Universidad de Buenos Aires
Facultades de Ciencias Económicas,
Ciencias Exactas y Naturales e Ingeniería

Maestría
en
Seguridad Informática

Confidencialidad del correo electrónico

Diseño de un esquema de seguridad basado en DNSSEC

Autor: Ing. Gustavo Luis Nakasone
Tutor: Dr. Hugo Scolnik

Año 2012
Cohorte 2010

Declaración Jurada de origen de los contenidos.

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO

Gustavo Luis Nakasone
DNI 23.811.862

Resumen.

El objetivo de la presente tesis es proponer el diseño de un esquema de seguridad que proteja la confidencialidad de la correspondencia electrónica. El mismo se fundamenta en el uso de certificados digitales accesibles a través de un servicio basado en DNSSEC y en la introducción de una serie de mecanismos que permitan extender sus beneficios al usuario común (con conocimientos básicos en informática).

Palabras claves.

Correo electrónico - Confidencialidad - Certificados digitales - DNSSEC

Tabla de contenido

1 . Introducción. 7
1.1. Planteo del problema. 7
1.2. Estado actual. 9
1.3. Una primera aproximación a la solución. 9
1.4. Hipótesis. 11
1.5. Objetivos. 11
1.5.1. General. 11
1.5.2. Específicos o particulares. 11
1.6. Alcances y limitaciones de la propuesta. 12
1.7. Metodología y plan de actividades. 12
2. Procurando confidencialidad. 14
2.1. Claves públicas y privadas. 14
2.2. Public Key Infrastructure. 14
2.3. Protección de la correspondencia electrónica. 16
3. Accediendo a los certificados digitales. 17
3.1. DNS. 17
3.2. Extensiones de seguridad. 17
3.3. Resolución de nombres bajo DNSSEC. 19
4. Esquema de seguridad. 25
4.1. Introducción. 25
4.2. Asegurando la confidencialidad. 27
4.2.1. Emisión. 27
4.2.2. Tránsito por internet. 31
4.2.3. Recepción / despacho. 31
4.2.4. Respaldo. 33
4.3. Firma corporativa. 33
5. Servicio de publicación de certificados. 35
5.1. Requerimientos. 35
5.2. El servicio. 35

5.2.1. DNSSEC. 36
5.2.2. LDAP. 36
6. Servicio de cifrado. 38
6.1. Introducción. 38
6.2. Requerimientos funcionales. 39
6.3. El servicio. 39
7. Prueba de concepto. 41
7.1. Software utilizado. 41
7.2. Software adicional. 42
7.3. La maqueta. 42
7.4. Resumen de las tareas completadas. 45
7.5. Resultado de las pruebas. 47
7.5.1. Firma corporativa. 47
8. Conclusiones finales. 49
ANEXO I - Prueba de concepto: El servidor de cifrado. 51
A. Lenguaje de programación. 51
B. Módulos utilizados. 51
C. Script. 52
ANEXO II – Prueba de concepto: Instalación y configuración de servicios. 53
A. Servicio LDAP (OpenLDAP). 53
A.1. Instalación. 53
A.2. Configuración. 53
A.3. Comandos utilizados. 54
A.4. Creación de las entradas. 54
B. Arquitectura PKI (OpenSSL). 55
B.1. Instalación. 55
B.2. Creación de las CA. 55
B.3. Observaciones. 56
C. Servicio DNSSEC (Bind). 57
C.1. Instalación. 57
C.2. Configuración. 58
C.3. Generación de zonas. 58
C.4. Generación de claves. 59
C.5. Firma de la zona. 59

C.6. Chequeo con dig. 59
D. Servicio IMAP (Cyrus). 60
D.1. Instalación..... 60
D.2. Configuración..... 60
D.3. Creación de usuarios. 61
Fuentes..... 63
Bibliografía. 64

Agradecimientos.

A Dios en primer lugar, por permitirme llegar a esta instancia, por todo aquello que me ha dado, por su amor incondicional.

A mi familia y amigos por el apoyo, la confianza y el ánimo que han sabido prodigarme durante esta etapa. Con especial cariño a mi madre, en quien siempre hallo un ejemplo a seguir por sus nobles virtudes.

A mis profesores de la Maestría en Seguridad Informática por la educación recibida, quienes con calidad, dedicación y esfuerzo han enriquecido mi formación académica y profesional. Especialmente al Dr. Hugo Scolnik, quien además me ha guiado en el desarrollo de la tesis. Solamente gracias a su dirección, estímulo y valiosa colaboración ha sido posible finalizar el presente trabajo.

Confidencialidad del correo electrónico
Diseño de un esquema de seguridad
basado en DNSSEC

1 . Introducción.

1.1. Planteo del problema.

La correspondencia electrónica se ha afianzado sólidamente como uno de los medios de intercambio de mensajes e información digital más utilizado en el ambiente laboral. Prueba de ello son los 112 emails que en el 2011, según informes de Pingdom, el usuario corporativo promedio ha enviado y recibido diariamente [1]. Pingdom, empresa sueca dedicada al monitoreo de servicios de internet, ya había reportado el año pasado (2011) que en el 2010 habían sido enviados cerca de 107 billones de emails [2].

El uso masivo del email, lo ha convertido en una importante y atractiva fuente de información digital. Al mismo tiempo, su escasa protección ha logrado atraer la mirada y el interés de terceros, tornándolo como el objetivo de variados ataques. La realidad es que asegurar su resguardo ante accesos no autorizados se puede transformar en una tarea por demás compleja. Especialmente porque se trata de información que viaja por la internet, atravesando distintos puntos (nodos) en los cuales se pierde el control completo de las acciones que pueden llegar a ser ejecutadas sobre la misma. Además, el hecho de que generalmente los correos electrónicos residan en las casillas en texto plano también deja abierta la posibilidad de que puedan verse comprometidos ante accesos lógicos y/o físicos no autorizados (al servidor de correo o a las cintas de respaldo) o ante el obrar desleal por parte de alguno de los administradores informáticos. Toda medida que persiga al aseguramiento de la confidencialidad de los emails,

en tránsito o en la misma casilla de correo, constituirá un avance significativo en la protección de la privacidad de la información personal y/o corporativa.

Transitando los últimos años pueden resaltarse algunos casos notorios de correspondencia electrónica "robada" cuya difusión ha trascendido a escala internacional:

- En noviembre del 2009, en el sitio de WikiLeaks (http://wikileaks.org), fueron publicados emails intercambiados entre científicos especializados en climatología, robados de un servidor de la Unidad de Investigación Climática de la Universidad de Anglia del Este, Norwich (Reino Unido). El conocimiento público de dicha correspondencia daría luego origen a un incidente conocido como Climagate. [3][4][5]
- En febrero del 2011, el grupo Anonymous hackeó el sitio web de la empresa de seguridad informática HBGary Federal. Como resultado de esa intrusión, entre otras acciones, pudieron copiar y difundir cerca de 60000 emails. [6][7]
- En agosto del 2011 la justicia argentina ordenó el bloqueo del sitio de Leakymails (http://www.leakymails.com), pues divulgaba emails de funcionarios públicos, jueces y periodistas. [8][9]
- En febrero de 2012, Wikileaks comenzó a publicar cerca de 5 millones de emails robados por hackers a Strategic Forecasting Inc. (Stratfor), una reconocida empresa especializada en servicios de inteligencia y espionaje global. [10]

Acontecimientos como los indicados ponen de manifiesto que el robo de emails resulta en una actividad estimada por los hackers y que las medidas de seguridad aplicadas para el resguardo de su confidencialidad no han resultado del todo efectivas. Y siendo la confidencialidad de la información uno de los tres pilares sobre los que se sostiene la seguridad informática, la importancia de su protección no admite discusiones.

1.2. Estado actual.

Hoy en día las claves públicas se han convertido en instrumentos valiosos, difíciles de sustituir, al momento de proveer seguridad sobre todo tipo de datos digitales. Muchos de los servicios informáticos prestados en redes privadas e internet los emplean bajo la forma de certificados digitales, asignándoles el rol protagónico en variados procesos de autenticación y cifrado en sus comunicaciones. Estos mismos certificados pueden ser hallados tanto en desarrollos populares como los conocidos web servers que utilizan el protocolo https, como en aquellas implementaciones más sofisticadas que han de responder a mayores exigencias en materia de seguridad, como es el caso de las tecnologías VPN (Virtual Private Network).

Uno de los servicios de red cuyo nivel de seguridad puede verse beneficiado enormemente con la inclusión de estos certificados digitales es, precisamente, el del correo electrónico. El empleo de certificados digitales para cifrar el contenido de emails hace años que ha dejado de ser una novedad, aunque es una realidad que la mayoría de los usuarios comunes desconoce. Y, hoy por hoy, el uso de los mismos requiere la activa participación del usuario final. También sucede que quienes están en conocimiento del tema muchas veces desisten de su utilización por la dificultad o molestia extra que conlleva la obtención y el uso del certificado digital del destinatario al momento de concretar el envío. En otras palabras, en los certificados digitales podemos hallar los instrumentos ideales para brindar al correo electrónico un nivel óptimo de confidencialidad, el desafío consiste en diseñar un sistema que facilite su introducción a la vida cotidiana del usuario común.

1.3. Una primera aproximación a la solución.

Para que un usuario envíe un email cifrado necesita, primero, acceder al certificado digital del destinatario y luego ordenarle al cliente de correo el cifrado del mismo. No existe un mecanismo transparente (al usuario) que

ejecute los pasos mencionados, ni una forma práctica y eficiente de disponer de los certificados necesarios para completar tal operación.

En lo que se refiere puntualmente a la disponibilidad de los certificados digitales, hace poco menos de una década se ha definido un estándar, conocido como DNSSEC (Domain Name System Security Extensions), que provee una forma segura y confiable de cumplimentarla. DNSSEC añade mejoras de seguridad al estándar DNS (Domain Name System). No obstante, la implementación global de DNSSEC no resulta una tarea sencilla, muy pocos avances han habido al respecto debido a inconvenientes encontrados durante la planificación de su puesta en producción. Más adelante, en el capítulo 3, se tratará el tema con mayor detenimiento. De todas formas otras soluciones alternativas son posibles siguiendo los mismos lineamientos dictados por DNSSEC, pero enfocados exclusivamente en el registro y la publicación de certificados digitales en internet.

Por otro lado, es importante tener siempre presente que una mala implementación de medidas de seguridad puede terminar generando resultados adversos. Por ejemplo, resulta claro que un email cifrado no podrá ser escaneado por un anti-malware/spam, por lo que la publicación y utilización inadecuada de certificados digitales podría facilitar la diseminación de malware, favorecer otros tipos de ataque y también permitir la proliferación de spam. Esa es la razón por la que han de tomarse una serie de recaudos a fin de evitar implicancias negativas derivadas de situaciones no deseadas.

El objetivo final es diseñar un esquema de seguridad que provea confidencialidad integral a los correos electrónicos a partir del momento mismo en que son enviados. Con ello se busca minimizar el número de amenazas dirigidas a vulnerar la privacidad de la información personal y/o corporativa contenida en la correspondencia electrónica, resultando en un aporte positivo en el campo de la seguridad informática.

1.4. Hipótesis.

Las hipótesis manejadas son las siguientes:

- El registro y la publicación de certificados digitales en un servicio basado en DNSSEC permitirá disponer de los mismos para el cifrado de correo electrónico.
- El empleo de servidores de cifrado con capacidad para realizar consultas DNSSEC (o a servicios similares) para obtener certificados digitales permitirá automatizar el cifrado de los emails sin necesidad de que intervengan las personas emisoras.
- La utilización de un certificado digital corporativo de la empresa que provee el servicio de correo al destinatario para cifrar el mensaje permitirá la ejecución correcta de operaciones de escaneo por parte de los servidores anti-malware y anti-spam.
- El uso de cifrado a partir del certificado digital del destinatario permitirá el resguardo confidencial de los emails en las correspondientes casillas de correo.

1.5. Objetivos.

1.5.1. General.

Diseñar un esquema de seguridad que proteja la confidencialidad de los emails basado en DNSSEC.

1.5.2. Específicos o particulares.

- Definir un servicio informático que permita el registro y la publicación en forma segura y confiable de certificados digitales en el ámbito de internet.
- Diseñar un mecanismo que provea confidencialidad al contenido del email saliente de manera automatizada, que no requiera la intervención activa del emisor.

- Proteger la confidencialidad de todos los emails a partir del momento en el que son despachados por el MUA (Mail User Agent). Incluyendo el tiempo que permanezcan en la casilla de correo del destinatario (y en las cintas de respaldo).
- Asegurar el correcto y debido accionar de las aplicaciones anti-malware y anti-spam corporativas.
- Implementar una prueba de concepto con el objeto de respaldar la solución de seguridad resultante.

1.6. Alcances y limitaciones de la propuesta.

- El esquema de seguridad empleará certificados corporativos y personales para preservar la confidencialidad de los correos electrónicos.
- El esquema de seguridad estará basado en el sistema DNSSEC.
- El esquema de seguridad permitirá resguardar la confidencialidad de los correos electrónicos enviados a partir de su aplicación.
- El esquema de seguridad no protegerá la confidencialidad de los correos electrónicos que ya se encuentren almacenados en texto plano en las casillas.
- Se realizará una prueba de concepto del esquema de seguridad solamente a efectos de su validación, no estará pensando para satisfacer las exigencias de un entorno 100% real. Primordialmente, el objetivo es el de brindar sustento práctico a la tesis a través de la implementación de un modelo de prueba enmarcado en un entorno simplificado.

1.7. Metodología y plan de actividades.

A fin de validar las hipótesis enunciadas se llevarán a cabo las siguientes tareas:

- Análisis del estándar DNSSEC en lo que respecta, específicamente, al registro y la publicación de certificados digitales. Se estudiará la viabilidad de su implementación efectiva a nivel global; de distinguirse serias dificultades se recurrirá al desarrollo de un servicio que satisfaga los mismos requerimientos (siempre basado en DNSSEC).
- Diseño funcional de un servicio de red que posibilite el cifrado de correo electrónico empleando certificados digitales. Dicho servicio es el que participará activamente en la protección de la confidencialidad del contenido de los emails desde su envío hasta la entrega a las casillas de correo respectivas.
- Diseño de una arquitectura de seguridad destinada a cifrar los correos electrónicos salientes con certificados digitales corporativos de la empresa del destinatario, a efectos de no obstaculizar el libre accionar de aquellas medidas de seguridad existentes en el extremo destino, como por ejemplo, las de detección de malware y spam. Al mismo tiempo se prevé en esta instancia la firma electrónica del correo con una clave corporativa a fin de avalar la autenticidad del origen.
- Diseño de una arquitectura de cifrado de los correos electrónicos a partir del certificado digital del destinatario para el resguardo de la confidencialidad de los mismos en la correspondiente casilla de correo.
- Desarrollo de una prueba de concepto que permita cristalizar los puntos anteriormente citados. Con ello se busca, por un lado, resaltar los beneficios resultantes de la implementación del esquema de seguridad propuesto, y, por el otro, probar su efectiva viabilidad.

2. Procurando confidencialidad.

El objetivo principal perseguido es el de proteger los correspondencia electrónica de la lectura no autorizada de terceros. Tal fin es fácilmente alcanzable a través del uso de las claves públicas, ajustándonos a los fundamentos de la criptografía asimétrica. Estas claves además, en una infraestructura que permita establecer cadenas de confianza, añaden a las mismas el poder de proveer una manera segura de verificar la autenticidad de los mensajes.

2.1. Claves públicas y privadas.

Como es sabido, el uso de claves públicas para cifrar un mensaje habilita a quien posea la correspondiente clave privada a descifrarlo. Asimismo, el uso de claves privadas para cifrar el resultado de aplicar un algoritmo de hash sobre un mensaje permite verificar su integridad. Pero solas no bastan para validar fehacientemente la autenticidad de las mismas. Una forma de resolver este problema es que un tercero en quien tengamos confianza certifique que la clave pública pertenece a quien dice ser. Y justamente esto es lo que ofrece PKI.

2.2. Public Key Infrastructure.

Esencialmente, en una infraestructura PKI (Public Key Infrastructure) los certificados se constituyen en artilugios digitales, emitidos por entidades de reconocimiento comprobable, que permiten asociar una clave pública con una identidad, estableciendo una cadena de confianza basada en la entidad emisora. Dicho certificado además contiene información extra relativa a la identidad del dueño de la clave pública y a la entidad que lo emitió, así como también sobre su propósito y período de validez. Los certificados respetan un formato definido por el estándar ITU-T X.509. La última versión, la 3,

contempla el soporte de extensiones que permiten la incorporación de más datos que, ordenados en una serie de campos, pueden ser utilizados para múltiples propósitos.

El proceso de asociación clave pública-identidad no es complicado. El interesado debe solicitar un certificado en base a su clave privada a la autoridad de una insfraestructra PKI, conocida como autoridad certificante. Es importante que la autoridad seleccionada sea considerada de confianza por quienes constituirán la contraparte en el proceso de identificación, de lo contrario el certificado pierde su utilidad. La autoridad, luego de verificar la identidad del interesado y la autenticidad de la solicitud, procederá a emitir el correspondiente certificado (la autoridad firma la clave pública del solicitante con su propia clave privada). El emisor del certificado (la autoridad certificante) deberá implementar los mecanismos más adecuados para corroborar la identidad de quien lo solicita. Este procedimiento suele implicar el uso de documentación probatoria. La validación del certificado emitido, siguiendo los principios de la criptografía asimétrica, se lleva a cabo utilizando el certificado autofirmado de la autoridad (su clave pública autofirmada).

La autoridad certificante, quien se encarga de la emisión de certificados, suele ser un ente privado o público especializado en el tema. Dicha entidad se encarga de administrar los certificados emitidos, que son identificados a través de un número de serie (serial). Dada la importancia de la tarea, los requisitos legales y técnicos para desempeñar dicha actividad son numerosos y muy exigentes, esto resulta muy necesario ya que el organismo emisor ocupa el primer lugar en esta cadena de confianza. Por ejemplo el NIST (National Institute of Standards and Technology), agencia federal perteneciente al Departamento de Comercio de EEUU, ha recomendado utilizar en una PKI, claves de 2048 bits cuando se trabaja con el algoritmo de cifrado RSA [11].

2.3. Protección de la correspondencia electrónica.

Los certificados digitales, bajo una estructura PKI, han probado ser los instrumentos adecuados para el manejo confiable de la seguridad en el entorno informático. Por un lado, permiten implementar mecanismos robustos que satisfacen diversos requerimientos de autenticación y cifrado. Por el otro, su aplicación directa sobre información digital proporciona altos niveles de confidencialidad e integridad. Es así que se han transformado en el elemento clave por excelencia en la implementación de mecanismos destinados a custodiar la autenticidad, la confidencialidad y la integridad de los correos electrónicos, misión que cubren con eficacia y eficiencia.

A pesar de sus evidentes beneficios, los certificados digitales no suelen ser empleados por el usuario promedio. El esquema de seguridad descripto en este trabajo define un mecanismo que busca vencer los dos principales obstáculos que suelen incidir en la toma de tales decisiones:

1) El simple desconocimiento o la inexperiencia por parte del usuario común en lo concerniente a aquellos temas vinculados con la seguridad informática. Mucho tiene que ver el pobre nivel de concientización recibido por el público internauta en general.

2) La dificultad para acceder fácilmente al certificado digital del destinatario del email. Situación que se torna en una verdadera molestia a medida que crece el número de destinatarios implicados.

3. Accediendo a los certificados digitales.

Para entender cabalmente el funcionamiento del esquema de seguridad proyectado resultará conveniente reservar un capítulo para analizar el sistema de publicación elegido. Especialmente en lo relacionado con la verificación de autenticidad de los datos publicados, en este caso particular, de los certificados digitales.

3.1. DNS.

DNS (Domain Name System) es el sistema utilizado en internet para asociar a nombres inteligibles para las personas con identificadores binarios de los equipos conectados a la red (direcciones IP).

Conceptualmente se sostiene sobre una base de datos distribuida y organizada jerárquicamente. El modelo define dominios de nombres que a la vez pueden irse dividiendo en subdominios, respetando una estructura en forma de árbol invertido, en donde el nodo superior es el denominado root.

La información es manejada a través de entradas en la base distribuida conocidas como RR (Resource Record). Los RR pueden soportar distintos tipos de datos, (direcciones IPv4/6, alias de nombres de dominio, servidores de intercambio de correo, texto, etc).

3.2. Extensiones de seguridad.

En el año 2005, a través de varios RFC's, entre los que se pueden destacar el 4033 (DNS Security Introduction and Requirements) [12], el 4034 (Resource Records for the DNS Security Extensions) [13] y el 4035 [14] (Protocol Modifications for the DNS Security Extensions), fueron propuestas varias extensiones de seguridad para el sistema DNS (Domain Name

System), las que conjuntamente se dieron a conocer como DNSSEC (DNS Security Extensions). En general resuelven diferentes vulnerabilidades detectadas en el diseño de DNS, relacionadas especialmente con debilidades en la autenticación e integridad de la información manejada. Además existe una especificación en particular, referida a través de la RFC 4398 [15], que trata el almacenamiento y la publicación de claves públicas y certificados digitales, como si de nombres de dominio se tratara.

No obstante, es importante señalar que la puesta en producción de esas extensiones a escala global constituye un desafío complejo que pone en juego cuestiones no fáciles de resolver. Principalmente se está hablando de ciertas incompatibilidades que podrían aparecer en los dispositivos de red debido al incremento no previsto del tamaño de los paquetes de respuestas devueltos [16]. El estándar DNS especifica un límite de 512 bytes para los mensajes enviados sobre UDP (el protocolo comúnmente usado en este servicio), RFC 2671 [17]. Se estima que no todos los dispositivos de red distribuidos actualmente por internet soportan tales cambios para ese estándar, y muchos de ellos terminarán por descartar esas respuestas. Esta situación es la que está demorando su implementación. De todas maneras, éste estándar sigue siendo útil para establecer las bases de una solución que provea un sistema de registro y publicación de certificados digitales, independiente del servicio de DNS (teniendo en cuenta la insalvable demora que supone la implementación de DNSSEC en internet). Por esta razón, en un próximo punto se describirá cómo se establece y verifica en DNSSEC una cadena de confianza para autenticar sus registros, con la idea de utilizar un mecanismo similar en un servicio alternativo.

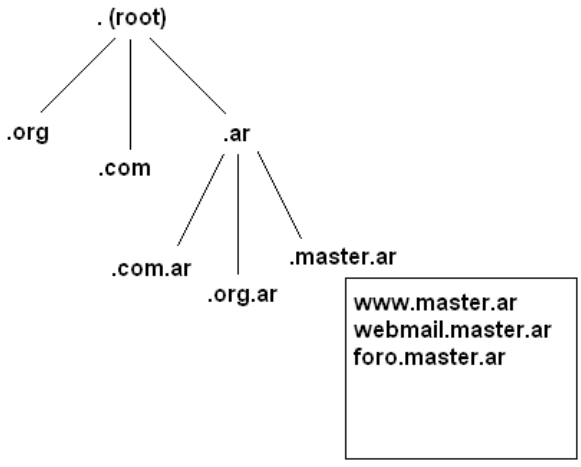
Uno de los principales objetivos de DNSSEC es la de impedir cualquier tipo de redireccionamiento no autorizado hacia un sitio malicioso basándose en la seguridad que brinda una cadena de confianza establecida desde la root zone (.). Para ello se ha introducido una nueva serie de tipos de registros (rfc 4034 [18]):

- DNS Public Key (DNSKEY): para almacenar las claves públicas utilizadas en la firma de registros.
- Resource Record Signature (RRSIG): para las firmas de los registros.
- Next Secure (NSEC): registros empleados para descartar nombres falsos de un dominio dado. Actualmente se recomienda su reemplazo por un tipo mejorado denominado NSEC3.
- Delegation Signer (DS): registros utilizados durante el proceso de autenticación (permite construir una cadena de confianza entre una zona padre y su/s zona/s hija/s). Básicamente es un hash de la clave pública de una zona hija.

3.3. Resolución de nombres bajo DNSSEC.

A continuación se describirá con un modelo de ejemplo cómo se construye la cadena de confianza que permite la validación de información publicada en un servicio de DNS con las extensiones de seguridad DNSSEC.

A partir del siguiente árbol de DNS:



se detallará como se procede con la validación de la ip asignada al nombre de dominio: webmail.master.ar. El mismo procedimiento es aplicable a cualquier otro tipo de información publicada, como los certificados digitales.

En este ejemplo las zonas vinculadas por la cadena de confianza son tres: . (root), .ar y .master.ar.

En DNSSEC, todos los registros (resource records o RR) de una zona deben estar firmados, publicándose el registro conjuntamente con su firma (registro RRSIG). Para ello, cada zona cuenta con dos pares de claves privadas/públicas:

- Key Signing Key (KSK): para firmar los registros de sus propias claves públicas (DNSKEY).
- Zone Signing Key (ZSK): para firmar los registros de la zona a excepción de los DNSKEY.

Cada zona exhibe sus claves públicas KSK y ZSK a través de los registros DNSKEY, con sus correspondientes firmas (registros RRSIG). A esto hay que sumar el registro DS, que es un hash de la clave pública KSK de la zona hija, que como todo registro debe estar firmado con la ZSK (la clave privada ZSK). Por razones de seguridad se recomienda cada cierto período de tiempo regenerar ambos pares de claves privadas/públicas.

En realidad, es posible utilizar un solo par de claves para firmar todos los registros. La ventaja de tener dos pares de claves es que sólo la regeneración de la clave KSK requerirá modificaciones en la zona padre (debido a la actualización del registro DS). En cambio, la regeneración de la clave ZSK (utilizada para firmar todos los recursos, excepto los DNSKEY) no requiere ser comunicado a los administradores de la zona padre. Esto favorece una gestión segura ya que permite manejar tiempos de expiración menores para las claves ZSK.

Volviendo al ejemplo: a continuación se exhibirán los registros de las tres zonas. Valores y hashes de los registros fueron modificados para simplificar la lectura, al igual que se omitieron aquellos registros que no son relevantes para la comprensión del caso.

Zona . (root):

```
.               10800  IN SOA dns. admin. (
                              1          ; serial
                              10800      ; refresh (3 hours)
                              3600       ; retry (1 hour)
                              604800     ; expire (1 week)
                              3600       ; minimum (1 hour)
                              )
...
                10800  DNSKEY 256 3 5 (
                              yzKZrZuANMScWoAh5gicbxxYW43TRnzhjUKH
                              7xStC48H35IG12wbuTrYb8oiQmdLKFGD
                              ) ; key id = 10001
                10800  DNSKEY 257 3 5 (
                              IJw1BuMJYaEGdbLnU2HQAa8VPudXRop8iwVW
                              joL46cJZp7jC5YSs8d71TUCGpi8fQZQr
                              ) ; key id = 10002
                10800  RRSIG  DNSKEY 5 2 10800 20120831161745 (
                              20120811161745 10002 .
                              FR0mUR1xAeXNG5FIa2Ep4r2UfRRhUb7zEKJY
                              8aVKJpqJ+a+XPZdM1fAKVngA+I4= )
                10800  RRSIG  DNSKEY 5 2 10800 20120831161745 (
                              20120811161745 10001 .
                              H3k74j9LIJmafeeqviSGvWF3i3oPuKY3kB8R
                              HAd3I+Aga0INObT0py4QPFiG7Y8= )
...
ar.             10800  IN DS   10004 7 1 43AE17BA8493CC0C4ABA580906
                10800  RRSIG  DS 7 2 10800 20120831161745 (
                              20120811161745 10001 .
                              +uM4SQxpQQykGnEcm2R0JdxTcjFDsGReUCvA
                              LbxOvNuizh1DH1+KvLHEDURY2eY= )
...
```

Zona .ar:

```
ar.             10800  IN SOA dns.ar. admin.ar. (
                              1          ; serial
                              10800      ; refresh (3 hours)
                              3600       ; retry (1 hour)
                              604800     ; expire (1 week)
                              3600       ; minimum (1 hour)
                              )
...
                10800  DNSKEY 256 3 5 (
                              zTCegwPJEFq4aBwPj/dItDw4cbTA5ku5fOuf
                              7xStC48H35IG12wbuTrYb8oiQmdLKFGD
                              ) ; key id = 10003
                10800  DNSKEY 257 3 5 (
                              8UXIwJGh8tI/R95Xm1E6uNSzRh9CGp+CZYhR
                              joL46cJZp7jC5YSs8d71TUCGpi8fQZQr
                              ) ; key id = 10004
                10800  RRSIG  DNSKEY 5 2 10800 20120831161745 (
                              20120811161745 10004 ar.
                              k3dC8vcgAC00Uo74Z864p19ch3JFijCEmPN1
                              8aVKJpqJ+a+XPZdM1fAKVngA+I4= )
                10800  RRSIG  DNSKEY 5 2 10800 20120831161745 (
                              20120811161745 10003 ar.
                              8eArJmydXD73Vb2shFT3g9sHGB93/1KdKNX2
                              HAd3I+Aga0INObT0py4QPFiG7Y8= )
...
master.ar.      10800  IN DS   10006 7 1 C0C4ABA5809064 3AE17BA8493C
                10800  RRSIG  DS 7 2 10800 20120831161745 (
                              20120811161745 10003 ar.
                              ztvzoWaw7muObB7oHyFsgC2U9SaXz/iQ1w5a
                              LbxOvNuizh1DH1+KvLHEDURY2eY= )
...
```

Zona .master.ar:

```
master.ar.          10800  IN SOA dns.master.ar. admin.master.ar. (
                                  1          ; serial
                                  10800      ; refresh (3 hours)
                                  3600       ; retry (1 hour)
                                  604800     ; expire (1 week)
                                  3600       ; minimum (1 hour)
                                  )
...
                    10800  DNSKEY 256 3 5 (
                                  AwEAAd1ExLb4AYJjk5ktnImpxHakDg03+v9q
                                  7xStC48H35IG12wbuTrYb8oiQmdLKFGD
                                  ) ; key id = 10005
                    10800  DNSKEY 257 3 5 (
                                  AwEAAdEXT4yPRvuv877b56FMut/1fXJZ8sZm
                                  joL46cJZp7jC5YSs8d71TUCGpi8fQZQr
                                  ) ; key id = 10006
                    10800  RRSIG  DNSKEY 5 2 10800 20120831161745 (
                                  20120811161745 10006 master.ar.
                                  WnWCfU3vBSj8mSRCYg/rxJ6q97YtJtgjrhNF
                                  8aVKJpqJ+a+XPZdM1fAKVngA+I4= )
                    10800  RRSIG  DNSKEY 5 2 10800 20120831161745 (
                                  20120811161745 10005 master.ar.
                                  xbExVvCL9yAwsqVJgPABPSNrspAVZ61v1A18
                                  HAd3I+Aga0INObT0py4QPFiG7Y8= )
...
webmail.master.ar.  10800  IN A    10.0.0.11
                    10800  RRSIG  A 5 3 10800 20120831161745 (
                                  20120811161745 10005 master.ar.
                                  jFU+tgwv9EZPoeNCH7Jy6opMPQEqajWeswTF
                                  LbxOvNuizh1DH1+KvLHEDURY2eY= )
...
```

Las KSK y ZSK de la zona . (root) son llamadas “trust anchor” y son confiables por definición (no necesitan ser verificadas). Todo aquello que esté firmado por alguna de las privadas de estas claves no necesita verificación. Desde luego, para obtener las claves públicas de las KSK y ZSK de la zona padre deberán tomarse todos los recaudos posibles, a través de un canal seguro. Los administradores de algunas zonas DNSSEC tienen publicados sus trust anchors en sitios web seguros.

Las figuras de la página anterior permiten ver que:

I. En la zona master.ar se hallan publicados:

- El registro A (10.0.0.11) del host webmail.master.ar y su firma. La firma fue hecha con la ZSK privada de esa zona (id=10005).
- Las ZSK y KSK públicas de la zona master.ar (id=10005 y id=10006 respectivamente) y sus firmas. Las firmas fueron realizadas con la KSK privada de la misma zona (id=10006).

II. En la zona .ar se encuentran publicados:

- Un hash (registro DS) de la KSK pública de la zona master.ar (id=10006) y su firma. Esta última fue hecha con la ZSK privada de la zona .ar (id=10003).
- Las ZSK y KSK públicas de la zona .ar (id=10003 y id=10004 respectivamente) y sus firmas. Las firmas fueron realizadas con la KSK privada de la misma zona (id=10004).

III. En la zona . (root) se han publicado:

- Un hash (registro DS) de la KSK pública de la zona master.ar (id=10004) y su firma. Esta última fue hecha con la ZSK privada de la zona . (root) (id=10001).
- Las ZSK y KSK públicas de la zona .ar (id=10001 y id=10002 respectivamente) y sus firmas. Las firmas fueron realizadas con la KSK privada de la misma zona (id=10002).

Teniendo presente todo lo anterior, verificar la autenticidad del registro A (address) del host webmail.master.ar es posible gracias a la cadena de confianza establecida desde la zona root. A saber:

1. La ZSK pública de la zona root (id=10001) es válida por definición. Al igual que la KSK pública (id=10002).
2. Con la ZSK pública de la zona root (id=10001) se verifica la validez del hash (registro DS) de la KSK pública de la zona .ar (id=10004). Porque este hash está firmado con la ZSK privada de la zona root.
3. Con este último hash se verifica la validez de la KSK pública de la zona .ar (id=10004).
4. Con la KSK pública de la zona .ar (id=10004) se verifica la validez de la ZSK pública de la zona .ar (id=10003).
5. Con la ZSK pública de la zona .ar (id=10003) se verifica la validez del hash (registro DS) de la KSK pública de la zona master.ar (id=10006).
6. Con este hash se verifica la validez de la KSK pública de la zona master.ar (id=10006).
7. Con la KSK pública de la zona master.ar (id=10006) se verifica la validez de la ZSK pública de la zona master.ar (id=10005).
8. Finalmente, con la ZSK pública de la zona master.ar (id=10005) se verifica la validez del registro A (10.0.0.11) del host webmail.master.ar.

De esta forma, siguiendo la cadena de confianza se puede validar la autenticidad de cada tipo de registro (dirección, servidor de nombre, registro de intercambio de correo, certificado digital, etc) de la zona master.ar.

Se puede apreciar fácilmente cuán decisivo resulta una adecuada gestión de claves en un modelo DNSSEC ya que cualquier descuido (expiración, demora en la publicación, incorrecta comunicación de sus cambios, etc) puede dejar sitios inaccesibles. Los resolvers, frente a consultas dirigidas a dominios DNSSEC, por default directamente descartan las respuestas recibidas cuando no pueden validar la autenticidad del registro solicitado.

También es posible establecer zonas seguras, que trabajen con DNSSEC, aún cuando sus zonas padres no lo sean. En este caso las trusts anchors son administradas precisamente por esas mismas zonas hijas. Esta conllevaría la necesidad de poder acceder en forma segura a esa trust anchors, situación que se torna más compleja a medida que aparecen otras zonas seguras con padres no seguras. Un resolver tendría que tener un repositorio con todas esas trust anchors lo que redundaría en una tarea difícil de cumplir. Para superar tal escollo existe un mecanismo conocido como “lookaside validation”. El mismo define un dominio DLV (DNSSEC Lookaside Validation) en donde han de publicarse las trust anchors mencionadas. Entonces lo único que habría que hacer es acceder de forma segura a la trust anchor de ese dominio DLV. Obviamente, las zonas seguras que carecen de una zona padre segura deben hacer llegar su trust anchor a los administradores del dominio DLV por medio de un canal altamente confiable.

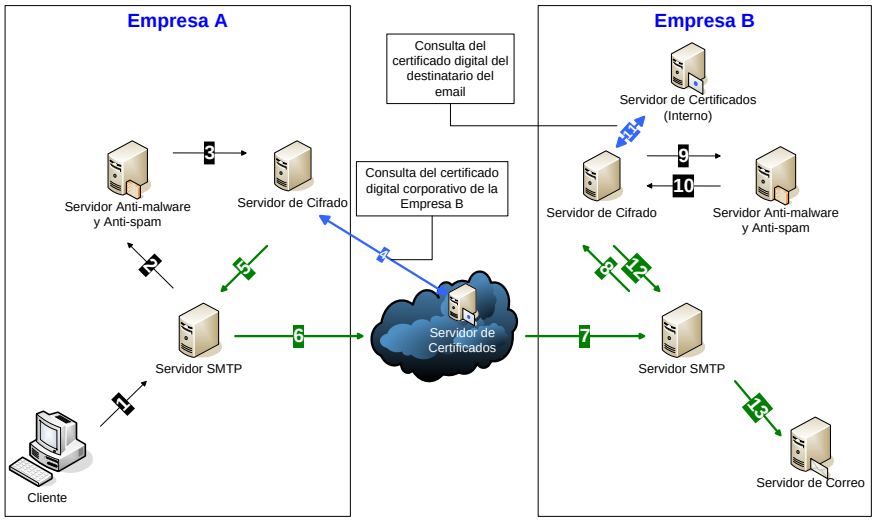
Una vez aclarado los conceptos principales es el momento de presentar el esquema de seguridad propuesto.

4. Esquema de seguridad.

4.1. Introducción.

Como se ha adelantado, el principal objetivo planteado es el de proveer seguridad al correo electrónico protegiendo su confidencialidad, sin que ello implique una intervención especial o manejo de conocimiento extra por parte de los usuarios interesados. A fin de brindar el deseado nivel de seguridad se ha optado por instrumentar la solución a través de certificados digitales basados en una arquitectura PKI. Con ello se busca salvaguardar los emails de la lectura no autorizada de aquellos que tengan o logren el acceso lógico y/o físico a los mismos. Al actuar de esta forma se protege al correo electrónico en tránsito y al que se encuentra almacenado en las casillas, limitando de esta manera el accionar de hackers y de los mismos administradores del servicio de correo.

En esencia, el esquema plantea la introducción al conjunto de servicios de red que comúnmente intervienen e interactúan en el despacho de un correo electrónico, uno de publicación de certificados digitales y uno de cifrado (a partir de esos certificados). Una visión general del funcionamiento del sistema durante el envío de un email es el siguiente:



Se puede apreciar a grandes rasgos la protección provista a un correo electrónico viajando entre dos puntos (desde la empresa A hasta la B) a través de internet. Es posible ver también que no sólo entran en juego los certificados digitales de los usuarios destinatarios sino también algunos identificados como corporativos, emitidos para las empresas que proveen las casillas de correo. Para mejor comprensión no han sido incluidos la totalidad de los dispositivos de red y servidores que suelen participar en el proceso.

Las flechas numeradas en verde indican que el email viaja cifrado. Las dobles flechas azules indican las consultas y respuestas realizadas para obtener los certificados digitales. Como se ve en el gráfico, los emails van cifrados con el certificado digital corporativo de la empresa B desde la etapa 5 a la 8 y con el certificado del destinatario a partir de la 12. El primer cifrado lo hace la empresa A y el segundo la B. La utilización de certificados digitales corporativos permite la ejecución de tareas de detección y eliminación de malware y spam. En el caso de emails dirigidos a usuarios dentro de una misma empresa la tarea se ve claramente simplificada al no necesitarse el certificado corporativo (ver más adelante la descripción del funcionamiento en detalle).

Otro punto interesante a considerar es que, siguiendo el ejemplo dado, el servidor de cifrado de la empresa A bien podría firmar los emails salientes con un certificado corporativo (una especie de firma corporativa oficial).

Antes de continuar, cabe una aclaración. La denominación de “servidor de cifrado” alude solo a su función principal, en realidad dicho servidor lleva a cabo otras tareas adicionales. Debe poder realizar las consultas necesarias a fin de obtener los certificados electrónicos y, además, es imprescindible que tenga la capacidad de verificar la validez de los mismos.

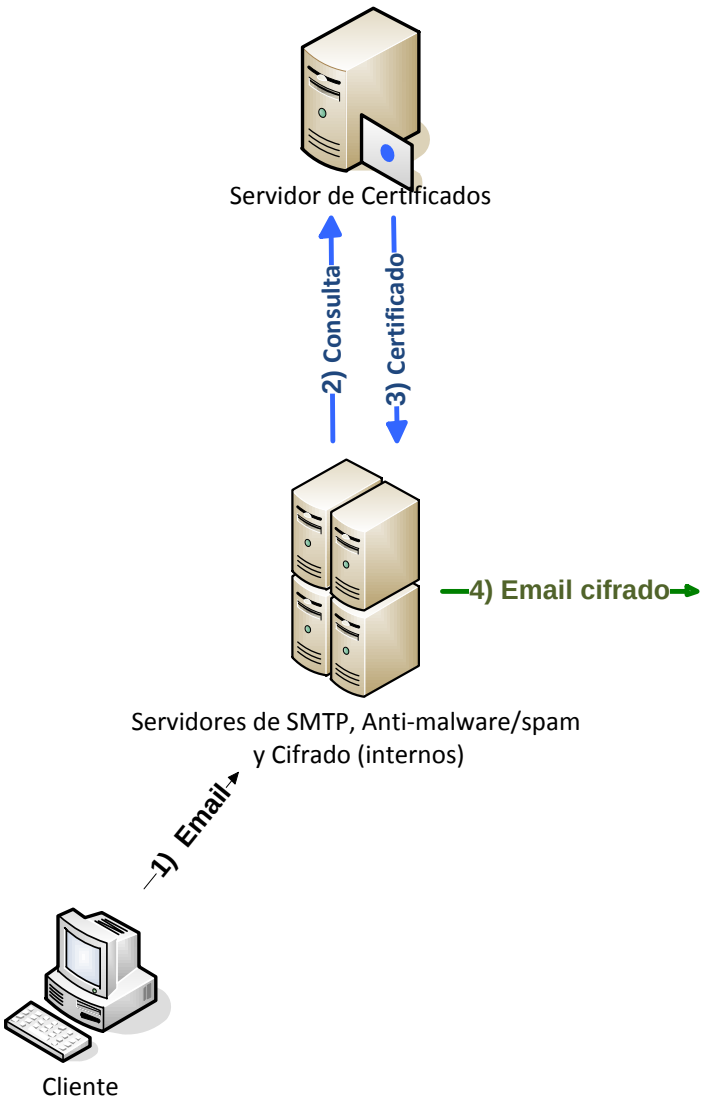
4.2. Asegurando la confidencialidad.

El esquema de seguridad supone la coordinación de diferentes servicios por lo que su acabada comprensión requiere un análisis detallado, teniendo en cuenta las distintas etapas que atraviesa la correspondencia digital durante su existencia.

4.2.1. Emisión.

Una vez emitido desde el correspondiente MUA (Mail User Agent) el correo electrónico ha de ser cifrado en el servidor de correo saliente de la empresa. De existir una etapa de escaneado anti-malware/spam, lógicamente ésta deberá ser ejecutada en un paso previo. Obviamente la ejecución de esta operación de cifrado puede ser omitida si ya fue hecho por el propio usuario remitente a través de su cliente de correo.

En esta instancia se debe decidir qué certificado digital utilizar para proteger la confidencialidad. Si el destino es una cuenta interna, el certificado es el del usuario destinatario, en cambio si es externo se utiliza el certificado corporativo de la empresa del destinatario. En realidad ambas situaciones representan instancias distintas en el envío de correo electrónico, en la primera se está hablando de la etapa final (despacho) mientras que en la segunda de la fase inicial. Si bien parece, a primera vista, más lógico utilizar siempre el certificado digital del usuario receptor, esto puede presentar ciertos riesgos de seguridad. Concretamente, en el caso de email con destinatarios externos, el cifrado de un email impedirá su escaneo por parte de las programas anti-malware/spam de la empresa destino (ya que esos agentes no contarán con la clave privada necesaria para proceder a su descifrado). Esta medida busca dificultar la propagación de malware y spam. De esta manera una empresa solo necesita poner a disposición pública, en internet, su certificado digital corporativo y no los de sus usuarios. Ver gráfico a continuación:

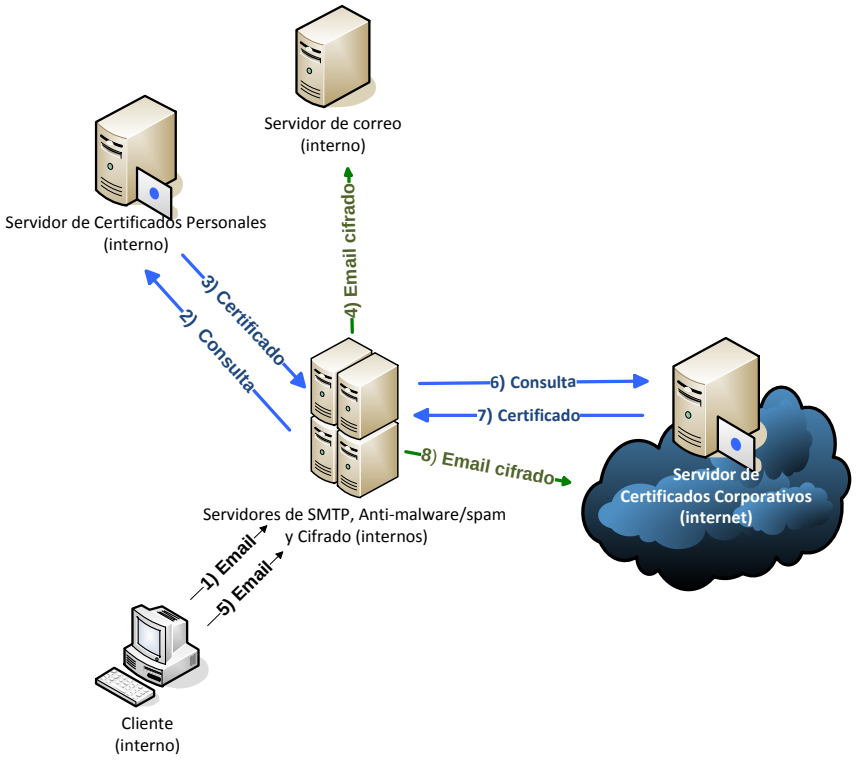


1. El email es enviado al servidor SMTP saliente.
2. El servidor de cifrado consulta por el correspondiente certificado digital.
3. El servidor de certificados devuelve el certificado pedido.
4. El email es cifrado y luego despachado.

Evidentemente la situación descripta plantea la necesidad de asegurar la disponibilidad de los certificados digitales involucrados, ya sean personales o corporativos. Dicho servicio de publicación de certificados puede ser cubierto por el sistema de nombres de dominio (DNS) con extensiones de seguridad (DNSSEC).

DNSSEC permite la publicación de certificados digitales de manera confiable. Pero dada la dificultad existente para su implementación en el ámbito de internet resulta también factible utilizar algún servicio similar, como el de directorio LDAP, para cubrir tal necesidad. Previendo esta situación más adelante se dedicarán unas líneas al servicio de publicación de certificados (ver capítulo 5). En una red interna el sistema de publicación podría ser brindado por un sistema DNSSEC, ya que es de suponer que los dispositivos empleados se encuentran bajo el completo control de sus administradores.

La publicación independiente de los certificados digitales personales y corporativos favorece el planteo de un escenario con dos servicios bien diferenciados. Uno en la red interna para los certificados digitales personales (despacho local) y otro en internet para los certificados digitales corporativos (envíos externos). En este modelo, resulta claro que el requerimiento de publicar hacia internet solo es necesario para los certificados corporativos. Es de prever que en una empresa el volumen de certificados digitales personales siempre será mucho mayor que el de los corporativos. Por este motivo, el hecho de disponer de la mayoría de los certificados en un directorio interno facilita las tareas de gestión de los mismos, mejorando especialmente los tiempos de altas y bajas y de propagación de los cambios (si el servicio se sostuviera sincronizado en varios servidores). Probablemente la publicación externa del certificado digital corporativo no signifique muchos movimientos (de altas y bajas), el compromiso de una clave privada alojada en la sala cofre del área de informática es poco factible. A esos beneficios hay que sumar que las consultas relacionadas con despachos internos de emails demorarán poco tiempo (por ser locales) y a su vez el volumen de consultas dirigidas a internet será mucho menor. En el próximo gráfico se describe el envío de dos emails, uno con destino interno y el otro con destino externo:



1-2-3-4) Destino interno.
5-6-7-8) Destino externo.

Destino interno.	Destino externo.
1) El email es enviado al servidor SMTP saliente. 2) El servidor de cifrado consulta por el certificado digital personal correspondiente (en la red local). 3) El servidor de certificados devuelve el certificado pedido. 4) El email es cifrado y luego despachado al destino interno (local).	5) El email es enviado al servidor SMTP saliente. 6) El servidor de cifrado consulta por el certificado digital corporativo correspondiente (internet). 7) El servidor de certificados devuelve el certificado pedido. 8) El email es cifrado y luego despachado al destino externo.

Recordar que en este esquema el cifrado no es llevado a cabo por el cliente de correo (MUA) del usuario sino por el servidor de cifrado. El cifrado es transparente para ambos usuarios (el emisor y el destinatario), ninguno de ellos necesita intervenir. El destinatario no tiene que preocuparse por enviarle el certificado digital al emisor, ni este último por tratar de conseguirlo, el mismo servidor de cifrado se encarga del manejo de los mismos . Tampoco requiere una interacción adicional entre el usuario y el cliente de correo. El servidor de cifrado es el componente clave, actor

principal, que interactúa con los servidores de SMTP, publicación de certificados y anti-malware/spam. En el capítulo 6 se describirán las características que debe cumplir este servicio. Obviamente, el servidor de cifrado deja pasar los emails sin procesar si no puede acceder a los certificados necesarios.

4.2.2. Tránsito por internet.

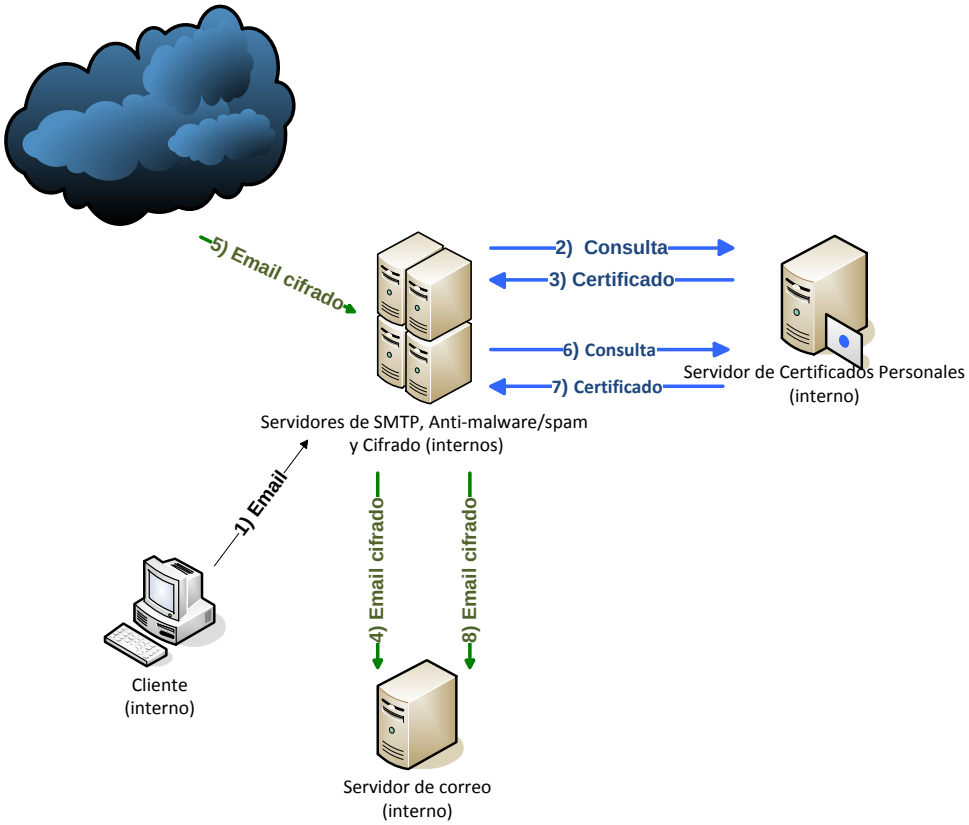
Durante esta etapa la confidencialidad del correo electrónico se encuentra protegida por el cifrado realizado oportunamente con el certificado digital corporativo de la empresa del usuario destinatario. Esta medida de seguridad obstaculiza aquellas posibles acciones destinadas a analizar el contenido del mensaje durante las transferencias entre los servidores SMTP intervinientes.

4.2.3. Recepción / despacho.

Si el email entrante proviene del exterior (internet) y está cifrado con el certificado digital corporativo, éste debe ser descifrado con la clave pública correspondiente. Esta operación resulta necesaria para aplicar las tareas de escaneado tendientes a disminuir las amenazas originadas por la presencia de malware y limitar la difusión de spam. En el caso de arribar desde la red interna esta operación puede considerarse como opcional.

Finalizado el proceso de escaneo, el email se encuentra en condiciones de ser despachado a la casilla del destinatario. Pero antes debe ser cifrado con el certificado digital del respectivo usuario (a menos que el remitente del mismo lo haya cifrado en el momento de la emisión). Con miras a la automatización de esta operación, sin la intervención del usuario destinatario, aquí también resulta necesaria la presencia de un servicio de publicación de certificados digitales, este aspecto ya fue tratado en la etapa de emisión (ver punto 4.2.1). En este caso, al tratarse de una red interna es perfectamente posible la implementación de un servicio de DNSSEC. A

continuación, se puede verificar el tratamiento que reciben dos emails entrantes (uno originado internamente y otro externamente):



1-2-3-4) Origen interno.
5-6-7-8) Origen externo.

Origen interno.	Origen externo.
1) El email es recibido de una estación local (no cifrado). 2) El servidor de cifrado consulta por el certificado digital personal correspondiente. 3) El servidor de certificados devuelve el certificado pedido. 4) El email es cifrado y luego despachado al servidor de correo interno.	5) El email es recibido desde internet y descifrado con la clave privada ad-hoc de la empresa. 6) El servidor de cifrado consulta por el certificado digital personal correspondiente. 7) El servidor de certificados devuelve el certificado pedido. 8) El email es cifrado y luego despachado al servidor de correo interno.

Como en la etapa de emisión, en esta fase también se pretende que el usuario destinatario no tenga que intervenir activamente comunicando previamente su certificado digital al emisor del correo electrónico. Aquí también el servidor de cifrado es la clave para que todo el sistema funcione correcta y exitosamente.

4.2.4. Respaldo.

Al quedar el email cifrado en la casilla del usuario, éste y sus posteriores copias permanecerán en esa condición en donde sea que se encuentren, incluyendo los subsiguientes backups que sean ejecutados.

4.3. Firma corporativa.

Un beneficio extra que este esquema de seguridad es capaz de brindar, es el de implementar una firma electrónica corporativa. Esto permitiría al destinatario validar el origen corporativo de un email, esto es, poder verificar que el email provino de la empresa que administra la cuenta del usuario remitente. Esto elevaría el nivel de seguridad del modelo.

No obstante cabe destacar que, según la Ley 25.506 [19] de la legislación argentina, la firma digital, y no la electrónica, es la que tiene el mismo efecto jurídico que una manuscrita (artículo 3º). La firma electrónica carece "de alguno de los requisitos legales para ser considerada firma digital" (artículo 5º). En su artículo 9º se especifican las condiciones que ha de cumplir una firma digital para que sea considerada válida:

> "a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante;
> b) Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente;
> c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado."

Un hecho interesante, que puede llegar a generar confusiones, es que en las legislaciones de otros países el mismo concepto de firma digital puede ser encontrado bajo una denominación distinta. En la legislación española, por

ejemplo, la Ley 59/2003 [20] se refiere a ella como “firma electrónica reconocida”.

Finalmente, la firma corporativa, ya sea digital o solo electrónica, podría ser efectuada por el propio servidor de cifrado (sobre el correo electrónico cuyo destinatario no fuera local, sino externo). La operación se completaría con alguna clave privada electrónica corporativa generada para tal fin, antes de proceder con el cifrado del email. Por otro lado, el uso de la clave privada electrónica asociada al certificado electrónico corporativo, que se encuentra publicado y accesible desde internet, facilitaría al destinatario la tarea de validación de la firma.

Observación: Durante los ensayos de laboratorio se incluyeron pruebas sobre esta funcionalidad. Si bien no se presentaron inconvenientes a la hora de su implementación, para aprovecharla habrá que tener en cuenta ciertas consideraciones relacionadas con los clientes de correo (para más apreciaciones ver Capítulo 7).

5. Servicio de publicación de certificados.

Para satisfacer el esquema propuesto los certificados digitales corporativos deben estar disponibles en internet. En cuanto a los certificados personales basta con que puedan ser accedidos internamente, esto es, dentro de una red corporativa.

5.1. Requerimientos.

El servicio de red que soporte la publicación de los certificados debe cumplir con ciertas características técnicas y de seguridad muy particulares. A saber:

- Poder almacenar certificados digitales y sus firmas (ya sea en formato texto o binario).
- Permitir una organización jerárquica de los registros, compatible con FQDN (Fully Qualified Domain Name).
- Ser escalable.
- Estar optimizado para atender consultas.
- Permitir operaciones de altas y bajas (expiración/revocación) de registros.
- Proveer un mecanismo de validación que permita probar la autenticidad de los certificados (por ejemplo, basado en una cadena de confianza).
- Soportar mecanismos de sincronización de los registros entre distintos servidores.

5.2. El servicio.

En base a las requerimientos expuestos en el punto anterior es posible optar dos servicios muy conocidos: DNSSEC y LDAP. La decisión se

fundamenta en que para ambos existen distintas implementaciones que satisfacen perfectamente las condiciones listadas en el punto anterior.

5.2.1. DNSSEC.

En el capítulo 3 se presentaron las características generales de este estándar.

5.2.2. LDAP.

LDAP (Lightweight Directory Access Protocol) es un protocolo que define un servicio de directorio optimizado para lecturas y búsquedas sobre un repositorio de datos dado, implementable de manera distribuida.

LDAP nació como un protocolo "liviano", más sencillo, para comunicarse con el servicio de directorio X.500 como backend, en una arquitectura cliente-servidor, sobre el protocolo TCP/IP. ITU-T X.500 es un servicio de directorio diseñado sobre el modelo OSI lo que implica cierto overhead en los mensajes que lo hacía "pesado". X.509, el estándar para PKI, forma parte del X.500. LDAP no contempla muchas de las operaciones soportadas por X.500 que fueron descartadas por considerarse de poco uso. Vale decir que muchas soluciones LDAP que se pueden conseguir en internet, en realidad no disponen de un X.500 como backend.

La información en un directorio LDAP está estructurada en un modelo de árbol en donde cada nodo constituye una entrada, todas ellas organizadas jerárquicamente. Este modelo es conocido como Directory Information Tree (DIT). Cada una de esas entradas contiene información asociada a una o más clases de datos, donde cada clase reúne una serie de atributos obligatorios y/u opcionales. Cada nodo puede ser unívocamente referenciado vía un identificador conocido como distinguished name (DN). LDAP soporta distintos tipos de datos como atributos, entre los que se pueden incluir claves públicas/privadas, certificados digitales y firmas.

LDAP también puede contemplar mecanismos de autenticación para que un cliente pueda acceder a la información almacenada en forma segura.

La flexibilidad que brinda LDAP para el manejo de datos y su modelo jerárquico (adaptable al utilizado por DNS) permitiría implementar un mecanismo muy similar al utilizado por DNSSEC para efectuar la validación de la autenticidad e integridad de los atributos de sus entradas. Esto convierte al protocolo LDAP en un adecuado candidato para la publicación en internet de certificados digitales. Solo habría que definir un de par de claves públicas/privadas y hashes que cumplan la función de las KSK y ZSK y los registros DS ya definidos para DNSSEC. En otras palabras, una solución alternativa a DNSSEC para el sistema de publicación externo (de certificados corporativos) debe contemplar las siguientes entradas en los servicios LDAP provistos:

- Certificados corporativos y personales y sus firmas.
- Claves KSK y ZSK públicas y sus firmas.
- Hashes de las KSK públicas de las zonas hijas y sus firmas.

Desde luego, para facilitar su gestión, el sistema ha de adaptarse a la actual estructura jerárquica de dominios utilizada por el servicio DNS. Siguiendo la misma línea de pensamiento, también es posible desarrollar una solución parecida al mecanismo de Lookaside Validation (ver Capítulo 3). En la prueba de concepto se empleó una versión simplificada del mismo.

6. Servicio de cifrado.

6.1. Introducción.

El rol desempeñado por el servicio de cifrado en el esquema de seguridad es tan importante como el del resto de los demás participantes. Su ubicación en el modelo funcional lo convierte en el componente que ha de interactuar con todos los demás servicios puestos en juego.

El servicio de cifrado, en primer lugar, debe emplear el protocolo SMTP (Simple Mail Transfer Protocol) para poder recibir y despachar el correo. Además debe estar capacitado para realizar las consultas correspondientes con el objeto de obtener los certificados digitales necesarios para efectuar las operaciones de cifrado. Debe también ser capaz de verificar la validez de los certificados, para esta operación cuenta con la colaboración del servicio de publicación, ya que está basado en el estándar DNSSEC. Por otro lado, es posible que tenga que comunicarse con aplicaciones anti-malware/spam corporativas, aunque por lo general éstos utilizan el protocolo SMTP para establecer conexiones TCP/IP directas con el resto de los servidores SMTP.

Es fácil notar que las tareas asignadas al servicio de cifrado no son complejas, resultan en operaciones básicas, algunas ya ejecutadas por otros servicios existentes. La clave radica en lograr una adecuada y aceitada integración del servicio con el resto de los involucrados. Pueden considerarse distintas configuraciones, por ejemplo, el servicio de cifrado puede estar detrás de un servidor SMTP local o recibir directamente los emails del exterior. Pero lo más importante aquí, es extremar los cuidados a efectos de lograr un diseño, un desarrollo, una implementación, un mantenimiento y una gestión segura, dado el nivel de confidencialidad pretendido. Distintas variantes son posibles en producción.

Este trabajo no pretende introducirse en el terreno de las técnicas y metodologías de programación segura existentes, ello se encuentra fuera del alcance definido para esta tesis.

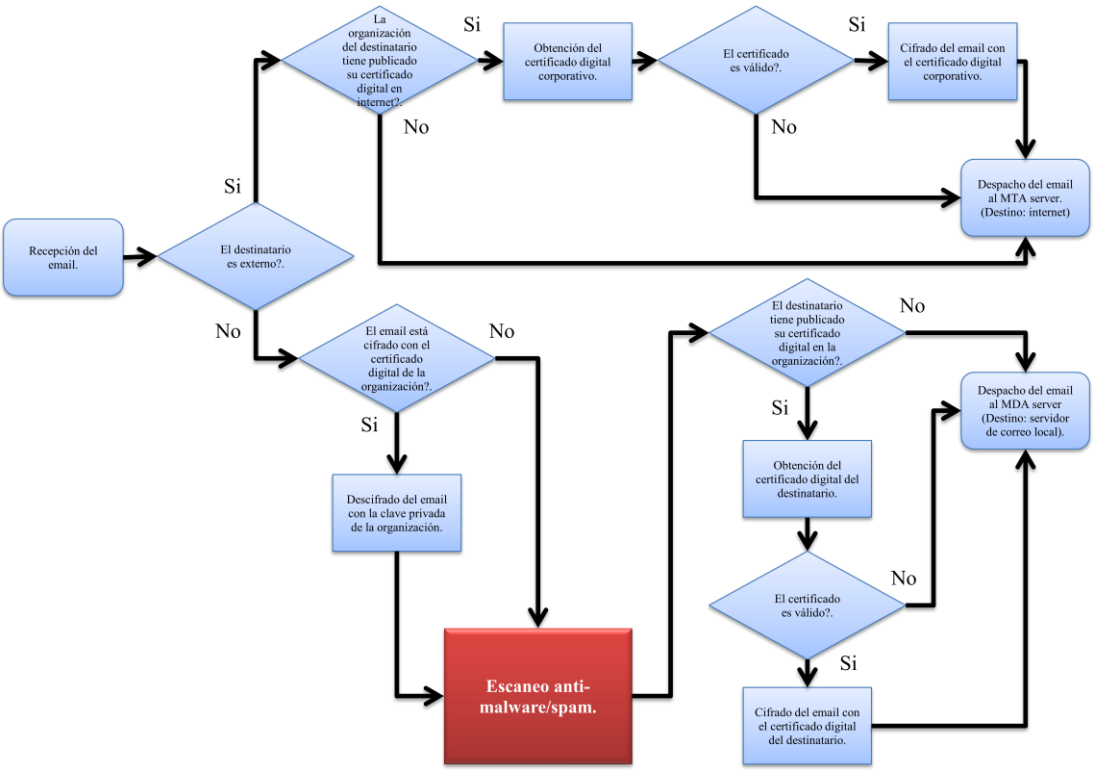
6.2. Requerimientos funcionales.

En vista de lo anteriormente expuesto, un servicio de cifrado deberá poder completar las siguientes funciones:

- Comunicarse con servidores SMTP.
- Realizar consultas (a servidores DNSSEC, eventualmente LDAP) para obtener certificados digitales.
- Verificar la validez de los certificados emitidos dentro de una infraestructura PKI.
- Cifrar/descifrar emails en base a certificados digitales.
- Manejar en forma segura las conexiones con los servicios de SMTP, especialmente cuando se trata de correspondencia no cifrada.
- Operar en forma aislada las conexiones externas (desde/hacia internet) de las locales.

6.3. El servicio.

En el capítulo 4 se ha descripto el procesamiento que recibe el correo electrónico, evidenciando el papel importante que cumple el servicio de cifrado. En base al comportamiento esperado y a los requerimientos mencionados es posible definir completamente el diagrama de flujo del proceso de cifrado llevado a cabo por este servicio. En la próxima página se podrá apreciar el diagrama en detalle.



La fase de escaneo anti-malware/spam se presenta en un color diferente porque la misma no forma parte del servicio, pudiéndose hasta considerar una etapa opcional. En realidad, la idea es que el servicio sea flexible y adaptable a las aplicaciones anti-malware/spam comerciales.

Para llevar a cabo la prueba de concepto se desarrolló un sencillo programa que, junto con aplicaciones open source, permitieron demostrar la factibilidad del esquema de seguridad propuesto.

7. Prueba de concepto.

7.1. Software utilizado.

El software utilizado para la puesta a punto de la prueba de concepto se describe y detalla a continuación:

Software	Descripción general	Características	Versión utilizada
OpenSSL	Open source desarrollado por el OpenSSL Project (http://www.openssl.org). Provee una serie de herramientas que permiten generar implementaciones basadas en SSL (Secure Sockets Layer) v2/3 y TLS (Transport Layer Security) v1. Cuenta con varias librerías criptográficas. El proyecto además creó el módulo OpenSSL FIPS Object Module (compatible con OpenSSL) que posibilita a las implementaciones el uso de criptografía validada según la FIPS 140-2, a través de la OpenSSL API. La FIPS 140-2 es el estándar de seguridad de la NIST (National Institute of Standards and Technology), agencia dependiente del Departamento de Comercio de los Estados Unidos que determina la validación o no de aquellos módulos criptográficos diseñados para ser utilizados por el gobierno norteamericano o las grandes corporaciones.	▪ Es multilplataforma. ▪ Soporta un amplio espectro de algoritmos criptográficos estándares. ▪ Provee un entorno auto-suficiente para la creación y administración de una CA (PKI). ▪ Posee el OpenSSL FIPS Object Module (ver Descripción general).	0.9.8s (4 Jan 2012)
Bind	Open source desarrollado originalmente por la Universidad de California en Berkeley. EEUU. Desde el 2010 es mantenido por el Internet Systems Consortium (http://www.isc.org). Es una implementación del protocolo DNS. La distribución comprende un servidor, librerías para desarrollar resolver's específicos y herramientas para realizar pruebas del servicio.	▪ Es multiplataforma. ▪ Soporta las extensiones de seguridad de DNSSEC.	9.8.1-P1
Cyrus	Open source desarrollado por la Universidad de Carnegie Mellon, en	▪ Es escalable. ▪ Soporta los protocolos IMAP,	2.4.13

	Pensilvania, EEUU (http://www.cyrusimap.org). Es una implementación de un servidor de correo IMAP adaptable a un ambiente corporativo a gran escala.	POP3 y KPOP (Kerberized POP). ▪ Admite el uso de filtros de correo electrónico. ▪ Permite el empleo de listas de control de acceso. ▪ Soporta múltiples conexiones concurrentes de lectura y escritura sobre una misma casilla.	
OpenLDAP	Open source desarrollado por el OpenLDAP Project (http://www.openldap.org). Es una implementación de LDAP que comprende un servidor LDAP, varios clientes, librerías y herramientas relacionadas con el servicio.	▪ Es multiplataforma, modular y escalable. ▪ Permite interactuar con diferentes formatos de repositorios de datos. ▪ Admite reglas de acceso. ▪ Soporta negociaciones SSL/TLS. ▪ Contempla distintos métodos de autenticación. ▪ Posee un mecanismo de replicación del repositorio.	2.4.23

7.2. Software adicional.

También se utilizaron los productos de virtualización VMWare Workstation (http://www.vmware.com) y Xen (http://www.xen.org) para crear y operar varias máquinas virtuales.

7.3. La maqueta.

La construcción de la maqueta requirió de los siguientes componentes de hardware (con detalle del software instalado):

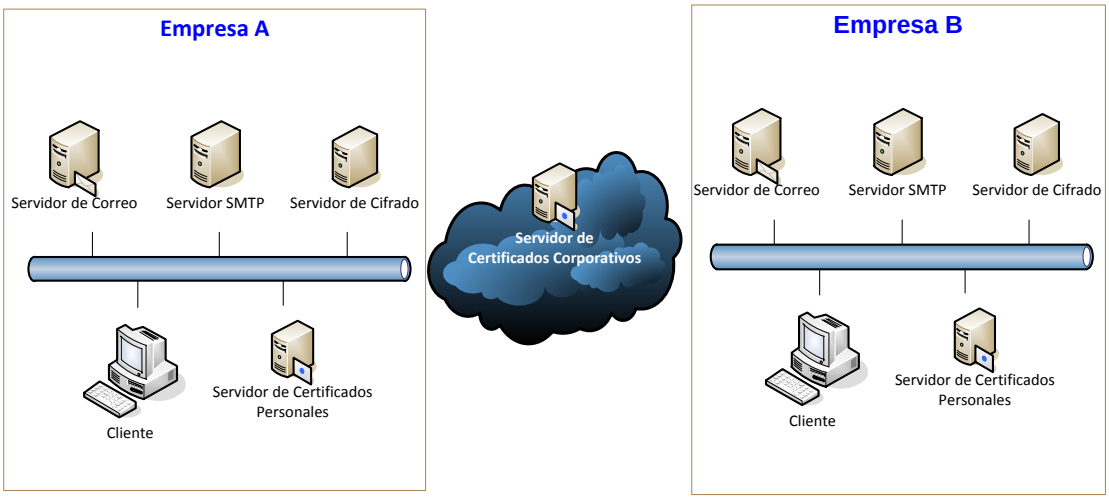
Equipo	Hardware	Sistema Operativo	Servicios
HP d325 Microtower PC (Servidor A)	▪ CPU: AMD Athlon XP 2600+ (1913.20 MHz). ▪ RAM: 256 MB. ▪ Disco rígido: 36 GB.	FreeBSD - Release 7.4	▪ DNSSEC. ▪ Imap.

HP dx5150 Microtower PC (Servidor B)	▪ CPU: AMD Sempron 3200+ (1794.831 MHz). ▪ RAM: 1 GB. ▪ Disco rígido: 36 GB.	Red Hat Enterprise Linux Server – Release 5 (Tikanga)	▪ DNS. ▪ Imap. ▪ PKI.
HP Compaq dc 7600 Convertible Minitower (Servidor C)	▪ CPU: Intel Pentium 4 (3.20 GHz). ▪ RAM: 1 GB. ▪ Disco rígido: 80 GB.	Microsoft Windows XP Profesional - Versión 2002 - (Service Pack 3)	▪ VMware Host,

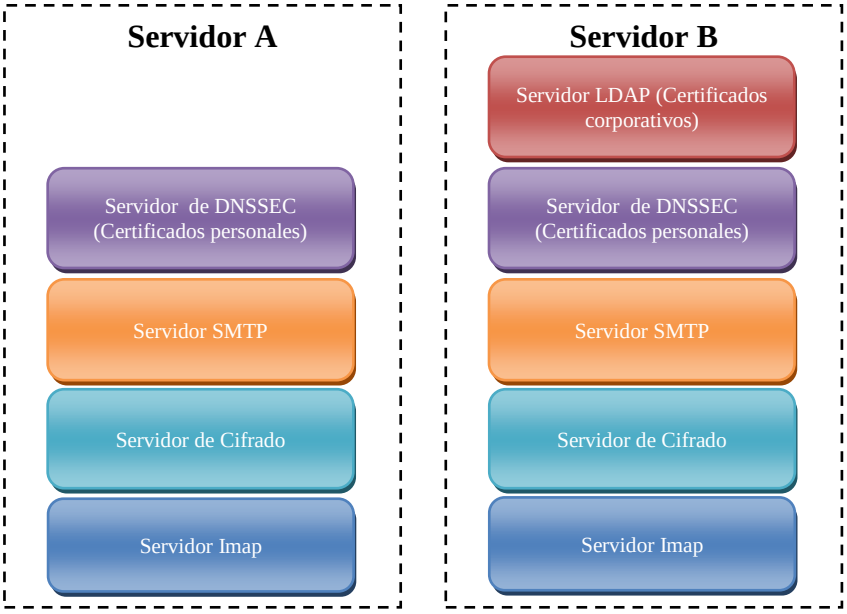
A este listado han de añadirse los dispositivos de red utilizados, que fueron modelos de switches y routers de la firma Cisco (http://www.cisco.com).

Las máquinas de los clientes (Microsoft Windows XP) fueron pc's creadas con el producto VMWare Workstation, instalado en el servidor C. También se utilizó el programa para virtualizar los servidores (A y B) con el fin de llevar a cabo la prueba de concepto en presencia del tutor designado (sobre virtualizadores Xen).

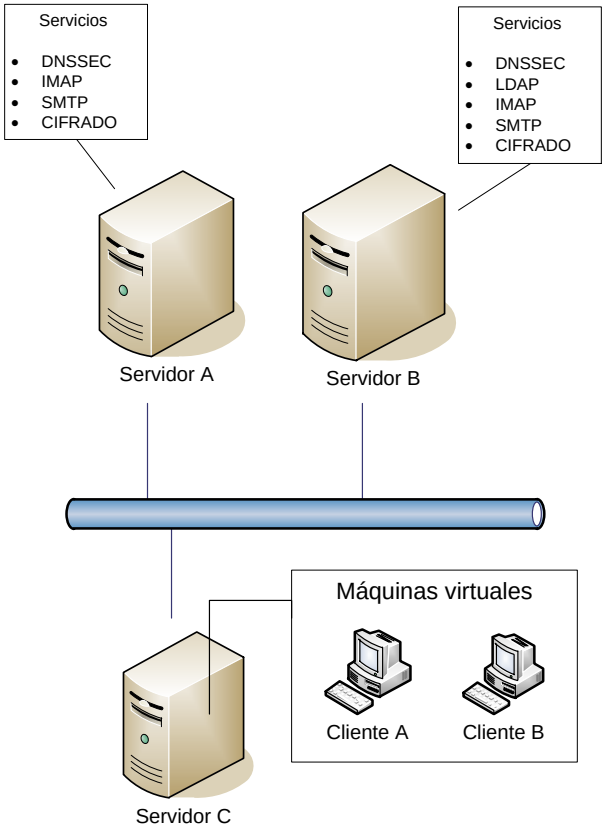
Una visión funcional de la arquitectura de red perseguida es la siguiente:



En la práctica todos los servicios fueron prestados por dos máquinas físicas, identificadas como servidores A y B:



Por razones de practicidad, el servicio de publicación de certificados digitales corporativos fue brindado por el servidor B. En el ensayo de laboratorio se empleó un servidor LDAP a fin de demostrar que el mismo puede constituirse en una alternativa válida para reemplazar un servidor de DNSSEC. El mecanismo elegido para verificar la autenticidad e integridad de las respuestas se basó en el uso claves privadas para firmar los certificados digitales electrónicamente. Finalmente la maqueta terminada fue:



7.4. Resumen de las tareas completadas.

1. Puesta a punto del servidor de DNS (servidores A y B).
   - 1.1 Instalación.
   - 1.2 Configuración general.
   - 1.3 Creación de los archivos de datos de la zona.
   - 1.4 Pruebas de funcionamiento.
   - 1.5 Pase a producción del servicio.
2. Puesta a punto del servidor de correo IMAP (servidores A y B).
   - 2.1 Instalación.
   - 2.2 Configuración general.
   - 2.3 Modificación del sendmail para que despache los correos hacia el servidor IMAP.
   - 2.4 Creación de los usuarios de prueba.
   - 2.5 Pruebas de funcionamiento.
   - 2.6 Pase a producción del servicio.
3. Generación de los certificados digitales (servidores A y B).
   - 3.1 Creación de la CA.
   - 3.2 Generación de las claves privadas y los certificados corporativos.
   - 3.3 Generación de las claves privadas y los certificados de los usuarios de correo de prueba.
4. Puesta a punto del servidor LDAP (servidor B).
   - 4.1 Instalación.
   - 4.2 Configuración general.
   - 4.3 Generación de la clave privada para firmar los certificados digitales a publicar.
   - 4.4 Firma de los certificados corporativos creados en el punto 3.2.
   - 4.5 Creación de las entradas en el directorio a fin de publicar los certificados corporativos y sus correspondientes firmas.

4.6 Copiado de la clave pública del servidor LDAP a los servidores de cifrado. En un ambiente real, esta operación exigirá la implementación de un mecanismo ad-hoc seguro y confiable.

4.7 Pruebas de funcionamiento.

4.8 Puesta en producción del servicio.

5 Puesta a punto del servidor de DNS con las extensiones de seguridad (servidores A y B).

5.2 Configuración específica (opciones dnssec).

5.3 Generación de las claves key-signing y zone-signing.

5.4 Incorporación de la clave pública de uno de los servidores en el archivo de configuración del otro para validación de las respuestas. Esto fue necesario ya que en las pruebas realizadas uno de los servidores DNS actuó como autoritativo de ambas zonas.

5.5 Incorporación de los certificados de los usuarios de prueba emitidos en el punto 3.3 al archivo de datos de la zona.

5.6 Inclusión de las propias claves públicas en el archivo de datos de la zona.

5.7 Firma de la zona y sus registros.

5.8 Pruebas de funcionamiento.

5.9 Puesta en producción del servicio.

6 Configuración de la estación de los usuarios de prueba (estaciones a y b).

6.2 Configuración del cliente de correo.

6.3 Carga del certificado de la propia CA y de las claves privadas correspondientes.

6.4 Pruebas de funcionamiento de todo el sistema.

7 Puesta a punto de los servidores de cifrado (servidores A y B).

7.2 Instalación de los módulos de perl necesarios.

7.3 Desarrollo del script del servicio.

7.4 Configuración específica del servidor y los clientes de correo (para brindar conectividad).

7.5 Configuración general del sistema.

7.6 Pruebas de funcionamiento.

7.7 Puesta en producción del servicio.

En los anexos I y II se pueden encontrar más detalles sobre las tareas ejecutadas.

7.5. Resultado de las pruebas.

Durante las pruebas se realizaron envíos de email entre los dos clientes (A y B), en ambas direcciones. Las mismas permitieron corroborar el correcto funcionamiento del modelo desarrollado en base al esquema de seguridad propuesto.

El modelo cumplió con los objetivos enunciados al principio al:

- Cifrar la correspondencia electrónica dirigida a un destinatario externo sin necesidad de que el remitente intervenga activamente en el proceso. Asegurando la confidencialidad de los emails al utilizar los certificados electrónicos corporativos de la empresa del destinatario (publicados en un repositorio externo).
- Cifrar la correspondencia electrónica dirigida a usuarios locales en forma automática empleando el correspondiente certificado electrónico personal (alojado en un repositorio interno).
- Proteger la confidencialidad del email en todo momento desde su emisión.
- Posibilitar la aplicación de distintas operaciones de escaneo sobre los emails recibidos.

7.5.1. Firma corporativa.

Durante los ensayos también se experimentó con el firmado corporativo automático de los emails, ver capítulo 4 (4.3 Firma corporativa). Si bien se comprobó la factibilidad de esta funcionalidad, habría que tener en

cuenta una serie de consideraciones para que los clientes de correo puedan aprovecharla. El inconveniente en cuestión es que los clientes, al no coincidir el email que figura en el certificado digital utilizado durante el proceso de validación con el del usuario remitente, no terminan por validar la firma completamente. Dependiendo del programa de correo electrónico utilizado, éste indicará tal situación de diferentes formas lo que puede llegar a generar confusiones en el usuario. Una de las soluciones posibles es utilizar alguna de las extensiones de la versión 3 del estándar X.509 de la ITU-T para resolver este problema. Estas extensiones permiten a una autoridad certificante emitir certificados digitales con propósitos más específicos, por ejemplo, el de contemplar firmas electrónicas corporativas. Obviamente, para que todo funcione correctamente los clientes de correo deben estar preparados para manejar y verificar adecuadamente esta nueva extensión.

8. Conclusiones finales.

El desarrollo de la presente tesis permite probar la factibilidad del esquema de seguridad propuesto. El mismo ha sido diseñado para asegurar la confidencialidad de la correspondencia electrónica, teniendo siempre presente al usuario común como principal beneficiario. Pensando en la solución y en los requerimientos de seguridad involucrados se han elegido y empleado tecnologías que han probado contar con aceptables niveles de madurez en sus desarrollos. El resultado final obtenido es alentador para los fines de este trabajo ya que se demostró que es posible llevar a la realidad una implementación basada en el modelo propuesto.

Este esquema definitivamente logra acercar al usuario común los avances en seguridad resultantes de la incorporación de los certificados digitales al uso cotidiano del correo electrónico. Le propone un camino más seguro, y todo ello sin exigirle un esfuerzo extra. Obviamente, las ventajas de este esquema se extienden a todos los usuarios no solo a los menos experimentados en materia de seguridad.

Si bien la idea principal aspira a una implementación a escala global, que como ya se vio no está atado al estándar DNSSEC, también es posible hacerlo en un entorno más reducido, menos ambicioso. Una empresa puede manejar el cifrado interno de la correspondencia entrante y hacer público un certificado corporativo ad-hoc. A medida que otras empresas se sumen y acuerden en cómo brindar el servicio, la concreción de esa idea principal se torna más asequible.

Este trabajo también evidencia que una solución de seguridad a veces se alimenta de otras soluciones (de seguridad) y la clave del éxito radica en poder combinarlos acertadamente.

Y en lo personal, todo el proceso que significó el desarrollo de esta tesis constituyó un verdadero e interesante desafío que, ciertamente, redundó en un crecimiento profesional. Sabemos que el universo de la informática se encuentra en continuo movimiento, será cuestión entonces de estar preparado para poder contribuir a que la seguridad informática evolucione en igual medida.

ANEXO I - Prueba de concepto: El servidor de cifrado.

A. Lenguaje de programación.

El lenguaje de programación utilizado para desarrollar el servidor de cifrado fue Perl (http://www.perl.org). Perl es un lenguaje de programación de propósito general. La elección del lenguaje se centró principalmente en su simpleza y eficiencia. Además existe por parte del tesista cierta familiaridad con el mismo, producto de su utilización para generar scripts diversos en el ámbito profesional. Además, para Perl se han escrito infinidad de funciones de toda clase, generales y específicas, disponibles en librerías organizadas en paquetes (módulos), que han facilitado el desarrollo de la implementación.

B. Módulos utilizados.

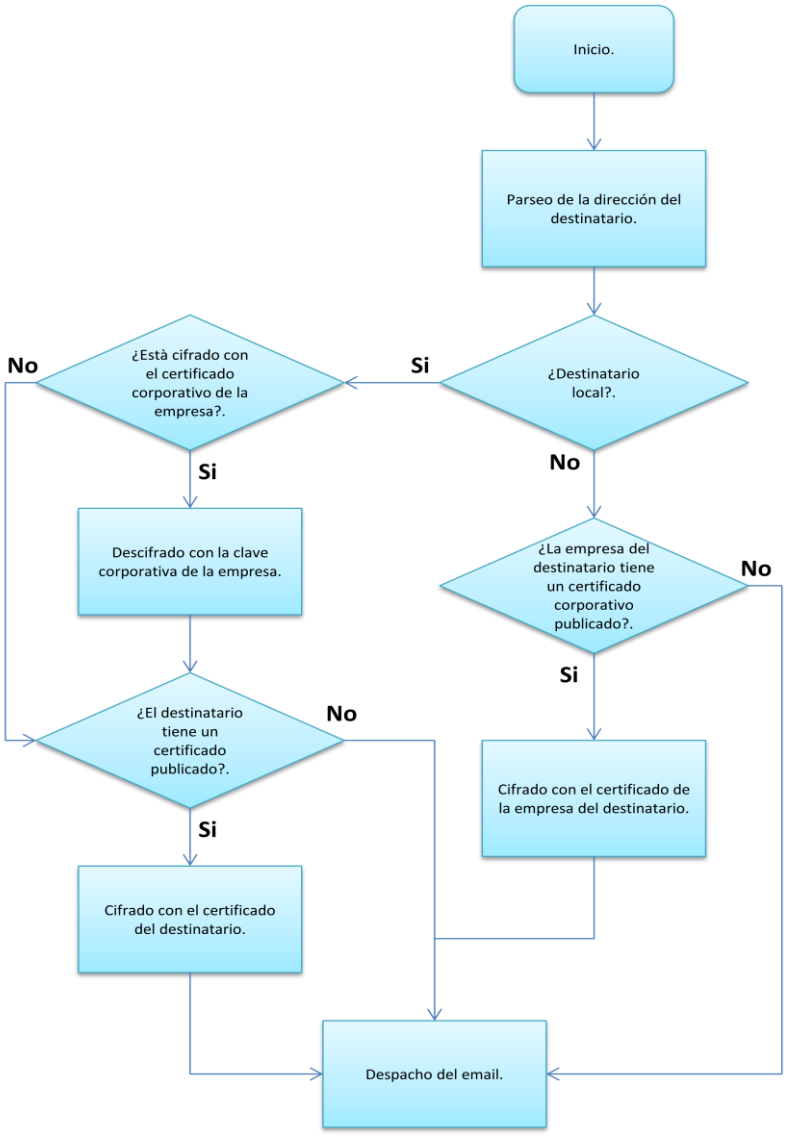
Para el desarrollo del script se utilizaron varios módulos publicados en el sitio CPAN (Comprehensive Perl Archive Network, http://www.cpan.org). Los mismos fueron los siguientes (con indicación de sus versiones):

Módulo	Función	Fuentes (versión)
Net::SMTP::Server	A native Perl SMTP Server implementation for Perl.	SMTP-Server-1.1.tar.gz
Digest::HMAC_MD5	Keyed-Hashing for Message Authentication.	Digest-HMAC-1.03.tar.gz
Digest::SHA	Perl extension for SHA-1/224/256/384/512.	Digest-SHA-5.71.tar.gz
Net::DNS	Perl interface to the Domain Name System.	Net-DNS-0.67.tar.gz
Net::DNS::Codes	Collection of C library DNS codes.	Net-DNS-Codes-0.11.tar.gz
NetAddr::IP::Util	IPv4/6 and 128 bit number utilities.	NetAddr-IP-4.058.tar.gz
Net::DNS::ToolKit	Tools for working with DNS packets.	Net-DNS-ToolKit-0.45.tar.gz

Net::NBsocket	Non-Blocking Sockets.	Net-NBsocket-0.21.tar.gz
Sys::Hostname::FQDN	Get the short or long hostname.	Sys-Hostname-FQDN-0.11.tar.gz
Sys::Sig	Return signal constants for this host.	Sys-Sig-0.04.tar.gz
Net::DNS::Dig	Dig like methods.	Net-DNS-Dig-0.04.tar.gz
Crypt::SMIME	S/MIME message signing, verification, encryption and decryption.	Crypt-SMIME-0.10.tar.gz
Net::LDAP	Lightweight Directory Access Protocol.	perl-ldap-0.44.tar.gz

C. Script.

A continuación, el diagrama de flujo del script desarrollado:



ANEXO II – Prueba de concepto: Instalación y configuración de servicios.

A. Servicio LDAP (OpenLDAP).

A.1. Instalación.

```
# tar xzf openldap-[…].tgz
# cd openldap-[…]/
# ./configure --prefix=/usr/local/openldap
# make install
```

A.2. Configuración.

Se utilizó una configuración estándar, siendo el archivo de inicialización el siguiente:

```
dn: dc=msi,dc=com
objectclass: dcObject
objectclass: organization
o: MSI
dc: msi

dn: cn=Manager,dc=msi,dc=com
objectclass: organizationalRole
cn: Manager
```

El esquema elegido para las entradas en el servidor LDAP fue:

```
dn: cn=msi.com,dc=msi,dc=com
objectclass:inetOrgPerson
userCertificate;binary:< file:///[certificado digital corporativo]
userSMIMECertificate:< file:///[firma del certificado digital corporativo]
sn: msi.com
cn: msi.com
description: msi.com
```

A.3. Comandos utilizados.

Operación	Comandos OpenLDAP
Incorporación de una entrada	ldapadd -x -D "cn=Manager,dc=[XXX],dc=[YYY]" -W -f [archivo ldif]
Búsqueda de entradas	ldapsearch -x -b [base] [filtro] [atributos]

A.4. Creación de las entradas.

I. Observaciones:

- El servicio LDAP se utilizó para publicar certificados digitales corporativos.
- A efectos de validar los certificados, los mismos fueron firmados con una clave privada generada para el servidor LDAP.
- Los certificados digitales corporativos (atributo userCertificate) fueron almacenados en formato DER. El resultado de las consultas resulta en formato PEM (Privacy Enhanced Mail), por ese motivo las firmas se realizaron sobre el formato PEM.
- Las firmas de los certificados digitales corporativos (atributo userSMIMECertificate) fueron almacenados en formato binario. El resultado de las consultas se encuentra codificado en base64.

II. Procedimiento:

1) Creación de la clave privada del servidor LDAP:

```
# openssl genrsa -out /tmp/Clave.privada -aes256 2048
# openssl rsa -in /tmp/Clave.privada -pubout -out /tmp/Clave.publica
```

2) Firma del certificado:

```
# openssl x509 -inform PEM -in /tmp/Certificado.pem -out /tmp/Certificado.der -
outform DER
# openssl dgst -sha1 -sign /tmp/Clave.privada -out /tmp/Certificado.pem.firma
do/tmp/Certificado.pem
```

3) Creación de una entrada, ejemplo en ldif (LDAP Data Interchange Format):

```
dn: cn=XXX,dc=YYY,dc=ZZZ
objectclass:inetOrgPerson
userCertificate;binary:< file:///tmp/Certificado.der
userSMIMECertificate:< file:///tmp/Certificado.pem.firmado
sn: XXX
cn: XXX
description: Certificado digital corporativo de XXX
```

4) Alta y chequeo de una entrada:

```
# ldapadd -x -D "cn=Manager,dc=YYY,dc=XXX" -W -f entrada.ldif
# ldapsearch -x -s sub -b 'dc=YYY,dc=ZZZ'
'(&(objectclass=inetOrgPerson)(cn=XXX))'
```

B. Arquitectura PKI (OpenSSL).

B.1. Instalación.

```
# tar xzf openssl-0.9.8s.tar.gz
# cd openssl-0.9.8s
# ./config --openssldir=/usr/local/openssl
# make install
```

B.2. Creación de las CA.

Con las herramientas provistas por OpenSSL se crearon dos CA's y se administraron sus correspondientes claves privadas y certificados.

Los comandos ejecutados pueden resumirse en:

Operación	Comandos OpenSSL
Creación de una CA (+ certificado autofirmado)	CA.pl -newca
Creación de una clave privada y un request	openssl req -new -keyout [clave privada] -out [request]
Lectura de una clave privada	openssl rsa -text -noout -in [clave privada]
Lectura del request de un certificado	openssl req -text -noout -in [request]
Creación de un certificado	openssl ca -policy policy_anything -out [certificado] -infiles [request]
Lectura de un certificado	openssl x509 -text -noout -in [certificado]
Chequeo de un certificado	openssl s_server -cert [certificado] -key [clave privada] –www
Conversión de un certificado de pem a der	openssl x509 -inform PEM -in [certificado .pem] -out [certificado .der] -outform DER
Exportación de una clave privada y un certificado a PKCS12	openssl pkcs12 -export -in [certificado] -inkey [clave privada] -certfile [certificado de la CA] -name "Descripcion" -out [contenedor PKCS12]
Revocación de un certificado	openssl ca -config [openssl.cnf] -revoke [certificado]
Creación de la lista de certificados revocados	openssl ca -config [openssl.cnf] -gencrl -out [listado]
Lectura de la lista de certificados revocados	openssl crl -in [listado] -text

B.3. Observaciones.

Otros comandos empleados durante el curso de las pruebas fueron los siguientes:

Operación	Comandos OpenSSL
Eliminación de la password de una clave privada	openssl rsa -in [clave privada] -out [clave privada sin password]
Firma de un email	openssl smime -sign -signer [certificado] -in [mensaje] -inkey [clave privada] -out [mensaje firmado]
Encriptado SMIME	openssl smime -encrypt -des3 -in [mensaje] -out [mensaje cifrado] [certificado]
Desencriptado SMIME	openssl smime -decrypt -des3 -in [mensaje cifrado] -inkey [clave privada] -out [mensaje]
Generación de una clave privada	openssl genrsa -out [clave privada] -aes256 2048
Generación de la clave pública	openssl rsa -in [clave privada] -pubout -out [clave pública]
Firma de un archivo de texto	openssl dgst -sha1 -sign [clave privada] -out [firma] [archivo]
Verificación de la firma de un archivo	openssl dgst -sha1 -verify [clave pública] -signature [firma] [archivo]
Codificación de un achivo a base64	openssl base64 -in [archivo] -out [archivo en base64]
Decoficación de un archivo en base64	openssl base64 -d -in [archivo en base64] -out [archivo]

C. Servicio DNSSEC (Bind).

C.1. Instalación.

```
# ./configure --prefix=/usr/local/bind --with-openssl=/usr/local/openssl
STD_CDEFINES="-DDIG_SIGCHASE=1"
# make install
```

El parámetro DDIG_SIGCHASE=1 utilizado en la configuración inicial (etapa de pre-compilación) habilita el uso de la opción sigchase en la ejecución de la herramienta dig. Dicha opción permite emplear el comando (dig) para validar la firma de un registro.

C.2. Configuración.

A la configuración estándar (archivo named.conf) se añadieron las opciones:

```
dnssec-enable yes;
dnssec-validation yes;
```

C.3. Generación de zonas.

Las zonas creadas, en principio, no incluyeron parámetros ni opciones especiales. Cabe destacar que a los registros usuales se han agregado también algunos de tipo certificados (CERT o TYPE37).

C.3.1. Observaciones.

Para poder firmar las zonas con registros tipo CERT se debieron publicar los certificados digitales, originalmente en formato PEM, siguiendo estos pasos:

1) Codificación de los certificados (en PEM) en formato base64.
2) Conversión de los certificados (en base64) a hexadecimal.
3) Incorporación de los certificados a la correspondiente zona como registro tipo TYPE37 respetando esta sintaxis:

```
[registro] IN TYPE37 \# [Tamaño en bytes del certificado digital]* 0001** 0000 05*** [certificado codificado en hexadecimal]
```

* Incluyendo los valores 0001 0000 05 (+5 bytes).

** 0001= PKIX

*** 05 = RSASHA1

C.4. Generación de claves.

```
# key-singing key: dnssec-keygen -f KSK -a rsasha1 -b 1024 -n zone [zona]
# zone-singing key: dnssec-keygen -a rsasha1 -b 1024 -n zone [zona]
```

C.5. Firma de la zona.

En primer lugar se debieron incluir las claves públicas en el archivo de datos de la zona a firmar. La firma se concretó con el comando:

```
# dnssec-signzone -o [zona] -k [clave privada] [archivo de datos de la zona]
```

El resultante fue un archivo (con la extensión .signed) de los datos de la zona que incluyó las firmas de cada registro. Al archivo de configuración (named.conf) se incorporaron las claves públicas correspondientes a los dominios confiables.

C.6. Chequeo con dig.

Para realizar operaciones de validación con la herramienta dig primero se debieron obtener las claves públicas del dominio involucrado:

```
# dig [dominio] DNSKEY | grep -Ev '^($|;)' > [archivo de claves]
```

La verificación se llevó a cabo de la siguiente manera:

```
# dig +sigchase +trusted-key=[archivo de claves] [registro] [tipo de registro]
```

Una validación exitosa devuelve al final del mensaje de respuesta la siguiente información:

```
;; WE HAVE MATERIAL, WE NOW DO VALIDATION
;; VERIFYING A RRset for ar51.esi.com. with DNSKEY:18621: success
;; OK We found DNSKEY (or more) to validate the RRset
;; Ok, find a Trusted Key in the DNSKEY RRset: 18621
;; VERIFYING DNSKEY RRset for esi.com. with DNSKEY:18621: success

;; Ok this DNSKEY is a Trusted Key, DNSSEC validation is ok: SUCCESS
```

En cambio si no es posible validar la firma del registro la respuesta es:

```
;; WE HAVE MATERIAL, WE NOW DO VALIDATION
;; VERIFYING A RRset for ar51.esi.com. with DNSKEY:18621: success
;; OK We found DNSKEY (or more) to validate the RRset
;; Now, we are going to validate this DNSKEY by the DS
;; the DNSKEY isn't trusted-key and there isn't DS to validate the DNSKEY: FAILED
```

D. Servicio IMAP (Cyrus).

D.1. Instalación.

```
# ./configure --with-openssl=/usr/local/openssl --with-cyrus-prefix=/usr/local/cyrus
(opcional: --with-bdb-libdir=/usr/local/lib/db43/ --with-bdb-
incdir=/usr/local/include/db43/ --with-sasl=/usr/local)
# make
# make install
```

D.2. Configuración.

Se utilizó una configuración estándar, no se introdujeron parámetros especiales. El archivo de configuración imapd.conf utilizado fue:

```
configdirectory: /var/imap
partition-default: /var/spool/imap
admins: root
sasl_pwcheck_method: auxprop
allowplaintext: yes
```

Se crearon los directorios de trabajo con sus correspondientes permisos:

```
# adduser cyrus
# cd /var
# mkdir imap
# chown cyrus.cyrus imap
# chmod 750 imap
# cd /var/spool
# mkdir imap
# chown cyrus.cyrus imap
# chmod 750 imap
# cd /usr
# mkdir sieve
# chown cyrus.cyrus sieve
# chmod 750 sieve
# su cyrus
# [directorio de instalacion]/tools/mkimap
```

El último paso consistió en modificar el comportamiento del MTA (en este caso el sendmail) para que despache los emails al servidor IMAP. Para ello fue necesario introducir cambios en las líneas de uno de los archivos de configuración (el sendmail.mc):

```
define(`confLOCAL_MAILER', `cyrusv2')
MAILER(`cyrusv2')
dnl DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl
```

Para posteriormente crearse un nuevo archivo de configuración general (el sendmail.cf):

```
# m4 sendmail.mc > /etc/sendmail.cf
```

D.3. Creación de usuarios.

En el método de autenticación utilizado se guardan las passwords en un archivo con estructura de de base de datos, el sasldb2. Los comandos utilizados fueron:

Operación	Comandos

Alta de usuario en la base (sasldb2)	# /usr/sbin/saslpasswd2 -c [usuario]
Listado de usuarios en la base (sasldb2)	# /usr/sbin/sasldblistusers2
Creación de la casilla de un usuario	# /usr/local/bin/cyradm localhost --user root --auth plain > cm user.[usuario]

Como las cuentas de correo no coincidían con las de los correspondientes usuarios creados, en el servidor IMAP se utilizaron los archivos local-host-names y virtusertable (virtusertable.db), para relacionarlos.

Fuentes.

- http://infoleg.mecon.gov.ar/infolegInternet/anexos/70000-74999/70749/norma.htm, Firma Digital, Ley 25.506, consultado en enero 2013.
- http://www.cpan.org, The Comprehensive Perl Archive Network, consultado en marzo 2012.
- http://www.cyrusimap.org, Project Cyrus, consultado en marzo 2012.
- http://www.isc.org, Internet Systems Consortium, consultado en marzo 2012.
- http://www.openldap.org, The OpenLDAP Project, consultado en marzo 2012.
- http://www.openssl.org, OpenSSL Project, consultado en marzo 2012.
- http://www.perl.org, The Perl Programming Language, consultado en marzo 2012.
- http://royal.pingdom.com, Pingdom, consultado en mayo 2012.

Bibliografía.

- Paul Albitz - Cricket Liu, DNS and BIND, O'Reilly, 5th Edition, Mayo 2006.
- P. Mockapetris (ISI), RFC 1034: Domain Names - Concepts and facilities, Noviembre 1987.
- P. Mockapetris (ISI), RFC 1035: Domain Names - Implementation and specification, Noviembre 1987.
- D. Atkins (IHTFP Consulting) - R. Austein (ISC), RFC 3833 - Threat Analysis of the Domain Name System (DNS) (Informational), Agosto 2004.
- R. Arends (Telematica Instituut) - R. Austein (ISC) - M. Larson (Verisign) - D. Massey (Colorado State University) - S. Rose (NIST), RFC 4033 - DNS Security Introduction and Requirements, Marzo 2005.
- R. Arends (Telematica Instituut) - R. Austein (ISC) - M. Larson (Verisign) - D. Massey (Colorado State University) - S. Rose (NIST), RFC 4034 - Resource Records for the DNS Security Extensions, Marzo 2005.
- R. Arends (Telematica Instituut) - R. Austein (ISC) - M. Larson (Verisign) - D. Massey (Colorado State University) - S. Rose (NIST), RFC 4035 - Protocol Modifications for the DNS Security Extensions, Marzo 2005.
- S. Josefsson, RFC 4398 - Storing Certificates in the Domain Name System (DNS), Marzo 2006.

[1] "Internet 2011 in numbers", http://royal.pingdom.com/2012/01/17/internet-2011-in-numbers/ (Consultado el 21/05/2012)
[2] "Internet 2010 in numbers", http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/ (Consultado el 21/05/2012)
[3] "Climatic Research Unit emails, data, models, 1996-2009", http://www.wikileaks.org/wiki/Climatic_Research_Unit_emails,_data,_models,_1996-2009 (Consultado el 14/10/2011)
[4] "Case Study: The Koch-funded "ClimateGate" Echo Chamber", http://www.greenpeace.org/usa/en/campaigns/global-warming-and-energy/polluterwatch/koch-industries/case-study-the-koch-funded-c/ (Consultado el 11/10/2011)
[5] http://www.washingtonpost.com/wp-dyn/content/article/2009/11/20/AR2009112004093.html (Consultado el 14/10/2011)
[6] "Hackers steal electronic data from top climate research center", http://nakedsecurity.sophos.com/2011/02/07/hbgary-federal-hacked-and-exposed-by-anonymous/ (Consultado el 14/10/2011)
[7] "HBGary leaked emails [complete]", http://thepiratebay.org/torrent/6177791/HBGary_leaked_emails_[complete] (Consultado el 14/10/2011)
[8] "Bloquearon Leakymails", http://www.clarin.com/politica/Bloquearon-Leakymails_0_533946665.html (Consultado el 14/10/2011)
[9] "Ordenan el cierre del sitio Leakymails", http://www.lanacion.com.ar/1396676-ordenan-el-cierre-del-sitio-leakymails (Consultado el 14/10/2011)
[10] "WikiLeaks to release five million emails stolen from Stratfor", http://www.csmonitor.com/World/Latest-News-Wires/2012/0227/WikiLeaks-to-release-five-million-emails-stolen-from-Stratfor (Consultado el 15/05/2012)
[11] "NIST Special Publication 800-57 Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance" , http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf (Consultado el 07/12/2012)
[12] "DNS Security Introduction and Requirements", http://tools.ietf.org/html/rfc4033 (Consultado el 14/10/2011)
[13] "Resource Records for the DNS Security Extensions", http://tools.ietf.org/html/rfc4034 (Consultado el 14/10/2011)
[14] "Protocol Modifications for the DNS Security Extensions", http://tools.ietf.org/html/rfc4035 (Consultado el 14/10/2011)
[15] "Storing Certificates in the Domain Name System (DNS)", http://tools.ietf.org/html/rfc4398 (Consultado el 14/10/2011)
[16] "Cisco ASA and DNSSEC-Probable Issue with Packet Size", http://www.networkstraining.com/cisco-asa-and-dnssec-probable-issue-with-packet-size/ (Consultado el 14/10/2011)
[17] "Extension Mechanisms for DNS (EDNS0)", http://www.ietf.org/rfc/rfc2671.txt (Consultado el 14/10/2011)
[18] "Resource Records for the DNS Security Extensions", http://www.ietf.org/rfc/rfc4034.txt (Consultado el 14/10/2011)
[19] "Firma Digital, Legislación Argentina, Ley 25.506", http://infoleg.mecon.gov.ar/infolegInternet/anexos/70000-74999/70749/norma.htm (Consultado el 19/01/2013)
[20] "Firma Electrónica, Legislación Española, Ley 59/2003", http://www.boe.es/buscar/doc.php?id=BOE-A-2003-23399 (Consultado el 19/01/2013)