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

firma Digital

3º informe parcial

CONSEJO FEDERAL DE INVERSIONES
CONSULTOR: LIC. PABLO GUILLERMO LIOY
Fecha de impresión 04/02/2005 11:46

ÍNDICE

I. Introducción

Se presentan a continuación, como 3º informe parcial, las actividades y tareas desarrolladas en el marco de planificación del proyecto de Firma Digital Mendoza.

Actividad	Estado
Implementación de experiencia piloto en la Penitenciaría Provincial:	Concluida
• Identificación de la necesidad: se recopila y analiza información sobre el problema, se entrevista a los posibles usuarios y se precisa la necesidad de aplicación de tecnología de firma digital	Concluida
• Análisis del sistema: se releva el circuito actual, y se define el alcance de la experiencia piloto	Concluida
• Diseño de la implementación: se elabora el diseño conceptual de la experiencia piloto.	Concluida
• Desarrollo e implementación: se lleva a la práctica la experiencia piloto real. Se emiten los certificados de firma digital, se realizan las configuraciones, instalación de protocolos, ajustes y desarrollos necesarios en el equipamiento informático	Concluida

•Prueba del Sistema: se elabora y se pone en práctica un Plan de Pruebas	Concluida
•Puesta en Marcha de la implementación: el sistema existente se reemplaza por el nuevo mejorado y se capacita a los usuarios.	Concluida
•Evaluación de la experiencia: se definen métricas de evaluación que a futuro permitirán evaluar el éxito de la implementación	Concluida

3º informe parcial: la culminación de la actividad 3 se presentará a los cuatro meses de iniciadas las tareas.

II. Implementación de Experiencia de Sitio Seguro en la Penitenciaría Provincial:

A partir de nuestra estrategia de difusión del proyecto y a través de las herramientas de interacción con la demanda local incluidas en nuestra página Web, continuamos dando respuestas a las necesidades de implementación de tecnología de firma digital, esta vez, en el ámbito de los sistemas de intranet en la Penitenciaría Provincial.

Hablamos de un "Sitio Seguro" cuando nos referimos a un lugar virtual confiable en Internet, perteneciente a una empresa u organización que lo mantiene en línea por medio de un servidor de www (World Wide Web).

Cuando una persona se conecta a un sitio seguro, el servidor presenta un certificado emitido y firmado por la Entidad Emisora de Certificados.

Los programas habitualmente utilizados para navegar por Internet (Browser o Navegador) deben estar configurados para aceptar certificados, que garantizan la confiabilidad del sitio, los que son emitidos por la Entidad Emisora de Certificados. Además, existe la posibilidad de ir más allá y asegurar la identidad de los usuarios del sistema utilizando la misma tecnología de certificación digital, es decir, garantizando al servidor que la persona que accede es aquella a la cual este le ha dado privilegios de acceso y si así lo establecen previamente podría ingresar la base de datos y agregar o modificar información sensible con total seguridad de que la única persona que pudo hacerlo es la titular del certificado digital.

A. Identificación de la necesidad:

El desafío planteado, en este apartado es determinar claramente cuáles son las necesidades de seguridad que el sistema demanda y cuáles son los fundamentos de la aplicación de tecnologías de clave pública en la Intranet de la Penitenciaría de Mendoza.

Tales conclusiones deberán surgir de la consideración del tipo de información que se está consultando y/o transfiriendo al sitio y la valoración de las posibles acciones que se puedan realizar en pos de quebrar la seguridad que éste método sugiere en función de la evolución del poder computacional disponible.

Tipo de información que se maneja

La Intranet de la Penitenciaría Cuenta con un Sitio web por el cual se presenta y manipula informacion sobre:

- Antecedentes de los internos
- Situación Judicial de los internos
- Beneficios otorgados a los internos
- Actuaciones Disciplinarias
- Informes de Asistentes Sociales y Psicológicos
- Jornales de los internos
- Fondos de reserva (contaduría)

Tal información a su vez, se somete a eventos tales como:

- Alta , modificación y eliminación de contenidos on-line

- Consulta de contenidos desde todas las áreas del establecimiento , Poder Judicial , Ministerio de Seguridad y Justicia , Investigaciones , Policia, etc.
- Generación de números de pieza relacionadas con internos o personal.
- Consulta y carga en las bases de datos desde Internet.

Los indicadores más significativos son:

- Aproximadamente 300 antecedentes diarios son consultados mediante la web
- Se realizan 30 beneficios diarios
- Se confeccionan 100 boletas de audiencias a tribunales diarias

Partiendo de la base que la información es un recurso que, como el resto de los activos, tiene valor y por consiguiente debe ser debidamente protegida surge la necesidad de valorarla según su sensibilidad y criticidad.

Para clasificar estos Activos de Información, utilizaremos los criterios ya definidos en los siguientes niveles:

1 – SIN CLASIFICAR	Información de dominio público que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de la dependencia o no.

2-RESERVADA-USO INTERNO	Información que puede ser conocida y utilizada por todos los empleados y algunos colaboradores externos autorizados, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la dependencia.
3 - RESERVADA - CONFIDENCIAL	Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas, materiales o de imagen.
4 - RESERVADA - SECRETA	Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección, y cuya divulgación o uso no autorizados podría ocasionar graves pérdidas materiales o de imagen.

Consideramos a este tipo de información Reservada y Confidencial ya que representan información sensible sobre los internos y su falsa manipulación o maipulación negligente podría provocar daños como:

- Daños y perjuicios a los titulares con las consiguientes acciones legales contra la dependencia.
- Otorgamiento de beneficios, jornales o cualquier otro tipo de valoración a los internos basados en antecedentes fraguados, no reales o tapados.

Entorno Seguro

En la actualidad, la falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios en su labor de piratería.

La propia complejidad de la red utilizada por la Administración Pública Provincial, es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad.

Se expone a continuación una lista exhaustiva de potenciales problemas analizados y que se transcribe por considerarla como un importante antecedente tenido en cuenta en el desarrollo de Sitio Seguro para la Intranet de la Penitenciaría de Mendoza

	PROBLEMAS EN SISTEMAS CONECTADOS A INTERNET
	Fuentes: "Firewalls and Internet Security. Repelling the Wily Hacker"
1.-	De todos los problemas, el mayor son los fallos en el sistema de passwords.
2.-	Los sistemas basados en la autenticación de las direcciones se pueden atacar usando números consecutivos.
3.-	Es fácil interceptar paquetes UDP.
4.-	Los paquetes ICMP pueden interrumpir todas las comunicaciones entre dos nodos.
5.-	Los mensajes ICMP Redirect pueden corromper la tabla de rutas.
6.-	El encaminamiento estático de IP puede comprometer la autenticación

PROBLEMAS EN SISTEMAS CONECTADOS A INTERNET	
Fuentes: "Firewalls and Internet Security. Repelling the Wily Hacker"	
	basada en las direcciones.
7.-	Es fácil generar mensajes RIP falsos.
8.-	El árbol inverso del DNS (Server Name Domain) se puede usar para conocer nombres de máquinas.
9.-	Un atacante puede corromper voluntariamente la caché de su DNS para evitar responder peticiones inversas.
10.-	Las direcciones de vuelta de un correo electrónico no son fiables.
11.-	El programa sendmail es un peligro en sí mismo.
12.-	No se deben ejecutar a ciegas mensajes MIME.
13.-	Es fácil interceptar sesiones telnet.
14.-	Se pueden atacar protocolos de autenticación modificando el NTP.
15.-	Finger da habitualmente demasiada información sobre los usuarios.
16.-	No debe confiarse en el nombre de la máquina que aparece en un RPC.
17.-	Se puede conseguir que el encargado de asignar puertos IP ejecute RPC en beneficio de quien le llama.
18.-	Se puede conseguir, en muchísimos casos, que NIS entregue el fichero de passwords al exterior.
19.-	A veces es fácil conectar máquinas no autorizadas a un servidor NIS.
20.-	Es difícil revocar derechos de acceso en NFS.
21.-	Si está mal configurado, el TFTP puede revelar passwords.
22.-	No debe permitirse al ftp escribir en su directorio raíz.
23.-	No debe ponerse un fichero de passwords en el área de ftp.
24.-	A veces se abusa de FSP, y se acaba dando acceso a ficheros a quien

PROBLEMAS EN SISTEMAS CONECTADOS A INTERNET
Fuentes: "Firewalls and Internet Security. Repelling the Wily Hacker"

no se debe dar.

25.- El formato de información de WWW debe interpretarse cuidadosamente.

26.- Los servidores WWW deben tener cuidado con los punteros de ficheros.

27.- Se puede usar ftp para crear información de control del gopher.

28.- Un servidor WWW puede verse comprometido por un script interrogativo pobremente escrito.

29.- El MBone se puede usar para atravesar algunos tipos de cortafuego.

30.- Desde cualquier sitio de la Internet se puede intentar la conexión a una estación X11 (X-Server).

31.- No se debe confiar en los números de puerto facilitados remotamente.

32.- Es casi imposible hacer un filtro seguro que deje pasar la mayoría del UDP.

33.- Se puede construir un túnel encima de cualquier transporte.

34.- Un cortafuego no previene contra niveles superiores de aquellos en los que actúa.

35.- Las X11 son muy peligrosas incluso a través de una pasarela.

36.- Las herramientas de monitorización de red son muy peligrosas si alguien accede ilegítimamente a la máquina en que residen.

37.- Es peligroso hacer peticiones de finger a máquinas no fiables.

38.- Se debe de tener cuidado con ficheros en áreas públicas cuyos nombres contengan caracteres especiales.

39.- Los caza-passwords actúan silenciosamente.

40.- Hay muchas maneras de conseguir copiar el password

41.- Registrando completamente los intentos fallidos de conexión, se capturan

PROBLEMAS EN SISTEMAS CONECTADOS A INTERNET

Fuentes: "Firewalls and Internet Security. Repelling the Wily Hacker"

passwords.

42.- Un administrador puede ser considerado responsable -si se demuestra conocimiento o negligencia- de las actividades de quien se introduce en sus máquinas.

Entonces, la constitución de un SITIO SEGURO consiste en la seguridad en la comunicación a través de redes, especialmente Internet, consistente en prevenir, impedir, detectar y corregir violaciones a la seguridad durante la transmisión de información, más que en la seguridad en los ordenadores, que abarca la seguridad de sistemas operativos y bases de datos. Consideraremos la información esencialmente en forma digital y la protección se asegurará mayormente mediante medios lógicos, más que físicos.

Los mecanismos básicos pueden agruparse de varias formas para proporcionar los servicios previamente mencionados. Conviene resaltar que los mecanismos poseen tres componentes principales:

- Una información secreta, como claves y contraseñas, conocidas por las entidades autorizadas.
- Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado, hash (desmenuce de un mensaje compilado) y generación de números aleatorios.
- Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envía qué a quién y cuándo.

Asimismo es importante notar que los sistemas de seguridad requieren una gestión de seguridad. La gestión comprende dos campos bien amplios:

- Seguridad en la generación, localización y distribución de la información secreta, de modo que sólo pueda ser accedida por aquellas entidades autorizadas.
- La política de los servicios y mecanismos de seguridad para detectar infracciones de seguridad y emprender acciones correctivas.

Conclusiones/Identificación de la necesidad

Nuestro, entonces, es: ***Proteger, a través de un sitio seguro, la información contenida en la Intranet de la Penitenciaría de Mendoza y la tecnología utilizada para su transmisión, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información manipulada en el Sitio web.***

B. Análisis del sistema:

Cuando usamos un típico sistema de intranet, en el que mantenemos un sitio para brindar servicios y/o simplemente información dentro de una institución, como el usado actualmente por la Penitenciaría, tenemos (como usuarios), un débil nivel de identificación del sitio al cual accedemos, es decir, dadas las condiciones y variables del entorno puede resultar adecuado o no aumentar ese nivel de seguridad. Por ahora, lo que resulta un hecho es que el método utilizado actualmente no garantiza:

- ***Identificación unívoca***: el usuario no sabe que está ingresando a su sitio o a una réplica.
- ***Confidencialidad***: la información puede ser interceptada.
- ***Integridad:*** los datos pueden llegar incompletos y con posibilidad de error.
- ***No repudio:*** la información no es digitalmente firmada probando así que fue enviado por cierta persona evitando el rechazo de la misma.

Sometimos las consideraciones anteriores a nuestra "Estrategia para la Identificación de Procedimientos Aptos", ya que creemos 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.

Según nuestras Guías de aplicación

- Transacciones electrónicas y privacidad de la información: la administración pública provincial puede expandir la prestación de sus ser-

vicios y acercarse al ciudadano a través de transacciones electrónicas seguras. Las características puntuales de la información contenida en el sitio de la intranet de la penitenciaría de Mendoza, verdaderamente estimula la aplicación de tecnología de sitio seguro sobretodo en aquellos procedimientos que implican envío, modificación o baja de información sensible.

Según los "Criterios de selección de circuitos administrativos" de nuestra estrategia, las conclusiones fueron:

- *Circuitos administrativos de transferencia de información con exigencias de calidad en la información:* La privacidad, integridad y autenticación de la información estan en la intranet en variedad de formas tales como correo electrónico, normativa interna, documentos, trámites, declaraciones juradas, informes psicológicos, etc. Lograr que tales comunicaciones no se encuentren expuestas a falsificaciones o adulteraciones es una cuestión de alta prioridad.

- *Circuitos que requieren autenticación de las partes involucradas:* resulta una variante interesante para la futura extensión de la experiencia la autenticación unívoca de los usuarios de la intranet que se crea conveniente, asegurando que las únicas personas que pueda acceder a determinados contenidos sean aquellas que fueron designadas específicamente para esa tarea.

- *Circuitos que incluyen información estrictamente confidencial:* como ya vimos que es el caso de la información contenidad en el sitio web de la intranet de la Penitenciaría de Mendoza

Mejoras puntuales:

La implementación de sitio seguro en la intranet de la Penitenciaría persigue la efectiva consecución de las siguientes mejoras en la seguridad:

- **Protección de los sistemas de transferencia o transporte.** En este caso debemos garantizar, en el diseño del sistema la transferencia segura de la información de forma transparente al usuario final. Ejemplos de este tipo de planteamientos serían el establecimiento de un nivel de transporte seguro, de un servicio de transmisión de datos seguro.
- **Gestión de claves:** Éste es un tópico de capital importancia, al que se aplica el uso de la criptografía y debe estar resuelto antes de que el usuario esté en condiciones de enviar un solo bit seguro. En el caso de las claves secretas el problema mayor consiste en mantener su privacidad durante su distribución, en caso de que sea inevitable su envío de un punto a otro. En el caso de clave pública, los problemas tienen que ver con la garantía de que pertenecen a su titular y la confianza en su vigencia (que no haya caducado o sido revocada).
- ***Identificación unívoca del servidor***: desde el sitio de la intranet necesitamos asegurarle a los usuarios que está ingresando al sitio de la penitenciaría y no a una réplica.
- ***Confidencialidad***: resulta de vital importancia garantizar que la información que se le carga al sistema llegue a la base de datos de una manera segura, evitando bajo todo punto de vista la interceptabilidad de la información
- ***Integridad:*** evitar la posibilidad de que los datos pueden llegar incompletos y con posibilidad de error.

C. Diseño de la implementación:

De acuerdo con la identificación de la necesidad básica y el relevamiento general de la situación actual hemos elaborado el diseño conceptual de la experiencia.

Un sitio seguro conlleva la emisión de **un certificado** (también conocido como certificado de clave-publica o identificador digital) es un documento electrónico, emitido por una Autoridad Certificadora, que **identifica de forma segura al poseedor del mismo** evitando la suplantación de identidad por terceros, es este caso del propio sitio web.

¿Cómo funciona?

•Client Hello : El "saludo de cliente" tiene por objetivo informar al servidor qué algoritmos de criptografía puede utilizar y solicitar una verificación de la identidad del servidor. El cliente envía el conjunto de algoritmos de criptografía y compresión que soporta y un número aleatorio. El propósito del número aleatorio es para que en caso de que el servidor no posea un certificado para comprobar su identidad, aún se pueda establecer una comunicación segura utilizando un conjunto distinto de algoritmos. Dentro de los protocolos de criptografía hay un protocolo de intercambio de llave que define cómo cliente y servidor van a intercambiar la información, los algoritmos de llave secreta que definen que métodos pueden utilizar y un algoritmo de hash de una sola vía. Hasta ahora no se ha intercambiado información secreta, solo una lista de opciones.

•Server Hello: El servidor responde enviando su identificador digital el cual incluye su llave pública, el conjunto de algoritmos criptográficos y de compresión y otro número aleatorio. La decisión de qué algoritmos serán utilizados está basada en el más fuerte que tanto cliente como servidor soporten. En algunas situaciones

el servidor también puede solicitar al cliente que se identifique solicitando un identificador digital.

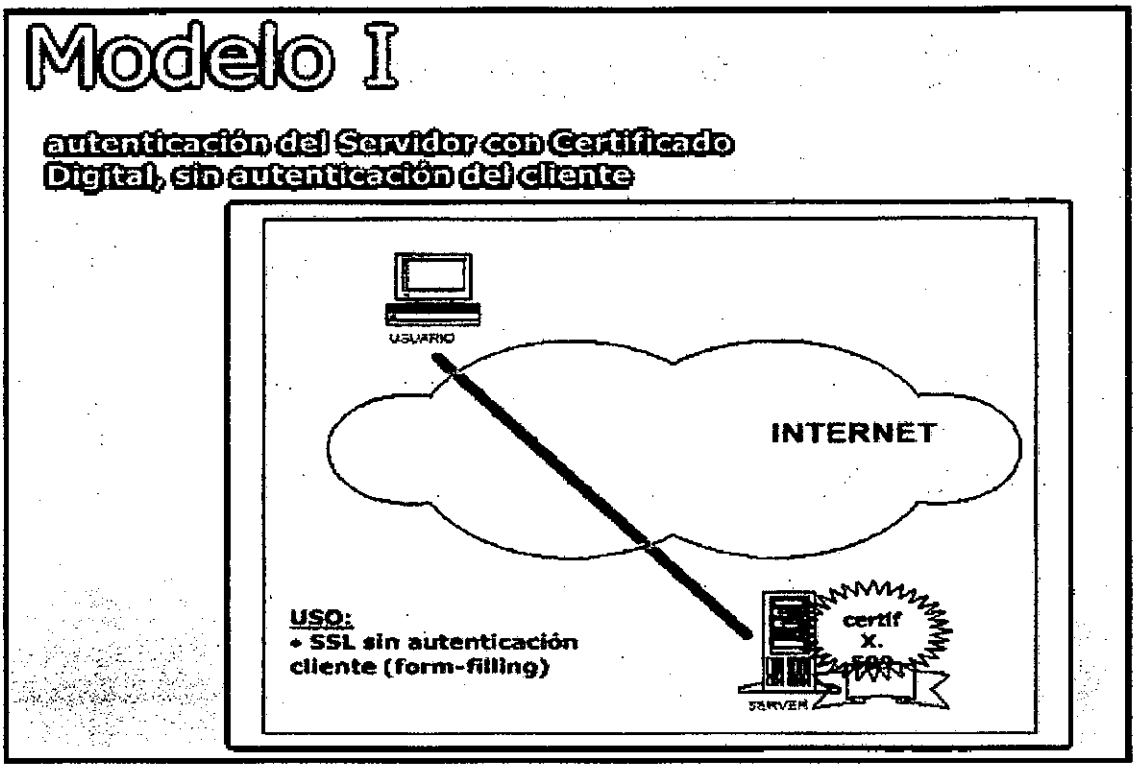
•Aprobación del Cliente: El cliente verifica la validez del identificador digital o certificado enviado por el servidor. Esto se lleva a cabo desencriptando el certificado utilizando la llave pública del emisor y determinando si este proviene de una entidad certificadora de confianza. Después se hace una serie de verificaciones sobre el certificado, tales como fecha, URL del servidor, etc. Una vez se ha verificado la autenticidad de la identidad del servidor. El cliente genera una llave aleatoria y la encripta utilizando la llave pública del servidor y el algoritmo criptográfico y de compresión seleccionado anteriormente. Esta llave se le envía al servidor y en caso de que el handshake tenga éxito será utilizada en el envío de futuros mensajes durante la sesión.

•Verificación: En este punto ambas partes conocen la llave secreta, el cliente por que la generó y el servidor por que le fue enviada utilizando su llave pública, siendo la única forma posible de desencriptarla utilizando la llave privada del servidor. Se hace una última verificación para comprobar si la información transmitida hasta el momento no ha sido alterada. Ambas partes se envían una copia de las anteriores transacciones encriptada con la llave secreta. Si ambas partes confirman la validez de las transacciones, el handshake se completa, de otra forma se reinicia el proceso.

Ahora ambas partes están listas para intercambiar información de manera segura utilizando la llave secreta acordada y los algoritmos criptográficos y de compresión.

Modelos

Concretamente existen dos modelos para mejorar la seguridad del sistema a través de la implementación de Sitio Seguro:



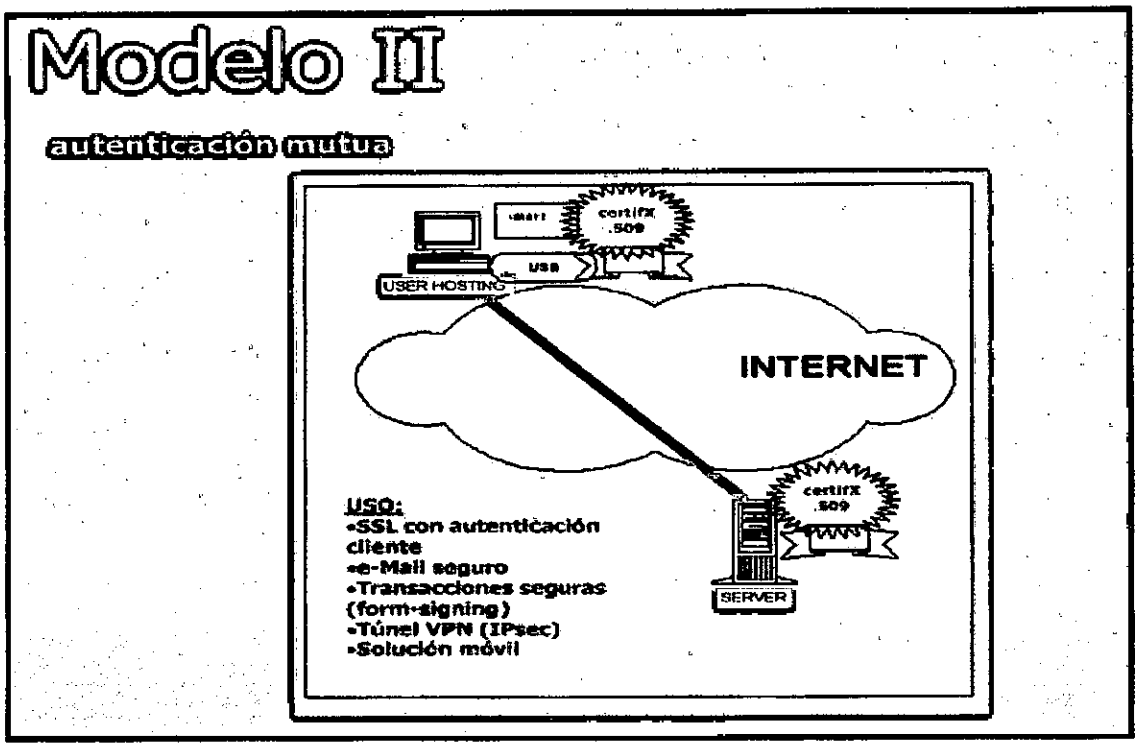
En el primer modelo la aplicación de ésta tecnología proporciona:

- **Autenticación unívoca del servidor seguro:** el cliente tiene la garantía de estar *hablando* con el servidor al que accede.
- **Privacidad en el intercambio de información:** sólo el cliente y el servidor seguro conocen lo que viaja por la red. Nadie distinto a ellos podrá leer la información que intercambien. Ahora que se ha establecido un canal de transmisión seguro SSL, es posible el intercambio de datos. Cuando el servidor o el cliente desea enviar un mensaje al otro, se genera un digest (utilizando un algoritmo de hash), encriptan el mensaje y el digest y se envía, cada mensaje es verificado utilizando el digest.

***"Este modelo es el elegido y será usado para la transmisión de datos confidenciales de los usuarios de la intranet de la Penitenciaría de Mendoza con el objeto de proveer una serie de garantías"**, a saber:*

- ***Identificación unívoca***: Constituye una mejora fundamental al momento de aportarle al usuario la total seguridad de estar ingresando por el sitio oficial de la Penitenciaría y no en una réplica del mismo.
- ***Confidencialidad***: la información que viaje desde el usuario a la Base de Datos no podrá ser interceptada. Constituye una mejora radical en la seguridad en el traspaso de datos mediante herramientas de encriptado de información. Contribuye al aseguramiento de la integridad y veracidad de la información.
- ***Integridad:*** los datos enviados por usuarios llegarán completos y sin posibilidad de error, ya que la tecnología garantiza la verificación de la integridad de los mensajes mediante la aplicación de una función de hash. Cualquier diferencia, pérdida de datos, o modificación de los datos originales enviados será alertada por el sistema.

De esta forma, todos los datos provenientes de los usuarios que realizan altas, modificaciones, bajas o simplemente consultas se resguardan, mediante métodos de encriptación que aseguran la integridad y confidencialidad de la información que viaja por la web.



Modelo II: En el segundo modelo la aplicación de ésta tecnología proporciona:

- **Autenticación mutua entre el servidor seguro y el cliente.** El servidor sabe con total seguridad quien es el cliente que esta al otro lado y el cliente tiene la garantía de estar *hablando* con el servidor al que accede.
- **Privacidad en el intercambio de información.** Sólo el cliente y el servidor seguro conocen lo que viaja por la red. Nadie distinto a ellos podrá leer la información que intercambien. Ahora que se ha establecido un canal de transmisión seguro SSL, es posible el intercambio de datos. Cuando el servidor o el cliente desea enviar un mensaje al otro, se genera un digest (utilizando un algoritmo de hash), encriptan el mensaje y el digest y se envía, cada mensaje es verificado utilizando el digest.

  "Este modelo representa una variante interesante para una futura extensión de la implementación de sitio seguro"

D. Desarrollo e implementación:

Instalación de la Plataforma de Desarrollo

La Intranet de la Penitenciaría provincial está montada sobre una Plataforma de Software Microsoft (Windows NT Server 4.0 + SP, IIS 4.0 con extensiones Active Server Page). Esto introduce cambios significativos en relación a los desarrollos de sitio seguro precedentemente implementados sobre plataformas Linux-Apache (Guía de Trámites) y Sun (Zona segura del sitio de resoluciones de la Secretaría Administrativa, Legal y Técnica) respectivamente. Por tal motivo se estimó conveniente instalar un servidor de desarrollo donde realizar la instalación y pruebas preliminares en lugar de operar directamente sobre el web-server en producción, a fin de preservar la integridad y disponibilidad de las aplicaciones que se sirven desde la Intranet Penitenciaria. Una vez que el proceso de instalación y configuración del sitio seguro estuvo debidamente probado y documentado se instrumentaron los cambios necesarios sobre el web-server en producción.

En esta línea de trabajo se instaló una plataforma de desarrollo con la siguiente configuración.

1. Windows XP-Professional SP2

2. Internet Information Server 5.0 con extensiones de servidor para Front Page y el complemento MMC (Microsoft Management Console)

Cabe aclarar que la penitenciaría cuenta con una plataforma basada en Sistema Operativo Microsoft NT Server 4.0 + SP e IIS 4.0. No obstante esto, se sugirió un upgrade a las nuevas versiones de software para mejorar las funciones generales de seguridad y administración del sitio. Por otra parte, se evaluó la documentación del software y se observó que la actualización de versiones no ha afectado los esquemas de trabajo con Sockets seguros (SSL) y el uso de certificados

de autenticación de sitios. Además el upgrade entre versiones de S.O y web-server es directo.

Configuración del sitio de prueba

Una vez instalado el software de base se procedió a instalar y configurar un sitio web con fines de prueba. En consistencia con el diseño estructural de la Intranet Penitenciaria se configuró un único sitio en el home-directory por defecto de IIS ubicado en el directorio c:\inetpub\wwwroot\ y accesible mediante los IP 192.168.0.1 o http://localhost o http://black4 según la configuración establecida para el protocolo TCP/IP en el servidor de prueba.

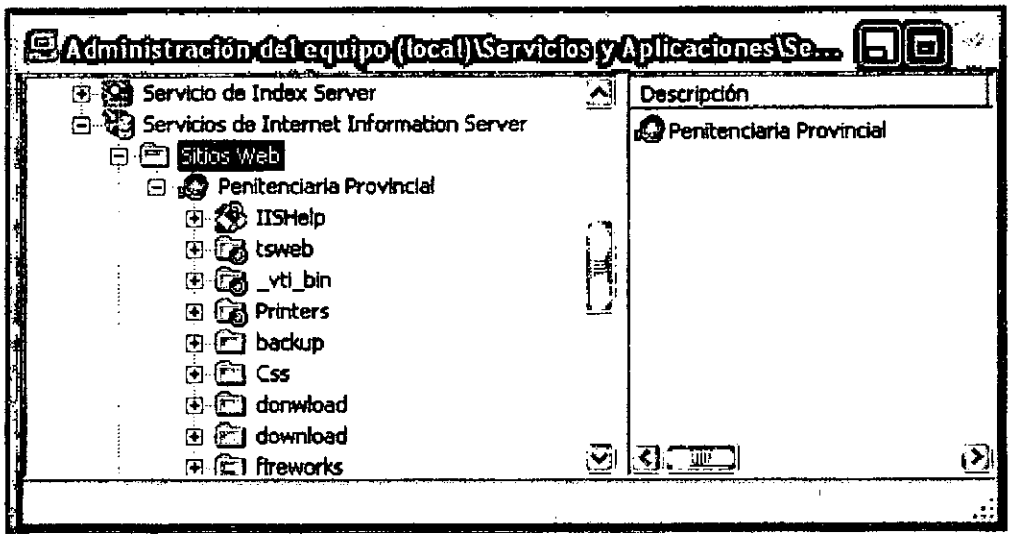
Nota: black4 es el nombre del equipo donde está instalado el servidor de desarrollo; por tanto en la plataforma de desarrollo constituye el dominio para el sitio de prueba.

En primera instancia no se configuraron directorios virtuales, puesto que la estructura de sitio de la penitenciaría provincial no hace uso de esta característica y que es recomendable para el uso de Certificados de Servidor configurar un único sitio.

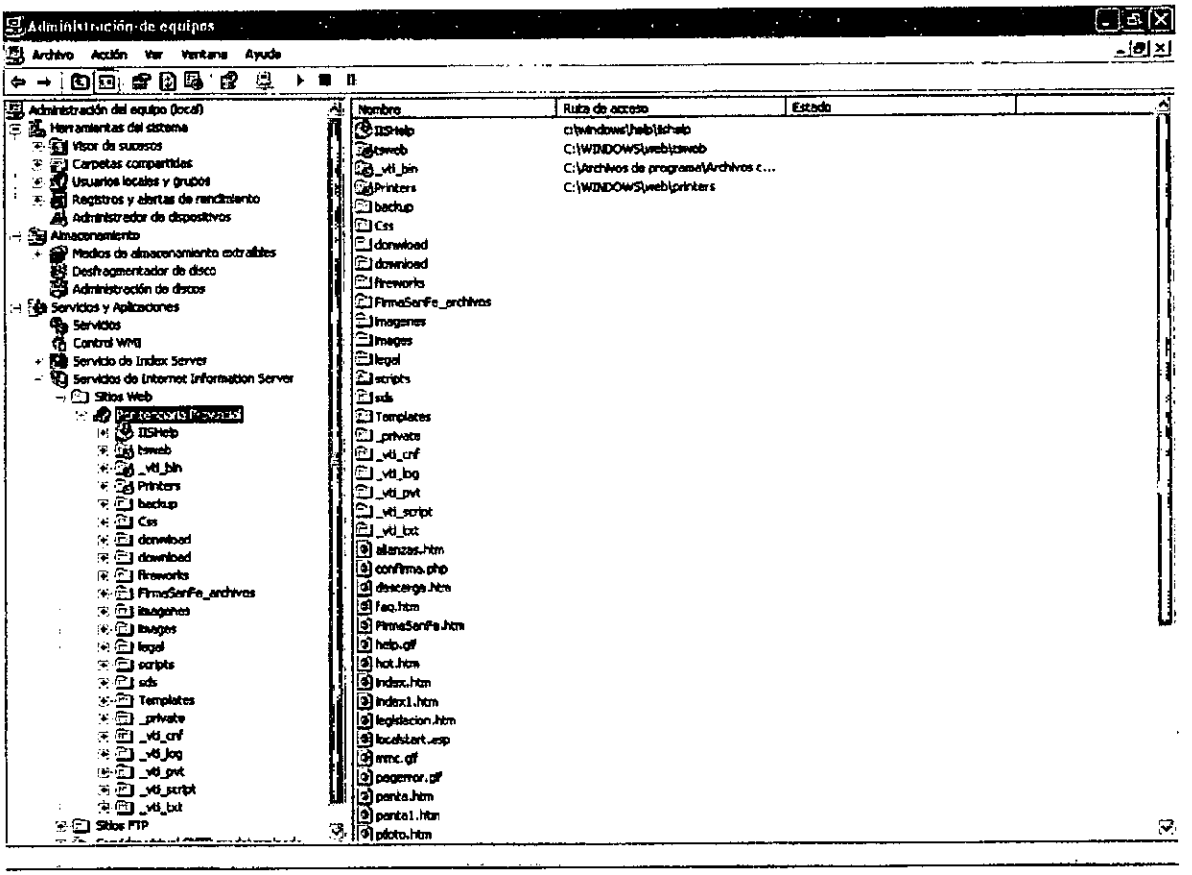
Para administrar el servidor se utilizó la intemase de administración de equipos de Windows XP, Microsoft Mangement Console (MMC). Esta herramienta provee un panel de control para la administración de los servicios de Internet Information Server incluyendo configuración de sitios, mapeo de directorios virtuales, definición de documentos por defecto, manejo de errores, administración de usuarios, instalación de servicios y componentes, administración de logs y desarrollo de los esquemas de seguridad incluyendo comunicaciones seguras SSL.

Una vez instalada la plataforma de desarrollo se efectuaron configuraciones alternativas y pruebas para estudiar el manejo de esta herramienta de control y

diseñar una configuración de sitio apropiada previo a la implementación de canal seguro SSL.



MMC – Microsoft Management Console



Sitio Web Plataforma de Desarrollo

La instalación de la plataforma de desarrollo implicó la instalación manual de IIS, componentes adicionales y la configuración de sitio. Las configuraciones adecuadas fueron después instrumentadas sobre el servidor en producción con sistema operativo NT Server. Sin embargo, es importante documentar que ante una eventual actualización desde NT 4.0 a Windows XP Professional en el servidor en producción como se ha sugerido, IIS 5.0 se instalará de manera predeterminada adoptándose todas las configuraciones preexistentes por lo que no será necesario en principio ajustar configuraciones.

Emisión e Instalación de Certificados para el Servidor de Desarrollo

Como se ha mencionado previamente, el desarrollo de sitio seguro proporciona seguridad usando una combinación del protocolo SSL (Secure Sockets Layer) y certificados digitales.

Secure Sockets Layer (SSL) es un protocolo desarrollado inicialmente por Netscape Communications Corporation para dar seguridad a la transmisión de datos en Internet. Utilizando la criptografía de clave pública, SSL provee autenticación de servidor y validación de cliente, encripción de datos sobre la capa de transporte, e integridad de los datos en las comunicaciones cliente/servidor.

Para el Sitio Seguro de la Penitenciaría se implementó a través de SSL, cifrado de 128 bits totalmente compatible con los principales navegadores Microsoft y Netscape.

SSL maneja las comunicaciones encriptadas y la mutua autentificación entre navegadores y el servidor seguro. Los certificados SSL proporcionan autentificación para el servidor seguro.

En esta primera fase de desarrollo, se implementó sitio seguro con autenticación de servidor, pero sin validación de cliente. Esta implementación prescinde de la presentación de Certificados Digitales de usuarios en transacciones con el sitio seguro. En el esquema actual, el acceso restringido a la información se garantiza mediante la utilización de la autenticación de Windows integrada, básica o de texto implícita. Esto permite, sólo a los usuarios autorizados, ver todos los archivos y tener acceso a las aplicaciones de páginas Active Server en el servidor Web. También da control completo a los administradores sobre el sitio.

Bajo este esquema de desarrollo, el paso siguiente a la instalación de la plataforma y la configuración del sitio de prueba, consistió en la emisión de un Certificado de Servidor para el servidor de desarrollo.

Al igual que otros web-server IIS da la posibilidad de trabajar con certificados autofirmados o con certificados validados por una Autoridad Certificante. Ante la alternativa de trabajar con certificados autofirmados; se decidió utilizar los certi-

ficados que podía emitir la AC-URME (Autoridad Certificante de la Unidad de Reforma y Modernización del Estado), aún en su carácter de prototipo, con dos objetivos.

1. Probar los servicios del software PKI implementado y sus desarrollos complementarios, en una aplicación concreta y con un marco procedimental determinado.

2. Instaurar la necesidad de contar con una Autoridad Certificante a la hora de emprender este tipo de desarrollos. Esto tiende a generar conciencia de que es la Autoridad Certificante quien proporciona garantías concernientes a la identidad de la organización que provee el sitio web.

A continuación se presenta a modo de marco general, el ***procedimiento informático*** que debe desarrollarse para obtener un Certificado Digital firmado por una Autoridad Certificante (AC). Este procedimiento que algunas veces es transparente al usuario, es el que en general proponen la mayoría de la empresas líderes en Certificación Digital y los documentos de trabajo más aceptados en la industria. Así mismo, es totalmente coherente con los requisitos establecidos por la Ley 25.506 y sus normas complementarias.

1. El solicitante o suscriptor crea, haciendo uso de alguna herramienta proveedora de servicios criptográficos, un par de claves encriptadas, pública y privada.

2. Una vez creado el par de claves, el solicitante genera una petición de certificado basada en la clave pública. La sintaxis detallada de esta petición o CSR está descripta por el Estándar PKCS#10 de RSA. La petición contiene información sobre el suscriptor. En el caso de que éste

sea un servidor habrá datos referentes al dominio, responsables y hosting del mismo.

3. El solicitante deberá entonces enviar la petición de certificado o CSR, junto con los documentos que prueben su identidad a una AC que resulte confiable para los usos a los que estará determinado el Certificado.

4. La Autoridad Certificante, a través de su Autoridad de Registro posiblemente, cumplimentará los procedimientos establecidos para verificar la identidad del suscriptor.

5. Una vez cumplimentadas las verificaciones pertinentes, la Autoridad Certificante firmará y enviará al suscriptor o responsable del sitio su certificado digital.

6. Luego los suscriptores deberán instalar los Certificados en su browser o en su servidor (en el caso de un certificado SSL) y utilizarlos para manejar transacciones seguras.

Presentado este marco general, documentamos a continuación detalladamente, el procedimiento informático que se siguió para emitir el Certificado SSL para el servidor de desarrollo.

La Interfase de Administración de Servicios de Internet Information Server incluye tres asistentes para administrar la seguridad de un sitio Web seguro. El Asistente para certificados de servidor Web permite administrar las características de Capa de sockets seguros (SSL) y los certificados de servidor. El asistente para CTL permite administrar listas de certificados de confianza (CTL). Las listas de certificados de confianza son listas de entidades emisoras de certificados de confianza para cada sitio Web o directorio virtual. El asistente de permisos permite

asignar permisos de acceso NTFS y Web a sitios Web, directorios virtuales y archivos en el servidor.

En este punto, nos interesa documentar en particular el modo de operación del asistente para certificados de servidor Web. Este asistente permite solicitar, instalar y renovar los certificados de servidor a través de una interfaz gráfica. El asistente detecta si ya se ha instalado un certificado de servidor y si va a caducar. Los Certificados a instalar pueden ser emitidos por una Autoridad Certificante según el estándar X509 ya sea por una entidad emisora de certificados en línea, como los Servicios de Certificate Server de Microsoft o la CA de VeriSign, o por un archivo que se ha obtenido previamente en el Administrador de claves (KeyStore en IIS).

Para solicitar y posteriormente instalar el Certificado SSL en el servidor de desarrollo se utilizó este asistente siguiendo los distintos pasos:

1. Mediante el Asistente para la Certificados de Servidor Web de IIS, se generó el par de claves pública y privada y se emitió la Solicitud de Requerimiento de Certificados según lo prescribe la norma RSA PKCS#10. Como resultado de este proceso se obtuvo un archivo de texto certreq.txt el cual contiene el requerimiento de emisión (CSR - Certificate Request).

—BEGIN NEW CERTIFICATE REQUEST—
MIIEeDC CA2ACAQAwgZcxDzANBgNVBAMTBmJsYWNrNDE1MDMGA1UECxMsVW5pZGFk
IGRlIFJlZm9ybWEgeSBNb2Rlcm5pemFjaW9uIGRlbCBFc3RhZG8xHDAaBgNVBAoT
E0dvYmllcm5vIGRlIE1lbmRvemExEDAOBgNVBAcTB01lbmRvemExEDAOBgNVBAgT
B01lbmRvemExCzAJBgNVBAYTAkFSMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA9nWzJ9CJuAKUr9dBPdONMkRvtvCIt6sqZPoZE3GDPHjnrlozAFrVclQc
oCCtSkNd/u/wjDIROnGD0FYEXyM6K7GZ6rYQsYW/2E8cX/GeKLxBJ5DhOlrQ9sjE
TtnO6SauRh9zAZLniP5ovo6WaNHSi7fCxMi1tnsQjMoTlw8yApaPLT/InYZMl1zH
iWQbp6ZqT2RVxS3ARR4ImFYHiBQ7Glasj1kjRWe5xjxvCgwAX+qV4z+QaNnJii4
osoZZQIrVqiVDEQaR+6gkhyBTN60y5rpv9+HhNW22RuqdiB7nDZQKE9dFYvdUN8z

GdUY70lA0subcVGNocCV2ffdCYWHawlDAQABoIIBmTAaBgorBgEEAYI3DQIDMQwW
CjUuMS4yNjAwLjIwewYKKwYBBAGCNwIBDjFtMGswDgYDVR0PAQH/BAQDAgTwMEQG
CSqGSIb3DQEJDwQ3MDUwDgYIKoZIhvcNAwICAgCAMA4GCCqGSIb3DQMEAgIAgDAH
BgUrDgMCBzAKBggqhkiG9w0DBzATBgNVHSUEDDAKBggrBgEFBQcDATCB/QYKKwYB
BAGCNw0CAjGB7jCB6wIBAR5aAE0AaQBjAHIAbwBzAG8AZgB0ACAAUgBTAEEAIABT
AEMAaABhAG4AbgBlAGwAIABDAHIAeQBwAHQAbwBnAHIAYQBwAGgAaQBjACAAUABy
AG8AdgBpAGQAZQByA4GJAKoQfdCmk/sTC7PqiHgRRcxsp2qJ4BxtDnaIVJepD+fX
EC0SlVR+Mgzd7GvjYSHJiWuVXtylQptKv95Dpz+GOJSLXsSm+V4EFXQGQVaxbMmh
KHHQGY4q8Ocog01ALcnJr4w3+31rHK4LB1RgmIuCU2eNwEtLEv/qGi9c0Mu4IuAw
AAAAAAAAAAAwDQYJKoZIhvcNAQEFBQADggEBAEzaCpJw2fvxOwELjx3FS6SPBiOL
dkczCwqCp5/LnbqhxBtJva64hTLOT9GH0i97QpdP/AIZq6TdlSatb6Ao0mg4zGdZ
RF5aKTRMlajnW/arSRXepoInx62Cqw9tAac60f9wzlAyvnw6sNgNRHprVCr27SEr
bGkBOxwCleV/CxozmneLjSGuOlgnZ+C91RKkO9s8q2TjNIM++ezquDX2Mw9JZZTk
hhAa/aOCREes/amNdTmpv8A41UQL9WTxVF/qc7+BeGm1rZHXy3+2G40gbmYw/iEZ
ngYMi0GjqtC5HslAMQqNXuKWh7Z1NNaoGtQ6yURLZDh5a/Rnhl63d936D9w=

——END NEW CERTIFICATE REQUEST——

2. Se agregó un usuario a la base de datos del prototipo AC-URME para procesar el requerimiento a nombre de este usuario. Los usuarios creados en la AC-URME permiten identificar a una entidad final o un servidor y gestionar el CVS de los Certificados asociados a esta entidad. A cada usuario en la ACURME se pueden asociar solicitudes y certificados en distintos estados: a la espera de ser aprobado, generado, revocado, etc. La líneas de comandos para completar esta acción en la ACURME fue:

[root@reform10 ejbca]# ./ra.sh adduser black4 *** "C=AR,O=Gobierno de Mendoza,OU=Unidad de Reforma y Modernizacion del Estado, CN=black4" null null 1 3***

Esta línea de comandos responde a la sintaxis general

ra adduser <username> <password> <dn> <subjectAltName> <email> <type> <token> [<certificateprofile>] [<endentityprofile>]

donde:

DN es el Distinguished Name

SubjectAltName es de la forma "rfc822Name=<email>, dNSName=<host name>, uri=<http://host.com/>". En nuestro caso, no utilizamos esta norma.

Email: email del solicitante

Type: Es una constante numérica que indica el tipo de entidad solicitante. En nuestro caso 1 corresponde a ENDUSER

Token: Indica formatos para el Keystore: User Generated=1; P12=2; JKS=3; PEM=4

Existing certificate profiles : Es una constante numérica que indica el perfil de certificado a emitir: En nuestro caso SERVIDOR indica el perfil de un certificado SSL con la estructura y extensiones que se han definido en la AC-URME por defecto para este perfil.

Existing endentity profiles : Define el perfil de la entidad que será certificada. En nuestro caso Certificado de Servidor indica que la entidad se ajusta al perfil de un servidor, tal como se ha parametrizado la AC-URME.

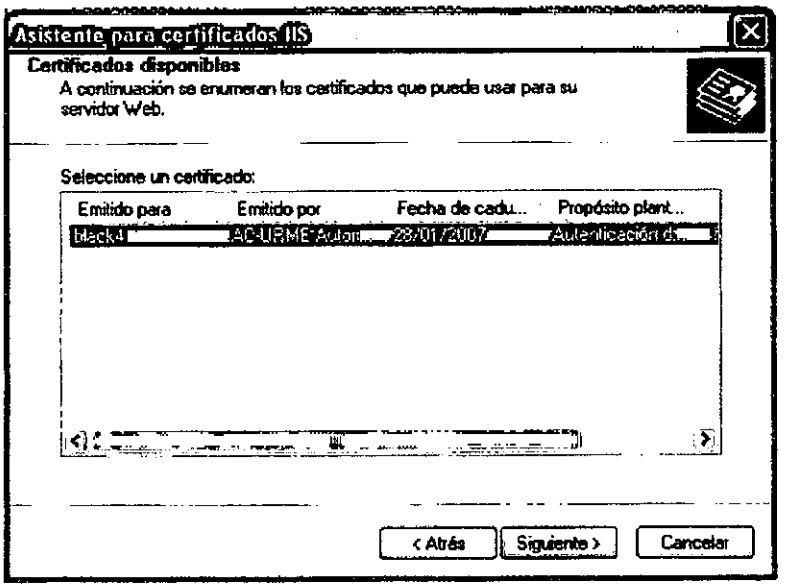
3. Se procesó el requerimiento de emisión de certificado para el usuario black4 agregado, obteniéndose el certificado en formato PEM-Encoded.

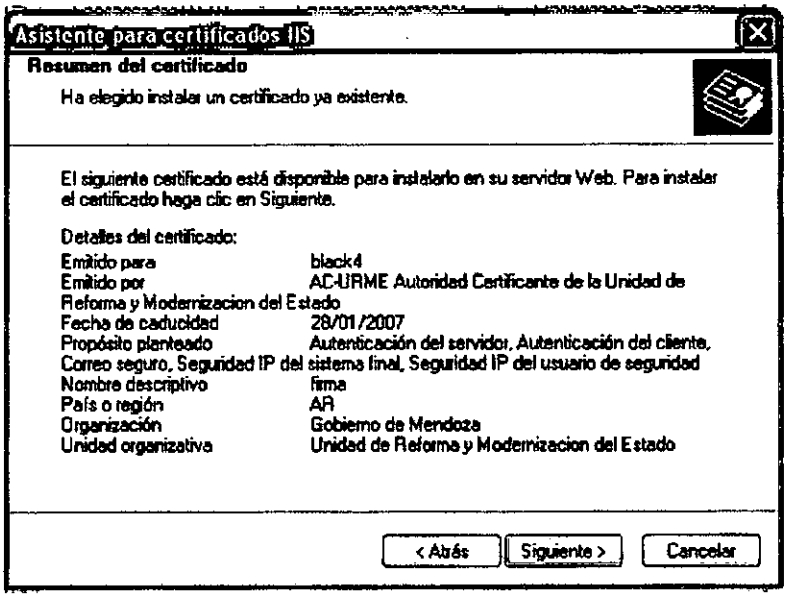
[root@reform10 ejbca]# ./ca.sh processreq black4 black4 certreq.txt black4.pem ca.sh ca.der -der

°-----BEGIN CERTIFICATE-----
JIEBSDSCEXoCHQEwLQMJSoZILvoNVQECSQAwcSETMRkOAMUTBhMuVrM
mloAnBdNVBAoTF1JTQSBEYXRhIFNlY3VyaXR5LCBJbmMuMRwwGgYDVQ
QLExNQZXJzb25hIENlcnRpZmljYXRlMSQwIgYDVQQDExtPcGVuIE1hc
mtldCBUZXN0IFNlcnZlciAxMTAwHhcNOTUwNzE5MjAyNzMwWhcNOTYw

NTE0MjAyOTEwWjBzMQswCQYDVQQGEwJVUzEgMB4GA1UEChMXUlNBIER
hdGEgU2VjdXJpdHksIEluYy4xHDAaBgNVBAsTE1BlcnNvbmEgQ2VydG
ImaWNhdGUxJDAiBgNVBAMTG09wZW4gTWFya2V0IFRlc3QgU2VydmVyI
DExMDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDU/7IrgR6vkVNX40BA
q1poGdSmGkD1iN3sEPfSTGxNJXY58XH3JoZ4nrF7mIfvpghNi1taYim
vhbBPNqYe4yLPAgMBAAEwDQYJKoZIhvcNAQECBQADQQBqyCpws9EaAj
KKAefuNP+z+8NY8khckgyHN2LLpfhv+iP8m+bF66HNDUlFz8ZrVOu3W
QapgLPV90kIskNKXX3a
-----END CERTIFICATE-----

4. Una vez obtenido el archivo ***black4.pem*** con el Certificado SSL firmado por la AC-URME, se procedió a instalar el certificado en el web-server. Esta instalación se realiza asociando el par de claves generadas previamente al archivo PEM-Encoded del Certificado mediante un wizard proporcionado por el Asistente para Certificados Web de IIS. Esta combinación de clave y certificado se almacena en un registro del servidor.





Nota: Aunque IIS permite realizar "Copias de seguridad de claves", implicando esto hacer una copia del registro completo (clave privada y certificado), las disposiciones técnicas requieren no generar copias de seguridad por cuanto esto podría comprometer la inviolabilidad de la clave privada.

El certificado SSL utilizado se ajusta al estándar X.509 con extensiones SSL.La siguiente tabla detalla la estructura y contenido del Certificado emitido para el Servidor de Desarrollo ***black4***, ajustada a las especificaciones de un X.509 v3, a la recomendación RFC 3280 y al diseño preliminar de los certificados SSL emitidos por la AC-URME.

Certificados de Servidor / SSL

TbsCertificate

SIGLA	Nombre del Campo ASN.1	Descripción	Contenido Certificado SSL Intranet Penitenciaria
V	***version***	Versión del Certificado	V3
SN	***serialNumber***	Número de Serie del Certificado	59 4d 91 d3 72 97 dd 4c
AI	***signature***	Algoritmo de firma	sha1RSA
CA	***issuer***	Expedidor / Emisor	C = AR O = Gobierno de Mendoza OU = Secretaria Administrativa Legal y Tecnica del Gobierno de Mendoza OU = Unidad de Reforma y Modernizacion del Estado CN = AC-URME Autoridad Certificante Unidad de Reforma y Modernizacion del Estado Gobierno de Mendoza
T	***Validity***	Validez	Viernes, 26 de Noviembre de 2004 10:47:58 a.m. Domingo, 26 de Noviembre de 2006 10:57:58 a.m.
UI	***subject***	UniqueIdentifier. Sujeto / Asunto	C = AR O = Gobierno de Mendoza OU = Unidad de Reforma y Modernización del Estado CN = black4
A	***subjectPublicKeyInfo***	Información de la clave pública del sujeto	Clave pública RSA (2048) bits
	Extensions	Extensiones	***No Críticas*** • Uso mejorado de Claves: Autenticación de Servidor (1.3.6.1.5.5.7.3.1) • Identificador de clave del sujeto: 5c 93 6d 00 21 d6 b1 99 a0 62 75 f9 51 44 a6 a8 b6 b3 9f d5 • Indetificador de clave de la Autoridad Certificante: Id. de clave=13 8d c7 41 8d 1e b5 d4 67 74 4b 31 be a2 1b 0e 3f 8d dd 49 • **Extensiones Críticas** • Restricciones Básicas Tipo de asunto=Entidad final Restricción de longitud de ruta=ninguna • Uso de la Clave: Firma Digital, Cifrado de clave (a0 00)

signatureAlgorithm: Sha1RSA	Sha1RSA
SignatureValue:	a6 41 f3 22 d1 65 ca 8e 63 72 24 92 7a 0d 51 f1 43 27 f3 fb

Configuración de SSL en IIS

Una vez instalado el certificado SSL en el servidor de desarrollo, se configuró SSL mediante el Administrador de Servicios de Internet del MMC (Microsoft Mangement Console).

IIS permite habilitar características SSL para todo el sitio o para determinados directorios físicos o virtuales mapeados en un sitio. Estos aspectos son configurados desde la hoja de propiedades Directorios en la consola de administración del web-server.

Este modo de operación implica decidir, previo a la puesta en marcha del sitio seguro de la Penitenciaría Provincial, que tipo de contenidos deben ser asegurados mediante el uso de esta tecnología y determinar que directorios reales o virtuales dentro de la estructura de archivos del sitio deben ser protegidos. En particular, IIS requiere que para cada directorio que se desee proteger se configuren adecuadamente los siguientes aspectos.

- ***requerir canal seguro (SSL):*** esta opción debe estar activada para requerir un vínculo de comunicación cifrada (https) para ese directorio en particular.

- ***requerir cifrado de 128 bits:*** el nivel de cifrado también debe configurarse explícitamente para cada directorio a asegurar. En el caso de la Penitenciaría se decidió trabajar en todos los casos con cifrado de 128 bits.

- ***certificados de cliente:*** en primera instancia no se implementará autenticación de clientes para el sitio seguro de la Penitenciaría. Por ello se desactivaron las funciones vinculadas a la solicitud de certificados de cliente para cada directorio a proteger. La opción ***omitir certificados de cliente*** fue desactivada.

E. Prueba del Sistema:

Una vez instalada y configurada la plataforma de desarrollo, se diseño e instrumentó un conjunto de pruebas para evaluar la operatoria completa del Sitio Seguro en función del modelo de comportamiento esperado. En función de los resultados se realizaron los ajustes necesarios en la configuración del webserver y en el formato de los Certificados de prueba emitidos previo a la puesta

En particular, se evaluaron los siguientes puntos:

Certificados SSL	*Certificados X509 v1 o superior* *Dominios* *Formato de certificados*	Se comprobó el funcionamiento del web Server con Certificados X509 v1 y superior. Se comprobó la necesidad de usar el URL real de cada sitio como CN en el Certificado de servidor para que los browsers no acusen diferencias entre el nombre del sitio y el nombre certificado. Se realizaron pruebas de instalación en IIS de certificados codificados en distintos formatos: PEM, P12
Cifrado	*Cifrado SSL 40 bits* *Cifrado SSl 128 bits*	Se comprobaron ambos esquemas de cifrado

1.1.1 ***Browsers***	*1.1.2 Internet Explorer 5 o superior* *Netscape Communicator 4 o superior* *Cadena de certificación*	Se comprobó la instalación de certificados emitidos por la AC-URME y el soporte SSL a 128 bits. Se comprobó el correcto reconocimiento de la cadena de certificación una vez instalado correctamente el Certificado RootCA en el browser del cliente.
Host Virtuales	*Configuración de IIS*	Se comprobó la necesidad de contar con números IP reales para cada sitio, aún cuando se configuraran host virtuales.
Seguridad	*Seguridad de las claves*	Se realizaron todas las pruebas asociadas con la encripción y protección de las claves privadas de los suscriptores. Y la protección de los Certificados de Servidor en el web Server. Se realizaron pruebas sobre la generación de copias de seguridad de claves, aunque finalmente se recomendó que no se realiza-

		ran backups de claves privadas.
Configuración de puertos	*Configuración de IIS*	Se comprobó la configuración alternativa de SSL en el puerto estándar 443 y en puertos alternativos como 8443 y 442.
Rendimiento	*Test de carga de trabajo*	Se realizaron pruebas intensivas de las aplicaciones Web con Web Application Stress (WAS) para garantizar la estabilidad y determinar las características de rendimiento de las aplicaciones en la plataforma de desarrollo.

F. Puesta en marcha de la implementación

Concretada la etapa de pruebas se realizaron las actividades necesarias para la instalación y puesta en marcha de sitio seguro en el servidor en producción y la capacitación del administrador del web-server.

En un trabajo conjunto con el responsable informático de la Penitenciaría Provincial se fijaron pautas en cuanto a responsabilidades asumidas, procedimientos de trabajo y controles.

La puesta en marcha implicó el desarrollo de las siguientes tareas:

1. Definiciones finales sobre la metodología de implementación y puesta en marcha
2. Identificación de aplicaciones a proteger
3. Asignación de recursos y responsables
4. Capacitación de responsables
5. Emisión del Certificado de Servidor
6. Configuración de sitio seguro en el servidor en producción

Definiciones finales sobre la metodología de implementación

De acuerdo a los resultados positivos de las pruebas realizadas en la plataforma de desarrollo y a las características operativas de la Intranet Penitenciaria se decidió implementar los cambios directamente en el web-server en producción, previendo un resguardo de las configuraciones previas de IIS como previsión de contingencias. No existe en la plataforma tecnológica de la Penitenciaría un esquema de hardware redundante para prevenir caídas de servidores u otro tipo de mecanismos de protección que permitieran proponer un esquema de implementación alternativo.

Identificación de aplicaciones a proteger

En función de los niveles de seguridad definidos para la información, se decidió requerir conexión segura para todas aquellas aplicaciones que sirvieran contenido dinámico en función de bases de datos internas.

Asignación de recursos y responsables

El administrador de la Intranet penitenciaria fue asignado como responsable de la administración del sitio seguro y de la preservación de la clave privada del Certificado de Sitio.

Esta persona se desempeño durante la etapa de implementación, con el soporte permanente del equipo de desarrollo de firma digital y bajo el control del responsable informático de la Penitenciaría Provincial.

La implantación efectiva de sitio seguro no requirió extender la actual infraestructura de conectividad, equipos e insumos con que opera la Intranet Penitenciaria.

Capacitación de responsables

Se capacitó al Administrador del Web-Server en los aspectos técnicos y procedimentales relativos al uso de tecnologías de clave pública, el uso de certificados, el protocolo SSL, el perfil de certificados de servidor y la infraestructura PKI. Se profundizó especialmente en las configuraciones técnicas necesarias en el Administrador de Servicios de Internet Information Server para la implantación de canal seguro SSL.

El adiestramiento requirió cuatro jornadas de 4hs. realizadas en la oficina de Cómputos de la Penitenciaría Provincial.

Emisión e Instalación del Certificado de Servidor

Siguiendo el mismo procedimiento descrito en la fase de desarrollo, se procedió a obtener e instalar el Certificado SSL para el servidor en producción. La siguiente tabla describe el perfil del Certificado de Servidor que actualmente se encuentra operativo en la Intranet Penitenciaria.

Certificados de Servidor / SSL

TbsCertificate

SIGLA	Nombre del Campo ASN.1	Descripción	Contenido Certificado SSL Intranet Penitenciaria
V	***version***	Versión del Certificado	V3
SN	***serialNumber***	Número de Serie del Certificado	59 3a 75 c3 72 57 bd ac
AI	***signature***	Algoritmo de firma	sha1RSA
CA	***issuer***	Expedidor / Emisor	C = AR O = Gobierno de Mendoza OU = Secretaria Administrativa Legal y Tecnica del Gobierno de Mendoza OU = Unidad de Reforma y Modernizacion del Estado CN = AC-URME Autoridad Certificante Unidad de Reforma y Modernizacion del Estado Gobierno de Mendoza
T	***Validity***	Validez	Lunes, 17 de Enero de 2005 10:47:58 a.m. Miercoles, 17 de Enero de 2007 10:57:58 a.m.
UI	***subject***	UniqueIdentifier. Sujeto / Asunto	C = AR O = Gobierno de Mendoza OU = Penitenciaria Provincial CN = penitenciaria
A	***subjectPublic KeyInfo***	Información de la clave pública del sujeto	Clave pública RSA (2048) bits
	Extensions	Extensiones	***No Críticas*** • Uso mejorado de Claves: Autenticación de Servidor (1.3.6.1.5.5.7.3.1) • Identificador de clave del sujeto: 5c 93 6d 00 21 d6 b1 99 a0 62 75 f9 51 44 a6 a8 b6 b3 9f d5 • Indetificador de clave de la Autoridad Certificante: Id. de clave=13 8d c7 41 8d 1e b5 d4 67 74 4b 31 be a2 1b 0e 3f 8d dd 49 • **Extensiones Críticas** • Restricciones Básicas Tipo de asunto=Entidad final Restricción de longitud de ruta=ninguna • Uso de la Clave: Firma Digital, Cifrado de clave (a0 00)

signatureAlgorithm: Sha1RSA	Sha1RSA
SignatureValue:	a6 41 d3 21 c2 78 ca ce 25 71 24 b2 7a 0d 01 f1 43 c7 f3 fb

El Certificado SSL fue emitido por la AC-URME a pedido formal del Responsable Informático de la Penitenciaría Provincial. No obstante se debe considerar que el carácter de prototipo experimental de la AC-URME restringe la validez y credibilidad del Certificado emitido. Por este motivo se ha solicitado formalmente a la ONTI (Oficina Nacional de Tecnologías de la Información) que contemple la posibilidad de adecuar su Autoridad Certificante para emitir Certificados de Autenticación de Equipos a personas jurídicas a través de nuestra Autoridad de Registro.

Configuración de sitio seguro en el servidor en producción

Una vez instalado el certificado SSL en el servidor en producción y determinados los directorios cuyo contenido sería accesible mediante canal seguro, se configuró el uso de SSL en el web-server del Servidor siguiendo, para cada carpeta en el Administrador de Servicios de Internet Information Server, el procedimiento documentado en la fase de desarrollo.

Este procedimiento fue realizado por los técnicos de la unidad en cooperación permanente con el Administrador del web-server de la Intranet Penitenciaria.

G. Evaluación de la experiencia:

Resulta necesario identificar las variables e indicadores más apropiados, y preparar o adaptar los instrumentos que se pueden utilizar para recoger la información, combinando métodos cualitativos y cuantitativos de investigación.

Hemos definido una serie de indicadores que son de gran utilidad a la hora de recoger feedback crítico. Nos servirán para evaluar los resultados de la experiencia piloto de Sitio Seguro en el tiempo y para diseñar las acciones correctivas que, en función de estos, resulten necesarias de implementar.

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

Indicadores críticos

La siguiente tabla define los indicadores generales utilizados para medir el rendimiento de la experiencia con enfoque en los procesos de las aplicaciones específicas.

Experiencia piloto Sitio Seguro (Mediciones realizadas al 07/01/05)	
Indicadores Cualitativos	**Métricas y Resultados**
Satisfacción de los usuarios: # Quejas y Reclamos	No se han registrado quejas por el sistema de Sitio Seguro

Indicadores Cuantitativos	Métricas y Resultados
Eficiencia:	
% de certificados emitidos correctamente	100 % (1 de servidor)
# de fallas del sistema	0 (No se produjeron fallas)
# de interrupciones del servicio	0 (El servició estuvo disponible 365/7)
Asistencia:	
# de asistencias otorgadas	8 (ocho) Acciones de asistencia técnica
% de asistencias exitosas	100%
Uso del Sistema:	
# de comunicaciones seguras establecidas	3123

Acciones correctivas detectadas	Acciones correctivas implementadas
No se han detectado hasta la fecha	Ninguna

Calificación ponderada final

Implementación exitosa de la experiencia

Consejo Federal de Inversiones

Lic. Pablo Guillermo Lioy

"Firma Digital"