***pequeña escala***, que en principio pueda ser aplicada eficazmente, con todos sus servicios, a uno o dos circuitos administrativos que reúnan las condiciones mínimas para demostrar las ventajas del uso de esta tecnología en la gestión pública, como experiencia concreta de modernización del Estado.

Consistentemente con este planteo, todo el cuidado en el diseño de la infraestructura de soporte tecnológico, deberá estar puesto en la ***ESCALABILIDAD*** de la arquitectura propuesta, de modo de garantizar la posibilidad de un crecimiento gradual en el tiempo, que no implique grandes cambios ni conversiones.

Por ***pequeña escala***, entendemos una PKI que pueda gestionar eficientemente un rango de entre ***500*** y ***1000*** certificados emitidos a usuarios finales; y un rango de entre ***20*** y ***40*** certificados de servidor, con los siguientes propósitos:

- Correo electrónico seguro, firma digital y no repudio
- Autenticación de identidad: de Servidores (sitio seguro) y de clientes (control de acceso)
- Canal Seguro (SSL)
- Secure Desktop – Cifrado de archivos (acuerdo de clave privada mediante clave pública)
- Encripción de bases de datos

4. Localización Óptima

En función de una valoración de los requerimientos de espacio físico, condiciones de conservación y medidas de seguridad física necesarias para la instalación de los servidores y dispositivos de comunicaciones que deberían conformar la plataforma tecnológica central de la PKI, sugerimos su implantación en las dependencias de la Gobernación, con una estrecha vinculación a las oficinas de la Unidad de Reforma del Estado de la provincia.

Esta propuesta, se sustenta además en condiciones operativas, vinculadas a la disponibilidad de recursos humanos capacitados y al apoyo político necesario para lograr el éxito en la implantación.

5. Ingeniería de Proyecto

5.1. Modelo de arquitectura PKI

Tal como lo propone el documento presentado por RedIRIS en las Jornadas Técnicas de Pamplona 2001 (gti-pca@rediris.es), existen actualmente en el mundo diferentes topologías PKI que se ajustan en mayor o menor medida a uno de los tres modelos siguientes, cuyas ventajas y desventajas hemos evaluado cuidadosamente en función del marco definido por el presente proyecto, a fin de decidir cuál es la estructura más recomendable para nuestra implantación.

5.1.1. Autoridad Certificante Única

Bajo este modelo existe una única Autoridad Certificante (CA) que emite todos los certificados, cualquiera sea su uso, tanto a personas como a computadoras o dispositivos.

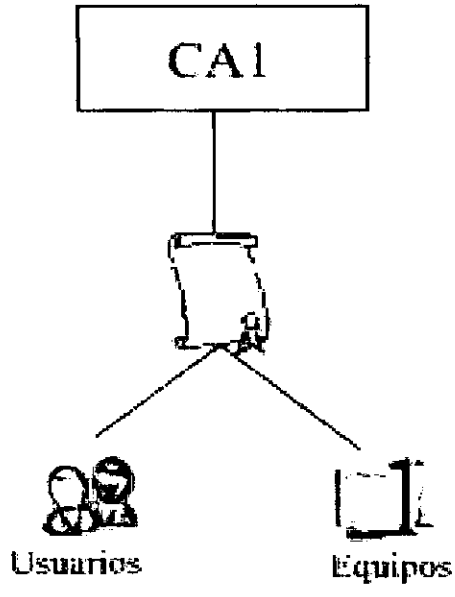


Figura 1 – Autoridad Certificante Única

Esto implica la existencia de un punto de confianza único, lo cual es ventajoso desde el punto de vista de la performance de la PKI; ya que no se necesita recorrer rutas para validar la confianza de un certificado. Sin embargo, es poco seguro en cuanto a la disponibilidad permanente de una ruta de confianza, ya que si la CA única falla, se cae toda la infraestructura.

Una ventaja de este modelo es que es fácil de implementar, pero como contrapartida es difícil de escalar.

5.1.2. Arquitectura Jerárquica

En una arquitectura jerárquica se definen relaciones de confianza unidireccionales entre una Autoridad Certificante Raíz, posiblemente licenciada a su vez por un Organismo Licenciante (OL) de mayor jerarquía; y uno o más niveles de autoridades certificantes (CAs) subordinadas.

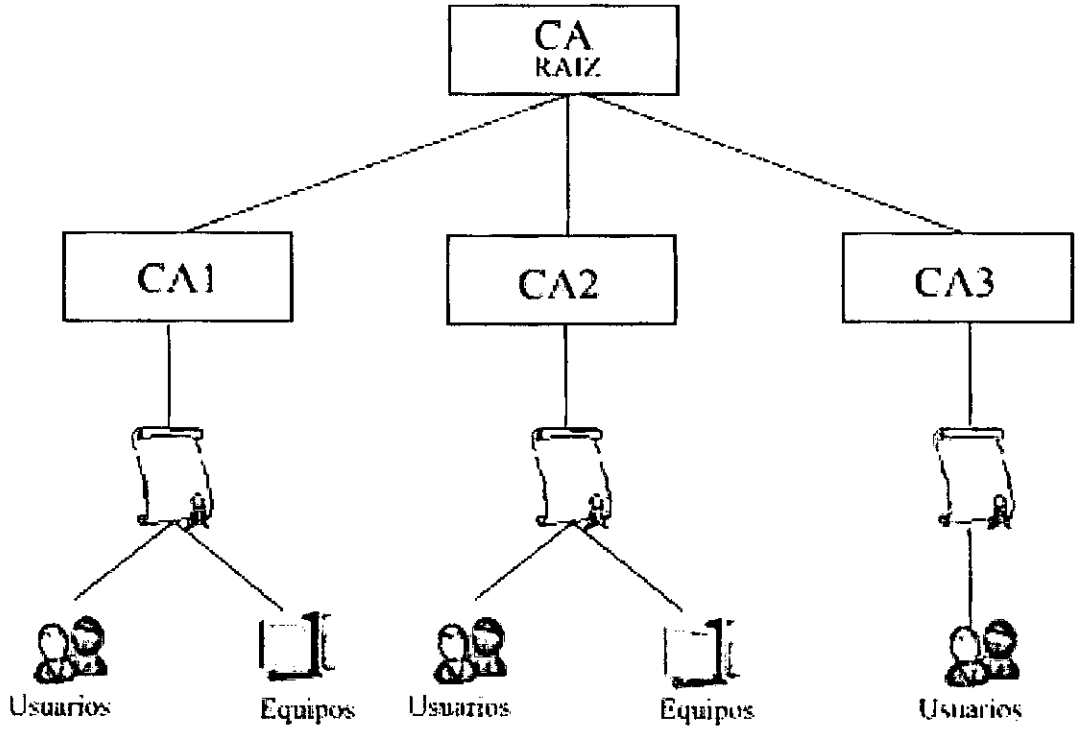


Figura 2 – Arquitectura Jerárquica

Este enfoque, quizá el más aceptado mundialmente, presenta importantes ***ventajas*** que debemos considerar:

- Facilita la escalabilidad y flexibilidad del modelo: es factible ir creciendo gradualmente en número de CAs subordinadas. Así mismo se puede escalar con un criterio de división de CAs por propósitos de los Certificados que emiten, por razones geográficas, por razones de estructura organizacional, etc.
- Al ser las relaciones de confianza unidireccionales, los caminos de certificación son fáciles de desarrollar y relativamente cortos (*Camino más largo = profundidad del árbol + 1).* En este sentido se debe tener cuidado en la manera como se escala la jerarquía, en cuanto a los niveles de profundidad y el ensanchamiento horizontal del árbol. Es decir se debe prever un crecimiento ordenado.

Como ***desventajas*** fundamentales la teoría contempla:

- La existencia de un único punto de confianza (CA raíz), aunque se mejora la total dependencia de la CA que se da en el modelo de CA única.
- Las imposibilidades operativas que eventualmente pueden presentarse para acordar políticas entre las distintas CAs subordinadas a una única CA raíz.

5.1.3. Estructura basada en "Red de confianza"

Este enfoque, propone la interconexión a través de certificación cruzada, de múltiples Autoridades Certificantes, constituyendo una malla o red.

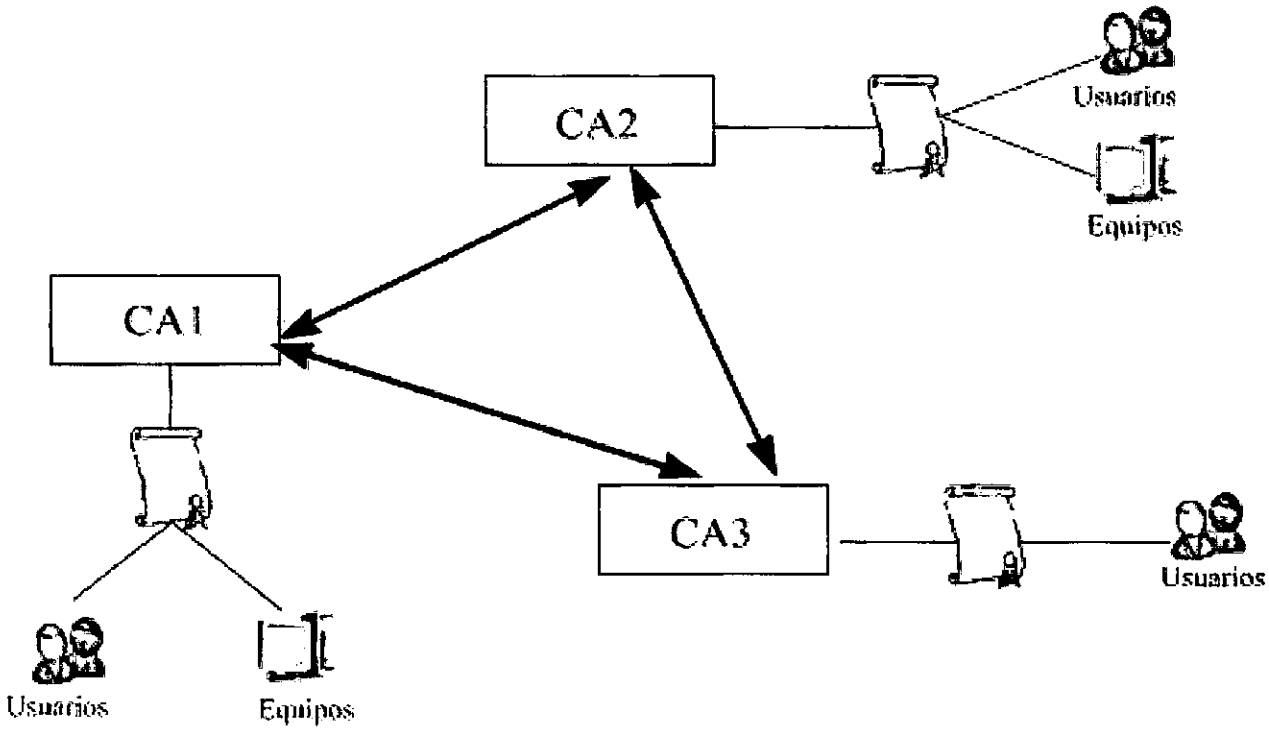


Figura 3 – Arquitectura en Red

Como ***ventajas*** de esta topología se mencionan:

- La flexibilidad, ya que puede crecer ampliamente incorporando nuevas comunidades de usuarios.
- La existencia de múltiples puntos de confianza, lo que trae aparejado mejores condiciones de disponibilidad ante la caída de alguna de las CAs involucradas.

Pero son ***desventajas*** muy críticas:

- La posible existencia de caminos de certificación largos y complejos (no determinísticos) y con posibles bucles. Esto puede ser devastador para la implantación.
- Mayores dificultades de control de políticas de seguridad y usos de certificados.

5.1.4. El modelo propuesto para la PKI provincial

Como lo hemos planteado desde los objetivos del presente estudio, es nuestra intención proponer un diseño técnicamente confiable y ajustado a los estándares nacionales e internacionales de modo de garantizar confiabilidad, confidencialidad, integridad y disponibilidad permanente. Así mismo, hemos propuesto como premisas fundamentales para el modelo, asegurar la escalabilidad y la interoperabilidad con la mayor cantidad de aplicaciones posibles.

Estos objetivos, en el marco del análisis de estructuras previo, y tomando en cuenta las dimensiones que se definieron en el *punto 3. Tamaño Óptimo*, implican considerar el diseño de una infraestructura de pequeña escala, lo que no amerita en principio la existencia de más de una Autoridad Certificante (CA) y alternativamente una o más Autoridades de Registro (RA), pero que contemple un mecanismo de ***crecimiento gradual y ordenado*** ajustado a políticas y procedimientos unívocos o al menos con un alto grado de consistencia.

Es fundamental considerar, en relación a este último punto, que nuestro proyecto contempla la inclusión en la PKI de grupos de usuarios y entidades que pertenecen a ***una misma organización institucional***, el Gobierno de la Provincia de Mendoza. Por esto debe existir coherencia en los modelos de implementación, las políticas de certificación y los manuales de procedimientos.

Bajo estas consideraciones proponemos el siguiente diseño preliminar de PKI provincial:

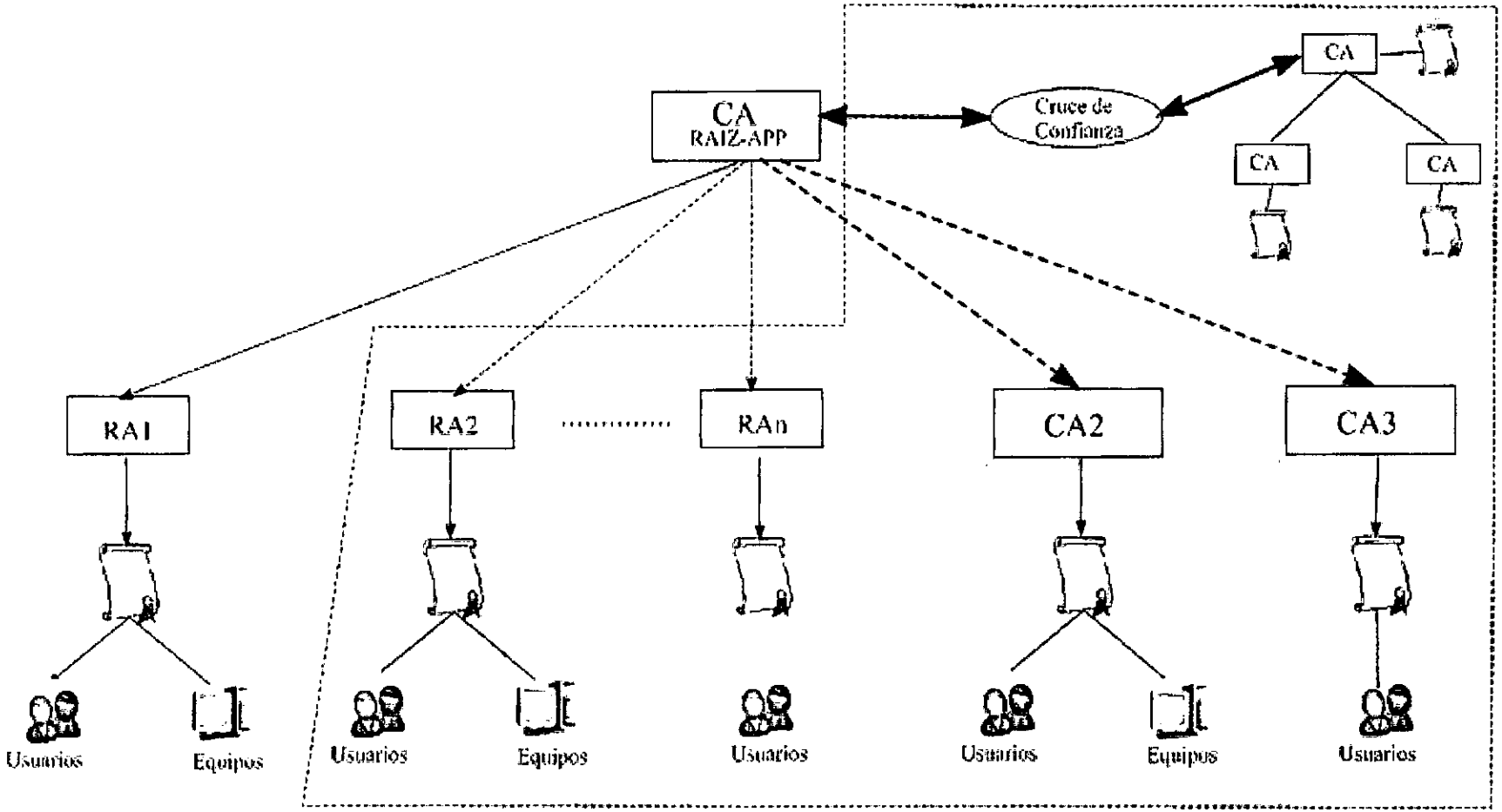


Figura 4 – Esquema de diseño preliminar propuesto para la PKI provincial

Importante: La parte sombreada prevé como debe escalar el modelo. La implementación inicial propuesta, sólo contempla una CA y una RA.

El modelo precedente propone una **implantación inicial** de:

- ***Una Autoridad Certificante (CA):*** que permita el manejo del ciclo de vida de certificados , a través de la solicitud, aprobación, renovación, auditoría y revocación de certificados
- ***Una Autoridad de Registro (RA):*** que permita desarrollar funciones, tales como aprobación de certificados, remisión de solicitud aprobada a la CA, auditoría, manejo de las solicitudes de revocación y otras; de manera distribuida entre un número ilimitado de administradores, asegurando la separación de roles.
- Sistemas totalmente redundantes acordes a un Plan de Contingencia, de modo de prever la posible caída del punto único de confianza.
- Sistema de recupero ante desastres.
- Disponibilidad total las 24 horas del día, 7 días por semana, 365 días al año.
- Plena seguridad sobre la red y los datos. Enlaces altamente confiables.

Y prevé un **modelo de escalabilidad jerárquico** con las siguientes características:

- Posibilidad de agregar nuevas Autoridades de Registro, eventualmente con funciones distribuidas por Organismo de Gestión o Ministerio; ó alternativamente por tipo de certificados que gestionan.
- Posibilidad de subordinar a una CA Raíz, otras Autoridades Certificantes que se ajusten a políticas, estándares y procedimientos consistentes. Esto tiene por objetivo, proveer al modelo de mecanismos de división de la carga de trabajo, mejora de performance, actualización tecnológica, distribución de roles, aseguramiento de la disponibilidad del sistema, etc.
- Eventual posibilidad de interconectar a la jerarquía provincial con otras PKI jerárquicas o en red a través de un Bridge o puente de confianza. *(Ver Federal Bridge Certification Autority of USA* – http://www.cio.gov/fpkisc*)*

5.2. Especificaciones funcionales que debe satisfacer la Infraestructura de Clave Pública

Teniendo en cuenta las expectativas expresadas en el diseño preliminar de la PKI provincial que se presentó en el punto anterior, se expone a continuación una vista de los requerimientos funcionales que a partir de la investigación preliminar se ha determinado, debería satisfacer la ***solución tecnológica*** que se adopte, de modo de garantizar los requisitos preestablecidos de seguridad, disponibilidad, flexibilidad, interoperabilidad y escalabilidad.

Esta lista de requerimientos no pretende ser una enumeración taxativa y acabada, ni un diseño detallado de las especificaciones funcionales de la PKI; sino un recorte de aquellos aspectos que se consideran más relevantes a tener en cuenta.

La misma, constituye una guía orientadora para evaluar a priori, y a los fines del estudio de factibilidad técnica, las distintas alternativas de implantación tecnológica que se postulan en la presente ingeniería de proyecto.

5.2.1. Seguridad de la clave privada de la CA

- Almacenamiento seguro mediante un dispositivo en hardware (HSM) de la clave privada de la CA que se ajuste al estándar FIPS 140-1 de nivel 3.
- Restricciones de Copyrigth que prevengan la distribución de la clave raíz de la CA.
- Reinicio de todos los servicios de la PKI luego de una caída del servidor de la CA sin compromiso de la clave de administrador ni otras claves maestras.
- Duplicado y recuperación, en caso de desastre, de la clave de la CA, con un sistema altamente seguro de puesta en común de información secreta entre múltiples partes, mediante la utilización de "k de n" tarjetas inteligentes.

5.2.2. Par de claves

- Posibilidad de generación centralizada de claves, backup de las claves privadas y la recuperación distribuida de claves.

- Esquemas de pares de claves duales: Alternativamente, se debe proveer a los usuarios dos pares de claves con fechas de expiración independientes: uno para firma y otro para cifrado. De este modo, se puede mantener un back-up (copia de resguardo) de las claves privadas de cifrado, de modo tal que documentos cifrados históricos puedan ser recuperados en el tiempo. La clave privada de firma sólo existirá durante la validez de un certificado emitido a un usuario final, de modo tal de garantizar no repudio.
- Posibilidad de que el administrador pueda especificar fechas de vencimiento independientes para la firma de la clave privada y la comprobación de la clave pública, de modo que las comprobaciones puedan tener éxito después de que la clave de firma expira.

5.2.3. Protección de claves privadas

- Protección de las claves privadas de usuarios finales, servidores o dispositivos de red con por lo menos, un esquema basado en password. Dicho sistema debe mantener reglas estrictas en cuanto a la generación de password que indiquen longitud, formato, fecha de finalización, etc.). Estas reglas deben poder ser configurables por el administrador central. Dichas password no pueden ser almacenadas como texto en claro (sin cifrar) en ningún sitio, ni ser transmitidas como texto en claro por la red bajo ningún motivo.
- Soporte a la autenticación mediante: passphrase o PIN; dispositivos biométricos y smart cards.

5.2.4. Resguardo y recuperación de claves de cifrado

El resguardo y recuperación de claves de cifrado es muy importante para asegurar que la Administración Pública Provincial siempre será capaz de desencriptar la información que le es propia, manteniendo el control sobre la misma.

- Resguardo y recuperación de claves de cifrado.
- Recuperación de una clave de usuario para cifrado ante la pérdida de la misma.

- Recuperación del histórico de claves de un usuario ante la pérdida de una de las claves.
- Recuperación de claves mediante la presentación de m de n cerfiticados de administrados, de modo tal de garantizar el proceso de recuperación de claves.

5.2.5. Gestión de Certificados

- Interfaz web para que los usuarios finales puedan enviar solicitudes de enrolamiento, solicitudes de renovación, solicitudes de revocación, descargar las CRLs, etc.
- Administración automatizada que permita la autenticación y revocación transparente de usuarios o dispositivos, utilizando directamente sistemas administrativos o bases de datos preexistentes.
- Aprobación manual de solicitudes de emisión de certificados.
- Emisión de cerfiticados para SSL, S/MIME y Object signing.
- Soporte a la inclusión de extensiones propias y personalizadas a los certificados emitidos por la CA, sobre un modelo de información básico.
- Soporte a la emisión masiva de certificados.
- Posibilidad de exportar e importar certificados y, alternativamente su par de claves asociadas como un mensaje cifrado, mediante contraseña proporcionada por un responsable.

5.2.6. Revocación de Certificados

- Interfaz web para que los usuarios finales puedan enviar solicitudes de revocación de sus certificados personales.
- Actualización y emisión automática de la Lista de Certificados Revocados (CRL) inmediatamente después de que un certificado ha sido revocado, de modo de garantizar plena actualización del estado de los certificados.
- Posibilidad de descarga de la CRL por parte de los usuarios para incorporarla a sus aplicaciones y hacer validaciones de certificados revocados off-line.
- Logs o seguimiento de la frecuencia de actualización de las CRLs.

- Posibilidad de revocación de certificados expirados de modo tal que puedan ser incluidos en las listas para verificación de firmas históricas. Es decir posibilidad de incluir certificados expirados en las CRLs.
- Ante una revocación por compromiso de la clave, posibilidad de ingresar una fecha que indique la última fecha cierta en la que la clave se supo no comprometida, de modo tal que esta información pueda ser tenida en cuenta por el usuario ante una comprobación de validez del certificado.
- Posibilidades de revocación manual (por parte del administrador) y automática.
- Posibilidad de revocación masiva de certificados.

5.2.7. Actualización de Clave y actualización de Certificados

- Interfaz web para que los usuarios finales puedan enviar solicitudes de renovación de sus certificados personales.
- Soporte a la actualización automática de certificados y claves de forma transparente al usuario final.
- Actualización simultanea del par de claves junto al certificado, de modo tal de asegurar la rotación de claves.
- Tiempo de vida de los certificados configurables de acuerdo a las políticas de seguridad que se definan.
- Almacenamiento automático en un archivo histórico de las claves privadas de cifrado cuando los usuarios actualizan su par de claves.

5.2.8. Repositorio de certificados / Base de datos de la CA

- Chequeo de la integridad de datos que asegure el mantenimiento adecuado de los datos de enrolamiento de los usuarios.
- Backup periódico de la base de datos de la CA fuera de horarios picos, con previo chequeo de la integridad de los datos que se resguardan.
- Encripción de la base de datos para almacenamiento seguro.

5.2.9. Mecanismos de gestión del servicio de directorios

- Servicio de directorio que permita administrar automáticamente certificados y listas de certificados revocados en directorios compatibles con LDAP.
- Publicación automática de los certificados emitidos en el servicio de directorio de la CA, de modo de asegurar la inmediata disponibilidad de los certificados para otros usuarios.
- Función de recuperación del directorio en caso de fallo.
- Integración de listas de certificados y listas de certificados revocados en directorios compatibles con LDAP.
- Soporte a la comunicación con múltiples servidores LDAP, para balancear la carga de trabajo, garantizar redundancia y proveer escalabilidad.

5.2.10. Certificación cruzada

La certificación cruzada es importante tanto dentro del dominio de control de la Administración Pública como con Autoridades Certificantes externas que sean validadas desde el punto de vista de una jerarquía de confianza. Esto tiene importantes implicancias tanto en los enfoques de interoperabilidad como de disponibilidad.

- Soporte a certificación cruzada con propósitos de lograr interoperabilidad y flexibilidad.
- Inclusión de extensiones personalizadas en la emisión de cerfiticados curzados generados por la CA.
- Revocación de certificados de CA cruzados, en caso de deterioro de la confianza o relación con la otra CA, e impacto inmediato de la revocación sobre los usuarios afectados.
- Aprobación de certificación cruzada mediante la presentación de m de n certificados de administrador.
- Posibilidad de que ante una caída de la CA raíz de la jerarquía, las CA subordinadas reestablezcan rápidamente su confianza en otro par de CAs.
- Tiempo de vida flexible para los certificados cruzados.

5.2.11. Gestión de reportes y pistas de auditoría

Mantener un registro administrativo de las acciones desarrolladas en la PKI es una característica fundamental que la solución debe satisfacer. El seguimiento de las transacciones en las que se basan los certificados se debe realizar a través de registros de auditoría, reportes y prácticas de seguridad auditables. Para ello se requiere:

- Generación auditable de la clave raíz .
- Historial completo de cada clave generada.
- Log de transacciones del o los administradores centrales.
- Reporte de certificados emitidos a una fecha y con una fecha de caducidad determinada.
- Logs y reportes exportables para ser integrados en otras aplicaciones mediante interfase ODBC o para ampliar facilidades de consulta (SQL query).
- Otros logs de transacciones tales como: habilitación y baja de usuarios, recuperación de certificados, cambios de nombres (DN) y certificados pendientes de aprobación.
- Posibilidad de programar (schedule) la generación de reportes.
- Logs o seguimiento de la frecuencia de actualización de las CRLs.

5.2.12. Configuración de políticas de acceso a la PKI

- Configuración de tiempo límite de login de un usuario a la PKI y sus servicios de usuario.
- Configuración de la cantidad de intentos fallidos de login.
- Configuración de intervalo de tiempo transcurrido antes de permitir un nuevo login.

5.2.13. Servicio de Time stamping:

Con propósitos de no repudio es deseable que la PKI preste el servicio de sello de fecha y hora asociado a la firma. Dado que no se puede confiar en el reloj de cada PC, este servicio debe ser brindado desde un servidor de Time Stamping. Es deseable que la solución sea capaz de prestar servicio de time stamping para firmas DSA y firmas RSA. Sería deseable también compatibilidad con tokens

PKIX. Se deberán llevar además logs de transacciones y pistas de auditoría de las operaciones de time stamping.

5.2.14. Integración con aplicaciones comunes:

Los certificados emitidos deben poder incorporarse y ser usados en las aplicaciones clientes típicas tales como outlook, outlook express, lotus notes, IE, Netscape communicator, etc. Para garantizar esto la solución debe proveer integración abierta con la mayor cantidad de aplicaciones y servicios de Internet, basada en los estándares del mercado, como X509 v3, LDAP, PKCS#7, PKCS#10, PKCS#12 y PKIX.

5.2.15. Condiciones de interoperabilidad

- Interoperabilidad testeada con los proveedores de servicios de certificación más importantes a nivel mundial: IBM, Verisign, GlobalSEt, Entrust, etc.
- Soporte a múltiples conjunto de caracteres para lenguajes internacionales.
- Integración abierta con la mayor cantidad de aplicaciones y servicios de Internet, basada en los estándares del mercado, como X509 v3, LDAP, PKCS#7, PKCS#10, PKCS#12 y PKIX.
- Soporte integral de todos los tipos de certificados estándar, incluyendo SMIME, SSL y IPSec (este último solo se considera por si en un futuro se escala a servicios de transacciones de comercio electrónico seguras bajo el estándar SET).

5.2.16. Condiciones de escalabilidad

- Soporte a la comunicación con múltiples servidores LDAP, para balancear la carga de trabajo, garantizar redundancia y proveer escalabilidad.
- La solución debe proveer un mecanismo escalable de gestión de certificados revocados de modo tal que no haya degradación de performance cuando el número de usuarios aumenta.

5.3. Ajuste a estándares

A continuación se especifican los estándares de la industria a los que deberá ajustarse la solución tecnológica que se adopte para garantizar los requisitos preestablecidos de seguridad, escalabilidad e interoperabilidad; así como también para cumplir con las condiciones legales impuestas en la Ley 25.506, su decreto reglamentario y demás disposiciones vigentes.

Característica o Servicio	Especificación de normas y estándares
Algoritmo de generación del par de claves	- 2048 bits (RSA) [PKCS#1] - 1024 bits (RSA/DSA)
Algoritmo de firma	- Md5withRSAEncryption con longitud de clave igual o superior a 1024 bits (RSA) - Sha1withDSAEncryption con longitud de clave igual o superior a 1024 bits (DSA)
Algoritmo simétrico de encriptado de clave privada	- TripleDES [X9.52] en sus distintos modos de operación CBC, CFB, OFB con longitudes de claves de 112 y 168 bits - IDEA con bloques de 128 bits e idénticos modos
Gestión de las solicitudes de certificados	- Las solicitudes desde el CL (Certificador Licenciado) hacia el Ente de Licenciamiento deben remitirse en formato DER o PEM (ISO25-1) - Las solicitudes desde los usuarios hacia el CL (Certificador Licenciado) deben ser remitidas en formato [PKCS#10] o alternativamente pueden utilizarse otros formatos o mecanismos que permitan generar la solicitud desde los navegadores de Internet, siempre y cuando se pueda garantizar que el solicitante posee la clave privada correspondiente a la clave pública incluida en la solicitud y que dichas claves han sido

	generadas con las condiciones impuestas en las especificaciones propuestas en el presente estudio. - Las solicitudes deben ser verificadas del modo que lo describe la sección 2.3 (Proof of Possession POP of Private Key) en Internet X.509 Public Key Infraestructure Certificate Managemente Protocols [PKIX-CMP]
Gestión de Certificados	- Emisión de certificados con el formato establecido en la norma X.509 v3 según el estándar ISO/IEC/ITU X.509 cuyos datos y formatos se ajusten a lo requerido en el apartado 4.2.2.2. de la Resolución 194/98 - Los certificados deben soportar el uso de extensiones (Key usage, basic constraint) según la norma X.509 v3 - Los mecanismos de revocación de certificados deben ajustarse a la norma X.509 [PKIX1] - El formato de entrega de los certificados para la integración con distintas aplicaciones debe ser PEM o DER [ISO25-1] - Identificación única del certificado de un titular, en un formato compatible con la norma X.520 - El periodo de validez, debe consignar fecha y hora expresada en Coordinated Universal Time (UTC) - Identificación del emisor de un certificado, en un formato que se ajuste a la norma X.520
Gestión de certificados para Servidores	Soporte a la emisión y gestión de certificados para servidores de aplicaciones de Internet sobre el protocolo HTTPS u otros servicios utilizando el protocolo TLS o SSL v3
Gestión de la lista de Certificados Revocados (CRL)	Debe ajustarse a la norma X.509 v2
Logs de transacciones, Registros de	Debe llevar logs completos y registros

Auditorías y Reportes	de auditoría de todas las actividades y transacciones realizadas en el ámbito de la Autoridad de Certificación y Autoridad de Registro.
Servicios de Directorio	El servicio de directorio debe permitir insertar automáticamente certificados y listas de certificados revocados en directorios compatibles con el protocolo LDAP
Servicio de TimeStamp (TSA: Time Stamp Authority)	Compatible con el estándar definido en [PKIX-TS]
Servicio de Notariado	De acuerdo a la norma Internet X.509 Public Key Infraestructure Data Certification Server Protocols [PKIX-DCS]
Transmición de mensajes en aplicaciones de correo electrónico	Compatible con el estándar [SMIME]
Protocolos de transmisión en línea segura	1. [PKIX-TSL] (Transport Layer Security) 2. SSL versión 3

Tabla 1 – Definición de Estándares

5.4. Alternativas de adquisición de plataforma tecnológica

Se presentan a continuación dos ***soluciones tecnológicas*** alternativas para la implantación de una PKI acorde al diseño y especificaciones funcionales propuestas. Las mismas se analizan en sus dimensiones de hardware, software, protocolos de comunicación y de seguridad. Se ha priorizado también el ajuste a estándares internacionales que garantizan seguridad e interoperabilidad testeada.

5.4.1. Alternativa 1: Tercerización de la plataforma tecnológica de soporte a la PKI en una empresa de servicios PKI

Uno de los escenarios posibles, que no podemos dejar de considerar en el presente estudio de factibilidad, es la alternativa de delegar en una empresa de

servicios PKI todo el soporte y gestión de la plataforma tecnológica necesaria para lograr una PKI operativa en los términos descriptos.

Existen en el mundo múltiples empresas especializadas en los servicios de certificación digital y firma digital, que se han constituido en la solución para múltiples organizaciones y Gobiernos. En los estudios preliminares se evaluaron las soluciones propuestas por Verisign Inc. (www.verisign.com) y Entrust Inc. (www.entrust.com) dos de las empresas más importantes a nivel mundial con presencia en los Gobiernos de Chile, España, Canadá y EE.UU. entre otros.

La siguiente figura ilustra el esquema de implantación de nuestra Autoridad Certificante y Autoridad de Registro, bajo un escenario de tercerización total de la infraestructura tecnológica.

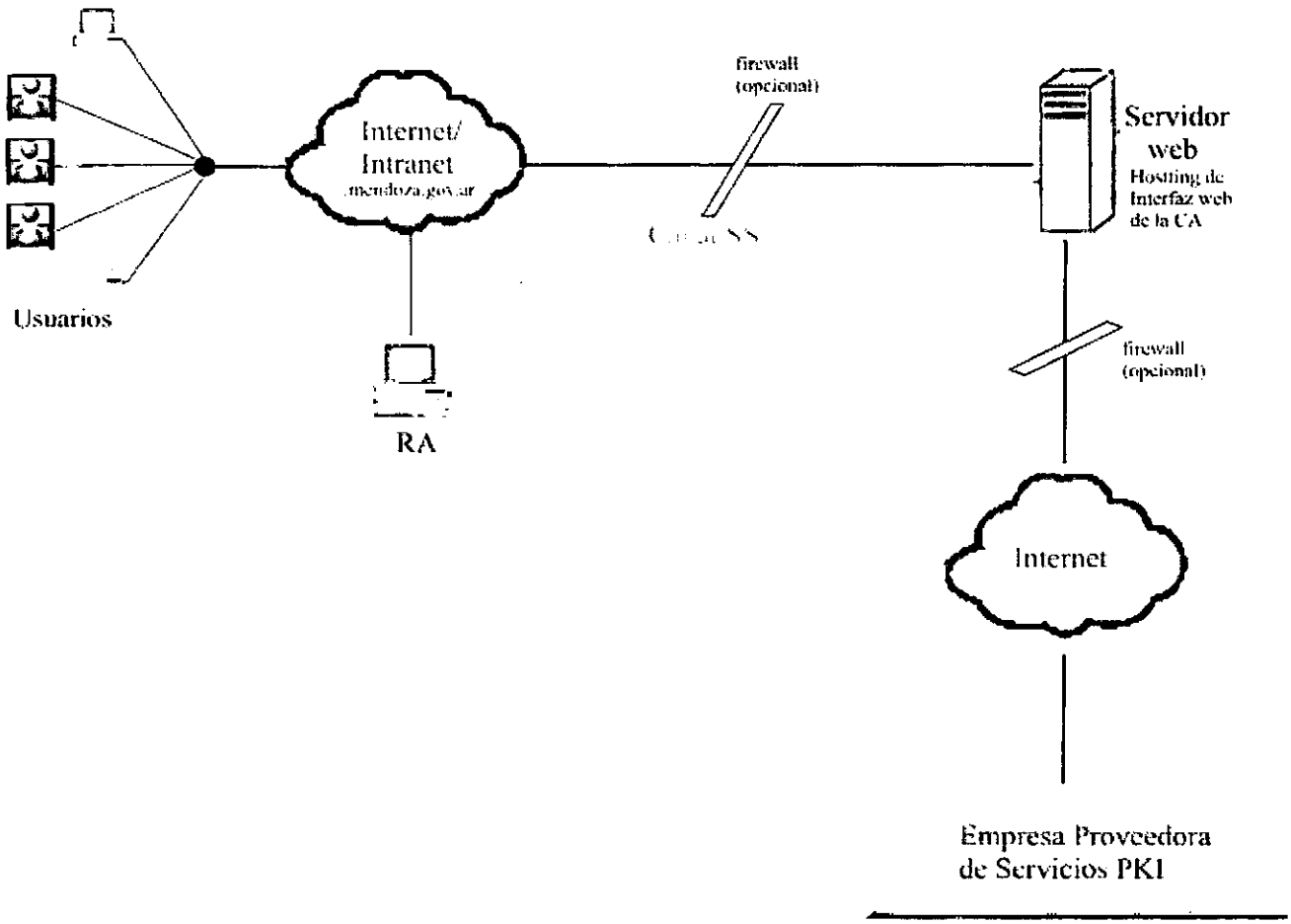


***Figura** 5 – Esquema de soporte tecnológico externo*

Esta solución delega en una empresa externa todo el soporte tecnológico para la implantación de la Autoridad Certificante y funciones de Autoridad de Registro, correspondiéndole contractualmente a dicha empresa garantizar la seguridad, disponibilidad permanente, interoperabilidad y escalabilidad de la infraestructura, así como también la construcción y gestión de planes de contingencia y recuperación ante desastres, en el marco de políticas de seguridad y procedimientos estandarizados mundialmente.

Bajo este esquema se provee a los administradores de la CA y RA provincial de una interfaz de administración remota, vía https (canal seguro) y asegurada mediante validación de cliente / servidor, que permite la configuración personalizada de los servicios de la PKI: Páginas de enrollamiento, gestión del CVC, gestión de las CRLs, configuración de políticas, administración de directorios, etc.

Las principal ***ventaja*** de este esquema de trabajo, es que en principio no se requieren inversiones especiales en equipamiento o conectividad fuera de las capacidades que hoy posee la provincia, puesto que solo se requiere hostting de las páginas de enrolamiento y administración del Ciclo de Vida de Certificados (CVC) junto a un Servidor Web para servirlas a los usuarios de la Intranet / Internet de Gobierno, y alternativamente un o dos dispositivos firewall. Todos elementos que hoy existen y se encuentran disponibles en la Administración Pública Provincial bajo los requerimiento técnicos de este tipo de implantación. Además se simplifican completamente las necesidades de Recursos Humanos capacitados y condiciones operativas para la administración de los servidores de la CA, Bases de Datos, directorios LDAP, mantenimiento de la seguridad, etc.

Sin embargo, esta propuesta presenta a nuestro criterio importantes ***desventajas*** de orden económico y técnico que no se pueden soslayar. En primer lugar, los costos de mantenimiento de los servicios externos son elevados y generan dependencia permanente de la empresa externa *(Ver Tabla 2 – Estimación de costos de outsourcing de la PKI)*. Por otra parte, consideramos poco confiable delegar todo el mantenimiento de la seguridad y los servicio de la PKI en una administración externa.

Cantidad de Certificados Gestionados	Costo estimado de mantenimiento anual para Certificados tipo X509 y S/Mime (En U$S)
	Costo Unitario U$S 12
200	2,400.00
500	6,000.00
1000	12,000.00
2000	24,000.00
10000	120,000.00
50000	600,000.00

Tabla 2 – Estimación de costos de outsourcing de la PKI

5.4.2. Alternativa 2: Implementación de una plataforma tecnológica propia

En este escenario definimos una ***vista lógica*** de los dispositivos y equipos que consideramos mínimamente necesarios para instrumentar la PKI propuesta de manera completa en las dependencias de la Gobernación de la Provincia de Mendoza. Proponemos también tres configuraciones alternativas de plataforma tecnológica para este modelo, con un análisis detallado de los costos, las debilidades y las fortalezas de cada una.

La siguiente figura ilustra el layout propuesto para la PKI provincial. En su lectura y análisis debe tenerse presente que el mismo propone un modelo de implementación concreta para el diseño propuesto en la *Figura 4 – Esquema de diseño preliminar propuesto para la PKI provincial* y que el ***criterio fundamental*** en su construcción ha sido lograr una estructura técnicamente confiable que garantice la seguridad, disponibilidad, eficiencia y escalabilidad de la solución con la mínima inversión posible.

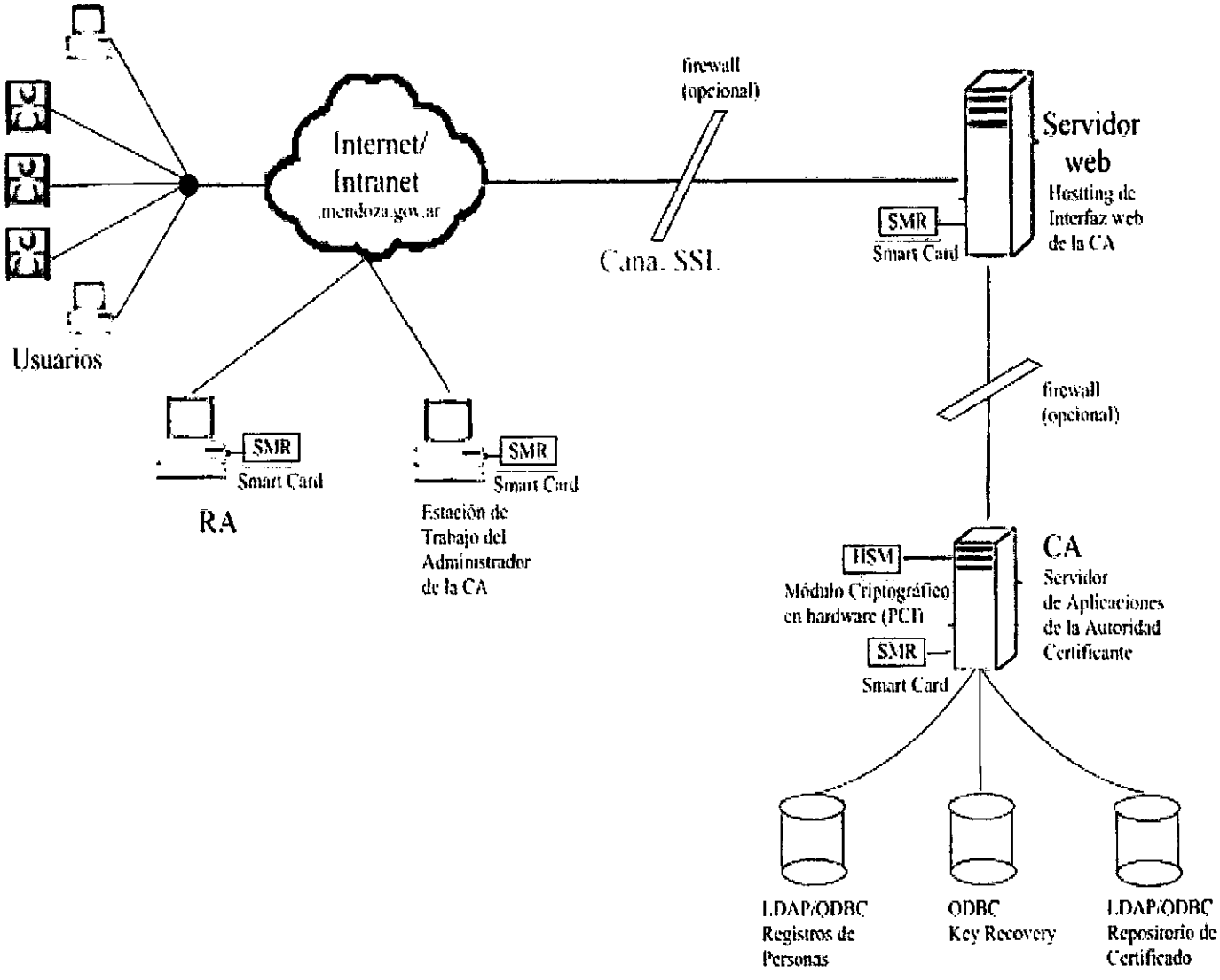


Figura 4 – Esquema de diseño preliminar propuesto para la PKI provincial

Exponemos a continuación tres alternativas de adquisición de plataforma tecnológica de soporte a este diseño PKI, las cuales varían en complejidad, calidad y costos.

Ver Configuraciones alternativas

Hoja de cálculo de
Microsoft Excel

	CONFIGURACIÓN 1		CONFIGURACIÓN 2		CONFIGURACIÓN 3	
	Componente	**U$S**	**Componente**	**U$S**	**Componente**	**U$S**
Máquinas de Usuarios Finales						
(No se especifican costos para equipos de usuarios finales porque se considera que esta infraestructura ya se encuentra constituida en la Administración Pública Provincial). Se requiere conectividad a Internet y a la Intranet de Gobierno desde los puestos de trabajo de usuarios de Certificados emitidos por la PKI provincial.	**Sistemas Operativos Soportados**		**Sistemas Operativos Soportados**		**Sistemas Operativos Soportados**	
	Windows 2000, ME, 9x, XP, NT		Windows 2000, ME, 9x, XP, NT		Windows 2000, ME, 9x, XP, NT	
	Linux		Linux		Linux	
	HP-UX		HP-UX		HP-UX	
	Solaris		Solaris		Solaris	
	Browsers soportados		**Browsers soportados**		**Browsers soportados**	
	Netscape Communicator 4.7x o sup.		Netscape Communicator 4.7x o sup.		Netscape Communicator 4.7x o sup.	
	Internet Explorer 5.5. O sup.		Internet Explorer 5.5. O sup.		Internet Explorer 5.5. O sup.	
	Clientes de email testeados		**Clientes de email testeados**		**Clientes de email testeados**	
	Outlook Express 5.0 o sup.		Outlook Express 5.0 o sup.		Outlook Express 5.0 o sup.	
	Ms Outlook		Ms Outlook		Ms Outlook	
Estación de Trabajo del Administrador de la CA						
(Se prevee una administración remota de la CA desde esta estación de trabajo)	**Hardware**					
	Intel Pentium 1.4 Ghz. o superior		Intel Pentium 866 Mhz. o superior		Intel Pentium 866 Mhz. o superior	
	512 MB RAM		512 MB RAM		256 MB RAM	
	30 Gbytes en disco		20 Gbytes en disco		20 Gbytes en disco	
	CD-ROM Drive		CD-ROM Drive		CD-ROM Drive	
	Lectora de Smart Card		Lectora de Smart Card		Lectora de Smart Card	
	Tarjeta de Red 10/100		Tarjeta de Red 10/100		Tarjeta de Red 10/100	
	1 Bahía PCI libre		1 Bahía PCI libre		1 Bahía PCI libre	
	1 Puerto Serial Disponible	1,800.00	1 Puerto Serial Disponible	1,500.00	1 Puerto Serial Disponible	1,100.00
	Sistema Operativo		**Sistema Operativo**		**Sistema Operativo**	
	Windows 2000 o XP	140.00	Windows 2000 o XP	140.00	Windows 98	70.00
	Browsers soportados		**Browsers soportados**		**Browsers soportados**	
	Netscape Communicator 4.7x o sup.	0.00	Netscape Communicator 4.7x o sup.	0.00	Netscape Communicator 4.7x o sup.	0.00
	Internet Explorer 5.5. O sup.	0.00	Internet Explorer 5.5. O sup.	0.00	Internet Explorer 5.5. O sup.	0.00
	Clientes de email testeados		**Clientes de email testeados**		**Clientes de email testeados**	
	Outlook Express 5.0 o sup.	0.00	Outlook Express 5.0 o sup.	0.00	Outlook Express 5.0 o sup.	0.00
	Ms Outlook	0.00	Ms Outlook	0.00	Ms Outlook	0.00
Cantidad	1 U **Costo Total U$S**	**1,940.00**	1 U **Costo Total U$S**	**1,640.00**	1 U **Costo Total U$S**	**1,170.00**
Estación de Trabajo del Administrador de la RA						
(Se prevee el cumplimiento de las funciones de RA de manera remota a través de una interfaz web con canal seguro).	**Hardware**					
	Intel Pentium 1.4 Ghz. o superior		Intel Pentium 866 Mhz. o superior		Intel Pentium 866 Mhz. o superior	
	512 MB RAM		256 MB RAM		256 MB RAM	
	30 Gbytes en disco		20 Gbytes en disco		20 Gbytes en disco	
	CD-ROM Drive		CD-ROM Drive		CD-ROM Drive	
	Lectora de Smart Card		Lectora de Smart Card		Lectora de Smart Card	
	Tarjeta de Red 10/100		Tarjeta de Red 10/100		Tarjeta de Red 10/100	
	1 Bahía PCI libre		1 Bahía PCI libre		1 Bahía PCI libre	
	1 Puerto Serial Disponible	1,800.00	1 Puerto Serial Disponible	1,100.00	1 Puerto Serial Disponible	1,100.00
	Sistema Operativo		**Sistema Operativo**		**Sistema Operativo**	
	Windows 2000 o XP	140.00	Windows 2000 o XP	140.00	Windows 98	70.00
	Browsers soportados		**Browsers soportados**		**Browsers soportados**	
	Netscape Communicator 4.7x o sup.		Netscape Communicator 4.7x o sup.		Netscape Communicator 4.7x o sup.	
	Internet Explorer 5.5. O sup.		Internet Explorer 5.5. O sup.		Internet Explorer 5.5. O sup.	
	Clientes de email testeados		**Clientes de email testeados**		**Clientes de email testeados**	
	Outlook Express 5.0 o sup.		Outlook Express 5.0 o sup.		Outlook Express 5.0 o sup.	
	Ms Outlook		Ms Outlook		Ms Outlook	

	CONFIGURACIÓN 1		CONFIGURACIÓN 2		CONFIGURACIÓN 3	
	Componente	U$S	Componente	U$S	Componente	U$S
Servidor Web (Hostting de interfaz web de la CA)						
	Hardware		**Hardware**		**Hardware**	
	Simple Intel Pentium 2.66 Ghz./ 133 MHz FSB 512 Kb L2 ECC Cache. 512 MB SDRAM 4 ranuras de expansión PCI mín. HDD SCSI Hot-plug de 72 GB 10000 rpm 2 Adptadores de Red 10/100/1000 Mbps 2 puertos USB 1 puerto serial Lectora de CD-ROM Grabadora de CD-ROM Lectora de Smart Card	3,300.00	Simple Intel Pentium 2.66 Ghz./ 133 MHz FSB 512 Kb L2 ECC Cache. 512 MB SDRAM 2 ranuras de expansión PCI mín. HDD SCSI Hot-plug de 36 GB 10000 rpm 2 Adptadores de Red 10/100/1000 Mbps 2 puertos USB 1 puerto serial Lectora de CD-ROM Grabadora de CD-ROM Lectora de Smart Card	2,800.00	Simple Intel Pentium 2.66 Ghz./ 133 MHz FSB 512 Kb L2 ECC Cache. 512 MB SDRAM 2 ranuras de expansión PCI mín. HDD SCSI Hot-plug de 36 GB 10000 rpm 2 Adptadores de Red 10/100/1000 Mbps 2 puertos USB 1 puerto serial Lectora de CD-ROM Grabadora de CD-ROM Lectora de Smart Card	2,800.00
	Sistema Operativo		**Sistema Operativo**		**Sistema Operativo**	
	HP-UX 11i	980.00	Windows 2000 Server	550.00	Linux Red Hat 9.0	0.00
	Web Server		**Web Server**		**Web Server**	
	Sun One Web Server Enterprise Edition	1,560.00	IIS 5.0 (incluido en W2000 server)	0.00	Apache 3.0 + JBOSS aplication server	0.00
Cantidad	**Costo Total U$S**	**6,840.00**	**Costo Total U$S**	**3,350.00**	**Costo Total U$S**	**2,800.00**
1 U			1 U		1 U	
Servidor CA - Gestión PKI						
En este servidor se desarrollará la gestión y almacenamiento de certificados, firma y emisión de certificados, operaciónes de validación, servicio de directorios, servicios de emisión masiva, gestión de la caducidad de certificados y administración de CRLs, etc. Se solicitan 2 unidades de esta plataforma para considerar el Hardware/software redundante necesario para Mirror y Plan de Contingencias.	**Hardware**		**Hardware**		**Hardware**	
	Arq. Intel con procesador simple 2.66 Ghz. (escalable a 4 procesadores)/ 133 MHz FSB 512 Kb L2 ECC Cache. 1 GB memoria base (2x512) 2 ranuras de expansión PCI mínimo 3 Bahías Ultra SCSI Hot Plug Controlador Smart Array 5 2 Adptadores de Red 10/100/1000 Mbps HDD 146.8 GB Ultra SCSI 10.000 rpm Capacidad de almacenamiento (max. En GB) 287 GB 1 puerto serial 2 puertos USB Lectora de CD-ROM Grabadora de CD-ROM Lectora de Smart Card compatibles con el estándar de seguridad de interoperabilidad [PKCS#11] Compatible con el estándar de Interoperabilidad [ISO7816] Compatible con el estándar de conectividad [PC/SC] Compatible con el estándar CryptoAPI para entornos Microsoft. UPS interna - 550W	7,500.00	Arq. Intel con procesador simple 3.06 Ghz. (escalable a 2 procesadores)/ 133 MHz FSB 512 Kb L2 ECC Cache. 1 GB memoria base (2x512) 2 ranuras de expansión PCI mínimo 2 Bahías Ultra SCSI Hot Plug Controlador Smart Array 5 2 Adptadores de Red 10/100/1000 Mbps HDD 72.8 GB Ultra SCSI 10.000 rpm Capacidad de almacenamiento (max. En GB) 287 GB puerto serial 2 puertos USB Lectora de CD-ROM Grabadora de CD-ROM Lectora de Smart Card compatibles con el estándar de seguridad de interoperabilidad [PKCS#11] Compatible con el estándar de interoperabilidad [ISO7816] Compatible con el estándar de conectividad [PC/SC] Compatible con el estándar CryptoAPI para entornos Microsoft. UPS interna - 325W	4,500.00	Arq. Intel con procesador simple 3.06 Ghz. (escalable a 2 procesadores)/ 133 MHz FSB 512 Kb L2 ECC Cache. 512 KB memoria base 2 ranuras de expansión PCI mínimo 2 Bahías Ultra SCSI Hot Plug 2 Adptadores de Red 10/100/1000 Mbps HDD 72.8 GB Ultra SCSI 10.000 rpm Capacidad de almacenamiento (max. En GB) 160 GB puerto serial 2 puertos USB Lectora de CD-ROM Grabadora de CD-ROM Lectora de Smart Card Lectora de Smart Card compatibles con el estándar de seguridad de interoperabilidad [PKCS#11] Compatible con el estándar de interoperabilidad [ISO7816] Compatible con el estándar de conectividad [PC/SC] Compatible con el estándar CryptoAPI para entornos Microsoft.	4,000.00

	CONFIGURACIÓN 1		CONFIGURACIÓN 2		CONFIGURACIÓN 3	
	Componente	U$S	Componente	U$S	Componente	U$S
	Módulo Criptográfico en Hardware - HSM		**Módulo Criptográfico en Hardware - HSM**			
	Conforme con las normas FIPS 140-1 de nivel 3 y en lo posible al estándar Internacional ISO 15782		Conforme con las normas FIPS 140-1 de nivel 3 y en lo posible al estándar Internacional ISO 15782			
	Capacidad de hasta 400 firmas/seg.		Capacidad de hasta 400 firmas/seg.			
	Conexión SCSI	7,000.00	Conexión SCSI	7,000.00		
	Sistema Operativo		**Sistema Operativo**		**Sistema Operativo**	
	HP-UX 11i	980.00	Windows 2000 Server	550.00	Linux Red Hat 9.0	0.00
	LDAP		**LDAP**		**LDAP**	
	Iplanet Directory Server 5.1 (incluido en HP-UX)		Microsoft Active Directory for windows (incluido en W2000 server)	0.00	Open LDAP	0.00
	Base de Datos		**Base de Datos**		**Base de Datos**	
	Oracle 9i	1,830.00	Ms Sql Server 7	1,700.00	Posigree o Mysql	0.00
	Software PKI		**Software PKI**		**Software PKI**	
	Verisign Managged PKI	10,000.00	Microsoft PKI (incluida en W2000 server)		EJBCA - Enterprice Java Bean Certification Autority	0.00
Cantidad	2 U **Costo Total U$S**	**64,620.00**	2 U **Costo Total U$S**	**27,500.00**	2 U **Costo Total U$S**	**8,000.00**
Otros elementos a tener en cuenta						
Se contemplan aquí otros dispositivos para instalaciones físicas, backup e insumos	1 Rack - Pallet para servidores	1,400.00	2 Unidad de Energía Ininterrumpida	3,000.00	1 Unidad de Energía Ininterrumpida	1,500.00
	2 Unidad de Energía Ininterrumpida	3,000.00	2 Sistema de Aire Acondicionado	2,400.00	5 Smart Cards	
	1 Unidad lecto grabadora DVD	200.00	10 Smart Cards	200.00	50 CDs R/W	100.00
	2 Sistema de Aire Acondicionado	2,400.00	50 CDs R/W	40.00		40.00
	10 Smart Cards	200.00	20 DVDs R/W	180.00		
	50 CDs R/W	40.00				
	20 DVDs R/W	180.00				
Cantidad	2 U **Costo Total U$S**	**7,420.00**	2 U **Costo Total U$S**	**5,820.00**	2 U **Costo Total U$S**	**1,640.00**
	COSTO TOTAL CONFIGURACIÓN 1 - U$S	**71,760.00**	**COSTO TOTAL CONFIGURACIÓN 2 - U$S**	**39,550.00**	**COSTO TOTAL CONFIGURACIÓN 2 - U$S**	**14,780.00**

La ***Configuración Alternativa 1*** propone un escenario de máxima seguridad y rendimiento para la CA y RA propuestas.

Veamos algunos de los ***fundamentos técnicos*** de esta configuración:

- HP-UX es uno de los sistemas propietarios más robustos del mercado y se integra perfectamente bien en aplicaciones de propósito crítico, por esto se lo eligió como base para la plataforma.
- Sun One es un web server sumamente flexible, robusto y con una gran cantidad de prestaciones integrando además toda la capacidad de la plataforma J2EE, líder en desarrollo de aplicaciones para Internet. Además es un servidor web que se acopla perfectamente bien a sistemas UNIX y con mucho menor costo que otras soluciones empresariales como las provistas por IBM, Macromedia, etc.
- Si bien la capacidad de almacenamiento masivo, tecnología de base de datos y performance del hardware excede los requerimientos tecnológicos de la PKI propuesta en primera instancia, estas características garantizan también una escalabilidad directa hacia una PKI de gran envergadura, sin necesidad de conversiones ni migraciones previas.
- La seguridad y aceleración de los tiempos de firma y validación que proveen los módulos criptográficos en Hardware (HSM) es una característica fundamental de esta propuesta. A medida que la criptografía de clave pública ha ido consolidándose como la base de la seguridad informática, el punto débil de la seguridad para las organizaciones se ha desplazado desde los datos en sí hacia las claves que los protegen. Los datos sólo son seguros en la medida en que lo sean dichas claves. Para solucionar el problema, se han desarrollado una serie de productos que tienen por objeto almacenar las claves, con la debida seguridad, en el interior de módulos de hardware protegidos y fiables, en los cuales se de protección

multifactorial, es decir una combinación de enfoques físicos y lógicos que permita generar un nivel más elevado de seguridad. Mediante la utilización de un potente sistema de cifrado multifactorial y la adición de medidas tales como la puesta en común de información secreta entre múltiples testigos protegidos por medio de contraseñas, se consigue un nivel de protección de las claves cifradas excepcionalmente elevado.

- El uso de smart cards para el control de acceso de los administradores de la CA y RA frente a la alternativa de sistemas de login/password es una medida de seguridad física y lógica ampliamente implementada en las soluciones PKI, cuyo costo no es excesivo en relación a los beneficios que el uso de estos esquemas provee.
- Se han contemplado también en esta propuesta los mecanismos de resguardo y backup, equipamiento redundante y degradado, procesamiento tolerante a fallas y medios de abastecimiento de energía ininterrumpibles y redundantes que una solución PKI en producción requiere.

En conclusión, esta configuración involucra servidores de amplio rendimiento, software de gestión pki mundialmente aceptado y testeado; y amplios dispositivos de seguridad que permiten garantizar confiabilidad y performance en el sistema; así como también allana en gran medida el camino que se deberá recorrer al momento de escalar significativamente la infraestructura.

La ***Configuración Alternativa 2*** propone una plataforma 100% integrada por soluciones de software Microsoft, desde los sistemas operativos hasta el software de gestión PKI, pasando por los servidores de directorio, motor de base de datos y web servers. En cuanto al hardware y dispositivos electrónicos

incluidos se ha degradado parcialmente las opciones incluidas en la configuración 1 para mostrar otra alternativa de menor costo global.

En principio esta segunda propuesta se fundamenta en la idea de mostrar una solución factible de costo medio para la PKI propuesta que sea fácil de implementar y gestionar. La integración de productos de una misma línea simplifica significativamente los procesos de instalación, configuración, pruebas y puesta a punto de toda la plataforma lo que puede ser un atractivo interesante si se cuentan con tiempos de implementación acotados o si no se dispone de un equipo de personas capacitadas en la administración de entornos propietarios Unix o Linux.

No obstante lo expuesto, creemos que desde el punto de vista de la seguridad y el rendimiento, los entornos Microsoft son mucho más vulnerables que las plataformas Unix y esto se pone aún más de manifiesto en aplicaciones con un alto grado de interoperabilidad con Internet.

Si evaluamos el cumplimiento de los requerimientos funcionales planteados para la PKI y su ajuste a estándares abiertos, la solución de Microsoft también tiene puntos débiles que adquieren principal importancia cuando se considera la escalabilidad futura del sistema.

La ***Configuración Alternativa 3*** es mucho menos ambiciosa en todos los sentidos que las dos propuestas precedentes; y se ajusta puntualmente a los requerimientos específicos de la PKI propuesta. La misma se basa fundamentalmente en software de libre distribución, aprovechando la potencialidad de los sistemas Linux y su integración natural con la plataforma J2EE.

Su gran ventaja, es que tanto el software de base como el software de gestión PKI (EJBCA) satisfacen los requisitos planteados sin demandar grandes inversiones económicas y de recursos humanos.

Se debe tener claro, no obstante, que con el espíritu de proponer una solución de menor costo económico, se redujeron en esta propuesta las especificaciones de los servidores y dispositivos de almacenamiento, el motor de base de datos y el módulo criptográfico en hardware (HSM). Este ahorro implica

en primera instancia degradar la performance y seguridad de la solución, así como también la necesidad de una mayor inversión de recursos económicos y humanos al momento de plantear un crecimiento de los servicios de la PKI.

En términos estrictamente técnicos creemos que es la solución ideal para una primera experiencia de implantación PKI, en los términos que se han definido.

6. Necesidades de Recursos Humanos

El abordaje de cualquiera de las soluciones técnicas que se han planteado para implementar la PKI provincial requiere la conformación de un equipo de personas técnicamente capacitado para administrarla de manera consistente y eficiente. Este equipo debería contar mínimamente con los siguientes perfiles.

- ***Administrador de servidores:*** administrador de los servidores implantados, encargado de gestionar la configuración del software de base y las aplicaciones que en el mismo se corren, el acceso de usuarios, las copias de seguridad de datos, el mantenimiento de los dispositivos periféricos y la seguridad lógica integral de todo el sistema.

- ***Administrador de Bases de Datos (DBA):*** encargado de administrar todas las aplicaciones vinculadas al almacenamiento de los datos que se mantienen en la PKI y su resguardo. En principio, estos repositorios serían el Registro de Personas, la base de datos para Recuperación de Claves en el esquema de par doble de claves (Key Recovery) y el Repositorio de Certificados.

- ***Administrador de la Autoridad de Registro (RA):*** Perfil con firma autorizada para desarrollar las funciones y procedimientos de Autoridad de Registro, tales como la aprobación de solicitudes de emisión, renovación y

revocación de certificados, comprobación de bases de datos de personal, comprobaciones de datos de personas y equipos y todo lo concerniente a la autenticación de identidad y roles necesaria para otorgar y gestionar Certificados digitales.

- ***Administradores de la Autoridad Certificante (CA):*** Este perfil es crítico puesto que en él recaen las funciones principales de administración y mantenimiento de la Autoridad Certificante, sus aplicaciones asociadas y la garantía de cumplimiento de las políticas y procedimientos de seguridad establecidas para la misma. La o las personas que desarrollen este rol, individual o conjuntamente, deberán ser las únicas que tengan acceso físico y lógico a la clave privada de la CA, pilar fundamental de toda la seguridad de la infraestructura. Con ella podrán cumplimentar todas las funciones y operaciones definidas para la CA.

- ***Mesa de ayuda y soporte técnico:*** Es fundamental implementar un servicio permanente de soporte a usuarios, de modo tal de solucionar lo más rápidamente posible las dudas o inconvenientes que pudieran presentarse, tanto en la operación de las aplicaciones informáticas que usen los Certificados Digitales, como en el cumplimiento de procedimientos y ajuste a las políticas definidas por la CA.

- ***Web master:*** Teniendo en cuenta que se ha definido un formato de interfaz web para la interacción de los usuarios finales con la CA, se necesita un perfil capacitado para diseñar, construir y mantener las páginas web que constituirán dicha interfaz. Desde estas páginas una persona podrá en principio solicitar un Certificado Digital (Clase 1), solicitar la renovación o revocación de su Certificados, buscar y descargar Certificados de Terceras Personas, descargar un certificado de sitio o el certificado de la CA, consultar el servicio de directorios, descargar las Listas de Revocación de Certificados (CRLs), acceder al soporte técnicos, etc.

Una persona puede concentrar más de uno de estos roles, pero se recomienda que de acuerdo a un criterio de ***separación de funciones*** los siguientes perfiles sean desempeñados por personas diferentes:

- El administrador de servidores, DBA, Administrador de RA y Administrador de CA deben ser personas distintas, con independencia funcional y jerárquica que desarrollen controles cruzados los unos sobre las actividades de los otros.
- Es recomendable que la Administración de la CA esté distribuida entre dos o más personas con independencia funcional y jerárquica. Se recomienda también que la clave privada se integre conjuntamente con k de n tarjetas de acceso privadas de cada una de estas personas. Este criterio de seguridad es fundamental aún en la implementación de pequeña escala propuesta.
- Las funciones de Autoridad de Registro pueden distribuirse entre distintas personas con firma autorizada, con el objetivo de distribuir la carga de trabajo. Esta distribución podría plantearse por distintos criterios, tales como: los usos de los certificados que gestionan, los sectores de la estructura de gobierno a los cuales están vinculados, etc.

6. Conclusiones y Sugerencias

Las siguientes conclusiones y sugerencias finales resultan de las investigaciones y pruebas preliminares realizadas; las cuales sustentan la información volcada en el presente documento.

Existen en el mercado múltiples configuraciones alternativas de equipamiento informático, aplicaciones de software, dispositivos de comunicaciones y de seguridad, que permiten implementar tecnológicamente una arquitectura PKI.

Las alternativas propuestas en la ingeniería de proyecto contemplan las ***especificaciones funcionales y técnicas*** deseables para una infraestructura técnicamente confiable, segura y escalable que brinde los servicios de certificación y firma digital a la comunidad del Gobierno de Mendoza. También consideran la adecuación de las soluciones a ***estándares abiertos.*** Existen hoy en día múltiples estándares asociados a las PKI. Debido a esto es muy importante contemplar que la solución que se adopte, se ajuste a determinados estándares y protocolos principalmente difundidos en la industria criptográfica de modo tal de garantizar condiciones de interoperabilidad, escalabilidad y seguridad. El ajuste a estándares es además un criterio fundamental para prevenir la rápida obsolescencia de la tecnología.

Desde el punto de vista técnico no recomendamos la alternativa de tercerización de la infraestructura tecnológica en una empresa de servicios PKI externa. Esta apreciación se sustenta en la dependencia que se genera de mecanismos y servicios tecnológicos, procedimientos y políticas, fijadas por terceras partes. Se debe tener en cuenta también, que en este caso se delega el manejo de los mecanismos que garantizan la seguridad y confidencialidad del sistema, pero no se delega la responsabilidad por las fallas de seguridad o disponibilidad que pudieran ocurrir.

Evaluando la relación costo / beneficio tampoco consideramos que la tercerización sea la alternativa más adecuada, ya que si bien soluciona la necesidad de una inversión inicial en tecnología, desaprovecha la economía de escala que se genera a medida que aumenta la cantidad de certificados gestionados por la PKI *(Ver Tabla 2 – Estimación de costos de outsourcing de la PKI)*. Si consideramos la proyección de crecimiento que podría tener la infraestructura en la provincia, es económicamente inviable sostener en el tiempo esta alternativa.

Entre las alternativas de configuración propuestas para la implantación de la PKI en las dependencias de la Gobernación de la Provincia de Mendoza, se sugiere en ***primera instancia*** adoptar la ***tercera alternativa*** *(Ver Configuración Alternativa 3)*. Esta recomendación se sustenta en que no requiere en principio inversión económica en software PKI, puesto que la solución propuesta es de código abierto y libre distribución. No obstante esto, satisface en gran medida las especificaciones funcionales y técnicas descriptas; y se ajusta a los estándares básicos propuestos en la legislación nacional, lo que garantiza posibilidades de escalarla progresivamente en el tiempo.

Luego de realizar una experiencia de gestión PKI primaria, se tendrá mayor información y conocimiento para proponer el diseño detallado de una infraestructura de mayor envergadura. Debe tenerse en cuenta en este sentido que el crecimiento no implica pérdida de la inversión en equipamiento realizada, ni conversiones inviables de los datos mantenidos en la jerarquía inicial, puesto que el ajuste a estándares descrito garantiza esta condición.

Al momento de implementar la solución concreta deberá tenerse presente que la ***Gestionabilidad*** de la PKI debe tener el mismo nivel de importancia que la ***seguridad, disponibilidad, interoperabilidad*** y ***escalabilidad***. En este sentido deberán realizarse dedicados esfuerzos para lograr el equilibrio justo entre estos objetivos en ocasiones contrapuestos.

Finalmente es fundamental tener en cuenta, que el ***punto crítico*** para una implementación exitosa de estas tecnologías, es desarrollar las ***capacidades humanas*** para adquirirla y manejarla, tanto en el nivel de los especialistas técnicos encargados de diseñar, montar y poner en marcha la infraestructura como de los usuarios intermedios y finales de la misma.

En este último nivel de la jerarquía, los usuarios finales, es donde se deberá poner mayor énfasis al momento de desarrollar una plan de pruebas y puesta en marcha, contemplando un cuidadoso proceso de difusión y capacitación, de modo de garantizar el uso correcto de los certificados emitidos por la CA provincial.

ESTÁNDARES

ITU-T X.509: Estándar de Interconexión de Sistemas Abiertos de la Unión Internacional de Telecomunicaciones. Las versiones X.509 v1,2 y 3 definen los formatos e información contenida en los certificados digitales.

FIPS 140-1 de nivel 1,2 y 3: Define estándares de seguridad e interoperabilidad para los dispositivos HSM.

[ISO 15782]: estándar por el que se rige el manejo seguro de las claves privadas de firma.

[ISO7816]: Información sobre smart cards asíncronas del International Standard Institute.

Triple DES [X9.52]: Norma de cifrado de datos. Algoritmo criptográfico simétrico, estándar en el sector, utilizado para el cifrado de las claves privadas.

LDAP: Norma para las aplicaciones de servicios de directorio.

[PKCS#7] Estándar industrial de respuestas a las solicitudes de certificados que contienen los certificados resultantes o bien las cadenas de certificados.

[PKCS#11] (Cryptographic Token Interface).

[PKCS-10P] Estándar industrial de mensajes de solicitud de certificados.

[PKCS#12] Estándar para exportar pares de claves en un formato cifrado mediante contraseña proporcionada por el usuario.

IETF (Internet Engineering Task Force www.ietf.org).

PKIX (Infraestructura de claves públicas, X.509).

CryptoAPI: interfaz estándar de Microsoft Corp. para la funcionalidad criptográfica proporcionada por los proveedores de servicios de cifrado instalables (CSP) integrados con Windows 2000 y que aprovechan la infraestructura de tarjeta inteligente de Microsoft PC/SC

IETF S/MIME v3: Estándar construido a partir de la propuesta S/MIME v2 de seguridad de datos mediante RSA que proporciona cifrado de claves públicas y firmas digitales mediante algoritmos RSA. Es utilizado por numerosos productos, Microsoft Outlook Express y Microsoft Outlook 98 de probada interoperabilidad entre fabricantes.

SET: Secure Electronic Transaction. Estándar para transacciones electrónicas seguras.

SSL: Protocolo de Capa de sockets seguros. Protocolo de seguridad que puede situarse sobre otros protocolos de la capa de transporte. Se basa en la tecnología de autenticación basada en claves públicas y utilizan la negociación de claves basada en claves públicas para generar una clave de cifrado única para cada sesión cliente servidor.

TSL (IETF) Protocolo de seguridad que puede situarse sobre otros protocolos de la capa de transporte. Se basa en la tecnología de autenticación basada en claves públicas y utilizan la negociación de claves basada en claves públicas para generar una clave de cifrado única para cada sesión cliente servidor.

SIGLAS

PKI: Public Key Infraestructure – Infraestructura de Clave Pública

AC / CA / ACL: Autoridad de Certificación Licenciada.

CL: Certificador Licenciado

CRL: Lista de Certificados Revocados.

CVC: Ciclo de vida de certificados

HSM: Módulo criptográfico en hardware

J2EE: Java 2 Enterprise Edition

DBA: Administrador de Base de Datos

ODBC: Open DataBase Client.