Infraestructura de clave pública en un ccTLD empleando al DNS

Pablo Greenwood, Rolando Chaparro, Benjamín Barán
Universidad Nacional de Asunción, Centro Nacional de Computación
Asunción, Paraguay, cc1439
{pgreen, rfox, bbaran}@cnc.una.py

Resumen

La mayoría de las implementaciones de infraestructura de clave pública (PKI) aún carecen de soluciones satisfactorias en la provisión de servicios de directorios escalables para el almacenamiento y localización de certificados. En tal sentido y en relación a los requerimientos de una PKI, el sistema de nombres de dominio (DNS) presenta algunas importantes características que pueden ser utilizadas para este propósito. Además de plantear las conveniencias del DNS como servicio de directorio simple para una PKI, este artículo propone extender el vínculo DNS-PKI integrando las operaciones de delegación de dominios en un *country top level domain* con la solicitud de certificados digitales, a partir de las notables coincidencias que se pueden encontrar en ambos procesos.

Palabras claves: Redes, Seguridad de Datos, DNS, PKI, Criptografía

Abstract

Most of today's Public Key Infrastructure (PKI) implementations still face some challenges to provide scalable directory services that allow locating and retrieving certificates. However, the Domain Name System (DNS) presents a number of benefits compared to current PKI solutions, namely those based on LDAP. This paper identifies the advantages of using DNS to provide simple PKI directory services. It also outlines the use this approach to integrate a PKI certificate request and issueance with a domain name delegation process in a DNS country top level domain, which is feasible considering the significant similarities found between both procedures.

Keywords: Networks, Data Security, DNS, PKI, Cryptography

1 Introducción

El progresivo aumento de la digitalización está cambiando la manera en que se relacionan las personas y las organizaciones. La naturaleza inmaterial e impersonal de las comunicaciones electrónicas ha creado la necesidad de implementar mecanismos que permitan, cuando menos, comprobar la identidad de los interlocutores y la veracidad de los datos transmitidos, sobre todo en los sistemas abiertos como Internet.

La infraestructura de clave pública o PKI (*Public Key Infraestructure*), basada en la criptografía de claves asimétricas y en los conceptos de certificados digitales y autoridades de certificación, es una alternativa para que las aplicaciones provean servicios de seguridad como la autenticación, la confidencialidad, la integridad de los datos y el no rechazo de su origen [18].

Sin embargo, y a pesar de la madurez de la tecnología de clave pública, la mayoría de las propuestas e implementaciones de PKI presentan aún ciertos inconvenientes [5]. Entre los aspectos que aún necesitan soluciones satisfactorias, se encuentra la provisión de servicios de directorio que puedan brindar mecanismos simples de localización y recuperación de certificados.

Una PKI provee normalmente acceso a sus certificados mediante LDAP (*Lightweight Directory Access Protocol*) [21], derivado de X.500 [2]. Ambos, X.500 y LDAP, están basados en sistemas centralizados, por lo que presentan desventajas de escalabilidad en términos de recursos computacionales, requerimientos de conectividad y carga administrativa [2]. Dadas estas consideraciones, un modelo no centralizado como el DNS es preferible.

En consecuencia, este trabajo muestra que el DNS (*Domain Name System*) [10], que es un sistema distribuido, simple, tolerante a fallos y ampliamente probado en la Internet, se ajusta a los requerimientos básicos y que su uso para proporcionar facilidades de una PKI no solo es técnicamente factible a través del registro denominado CERT [3], si no que también resulta realizable en términos prácticos.

Se plantea además potenciar y extender el vínculo DNS-PKI, mediante la integración de los servicios de generación y provisión de certificados en una PKI con el registro de nombres de dominio bajo un ccTLD (*country-code Top Level Domain*) [13], debido a que se pueden encontrar notables coincidencias en los procesos para delegar un dominio y obtener un certificado. Se debe considerar que actualmente las autoridades certificadoras recurren a referencias indirectas[1], como ser los administradores de dominios, para comprobar la veracidad de los datos suministrados en las operaciones de solicitud de certificados.

En la sección 2 de este artículo se presentan las características más importantes de la infraestructura de clave pública. En la sección 3 se define la estructura del sistema de nombres de dominios y algunas de sus características que pueden ser utilizadas en una PKI. La sección 4 presenta las ventajas del protocolo DNS respecto a LDAP para almacenar certificados. En la sección 5 se identifican los factores por los cuales se puede asumir que las funciones de los ccTLDs pueden estar asociados a los procesos de certificación desde el punto de vista operacional y del DNS. La sección 6 incluye las conclusiones y algunas futuras actividades que pueden surgir a partir de este trabajo.

2 Estructura y operación de las PKIs

2.1 Modelo de organización

Las técnicas de clave pública requieren de la utilización de certificados y los correspondientes repositorios para almacenarlos. Los certificados vinculan los datos del subscriptor con su clave pública, por lo que deben tener alta disponibilidad y facilidad de recuperación.

Las recomendaciones propuestas por la IETF para una PKI (llamadas PKIX [1]), son directa derivación de los certificados X.509, los cuales se han convertido en un estándar de facto. A los efectos prácticos se identifica a PKIX como X.509 [5].

La organización de los certificados X.509 es jerárquica, utiliza una RCA (*Root Certification Authority*) en la cual se basa la confianza, que a su vez podría ser trasferida verticalmente a los usuarios mediante otras CAs (*Certification Authorities).* Específicamente la clave pública de la RCA es conocida por los usuarios. Este conocimiento es utilizado para construir un camino confiable en la jerarquía de los certificados [2].

Existen además otros modelos de certificación como PGP (*Pretty Good Privacy*), en los cuales la confianza se construye horizontalmente, entre usuarios, y no a través de las Autoridades Certificadoras. Los mismos no pueden ser implementados a gran escala, debido a la complejidad que presupone la verificación de la confianza [8].

2.2 Espacio de nombres de los certificados

Los certificados X.509 fueron desarrollados para dar seguridad al servicio de directorio X.500, pero su uso no está asociado exclusivamente al mismo [3]. La identificación de los certificados X.509 se fundamenta en el "*distinguished name*" (DN) [7].

El DN está formado jerárquicamente por un conjunto de atributos abreviados, que corresponden al país (C, *country*), la entidad (O, *organization*), a la unidad dentro de la organización (OU, *organization unit*) y la persona, máquina, etc. (CN, *common name*). Un certificado X.509 representa la asociación del DN (C+O+OU+CN) con la correspondiente clave pública del subscriptor, más otros datos relacionados [7].

La versión 3 de X.509 permite nombres "alternativos" [6], con lo cual, para identificar certificados se pueden utilizar direcciones IP, direcciones de correo, URLs, entre otros, de forma similar a lo utilizado en el DNS.

1 Referencias de otras organizaciones que prestan algún servicio al solicitante

Debido a que las CAs manejan sus propias políticas de asignación de nombres, la misma entidad podría tener el mismo DN en diferentes CAs, o distintos DNs, en distintas CAs, lo cual es ambiguo y puede representar un problema de interoperabilidad, o al menos, para la identificación unívoca de los subscriptores [5].

2.3 Servicio de directorio y protocolo de acceso

A fin de establecer una comunicación segura, las usuarios requieren buscar y obtener los certificado de otras entidades en los servicios de directorios. Por lo general las PKIs que utilizan X.509 almacenan sus certificados y listas de revocación (CRL)[2] en repositorios X.500 y como protocolo de acceso utilizan LDAP [2]. El modelo X.500 define el protocolo DAP (*Directory Access Protocol)* que requiere muchos recursos computacionales para su funcionamiento. LDAP opera sobre TCP y provee la funcionalidad de DAP pero de forma más eficiente [21]. La "L" en LDAP proviene de *Ligth* DAP.

LDAP permite almacenar y mantener completa información sobre cada una de sus entradas, en uno o más servidores. La información es almacenada jerárquicamente y los datos pueden ser actualizados mediante un mecanismo de autenticación llamado SASL (*Simple Authentication and Security Layer)* [12].

Como se puede notar, LDAP no ha sido definido para almacenar exclusivamente certificados y de hecho se lo utiliza normalmente dentro de las organizaciones para diversas aplicaciones, como por ejemplo, para repositorio de red de datos personales, para autenticación centralizada, como *yellow pages* (paginas amarillas) [22], entre otros.

2.4 Mantenimiento y operación

Una PKI tiene varios componentes que están relacionados en su funcionamiento. En una PKI participan:

- Las CAs que generan los certificados. El registro puede hacerse en una RA (*Registration Authority).*
- Los subscriptores que poseen un certificado.
- Los usuarios que recurren a las CAs para validar la clave pública de los subscriptores.

Si bien el estándar X.509v3 referencia algunas reglas o CPS (*Certification Practice Statement*) para el proceso de obtención de un certificado, en la práctica cada CA define sus propias reglas de validación [5]. Por ejemplo, es usual que una CPS acepte referencias indirectas de otras organizaciones que prestan algún servicio al solicitante del certificado [20].

En general, es posible obtener certificados de empresas comerciales internacionales. Si se requiere usar una PKI para aplicaciones legales en un contexto nacional, las operaciones y otros controles definidos en un CPS, así como otras operaciones de las PKIs, deberán estar reglamentados por las leyes gubernamentales. Difícilmente, estas reglamentaciones puedan ser consensuadas con prestadores no nacionales del servicio, lo que dificulta su utilización específicamente en dominios como el de PY.

Debido a la estructura jerárquica, las RCAs normalmente se certifican a sí mismas, o dependen de otra RCA que a su vez se autocertifíca [5], por lo cual la confianza en la jerarquía de las PKIs se basa en la autovalidación de la unidad certificadora raíz. En la Figura 1 se presenta un diagrama abreviado sobre la relación de los participantes de una PKI, asumiendo la participación de una RA, conforme se explica a continuación:

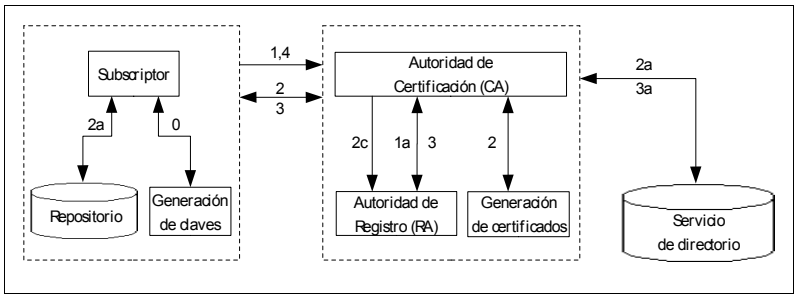

Figura 1:Organización de una PKI

2 *Certificate Revocation List*: lista para mantener los certificados que por alguna razón han sido anulados.

- *Generación de claves(0):* las entidades subscriptoras generan un par de claves, una pública y otra privada. Almacenan la privada en un repositorio seguro. La clave pública será utilizada para la generación del certificado.
- *Solicitud del certificado(1):* lo cual es posterior a la creación de las claves. Esta solicitud puede estar delegada en las Ras (1a) o ser realizadas directamente por las CAs. En este punto, la CA o RA, debe verificar la validez de los datos enviados en la solicitud por parte de las entidades.
- *Generación del certificado(2):* posterior a la verificación, el certificado es generado por la CA. La CA puede solicitar al subscriptor la comprobación de su clave pública. El certificado es almacenado en el servicio de directorio (2a) y enviado al subscriptor través de la RA si existe (2c).
- *Revocación de certificados(3):* en el caso que la clave privada del subscriptor se encuentre comprometida, el certificado deberá ser revocado (3a). También la CA podría revocar el certificado si es que comprueba que los datos proveídos no cumplen reglas de la CA.
- *Actualización de certificados (4):* generada por el vencimiento del certificado o por el cambio de alguno de los datos asociados al mismo, puede ser originada por la CA o por los subscriptores.

Si bien algunos de estos procesos utilizan a modo de referencia los estándares de clave pública criptográfica PKCS desarrollado por RSA Inc.[3], como por ejemplo, PKCS#10 [15] o PKC#12 [16], las CAs utilizan éstos u otros procesos, según sus propias normas de certificación (CPS).

3 Sistema de resolución de nombres (DNS)

3.1 Estructura organizativa

Las personas pocas veces hacen referencia a los recursos de la red mediante direcciones IP, sino que lo hacen mediante cadenas de caracteres como el URL *http://www.cnc.una.py*. Sin embargo, la red en sí misma requiere de direcciones binarias para direccionar los recursos. Por lo tanto, se necesita algún mecanismo para convertir las cadenas de caracteres en direcciones IP.

Para resolver este problema se desarrolló el DNS [19] que es un protocolo con un esquema de nombres jerárquico, basado en dominios y en una base de datos distribuida que soporta esta organización [10]. Si bien el DNS se usa principalmente para relacionar las direcciones destino con números IP, también puede utilizarse con otros fines, como por ejemplo, para asociar certificados a éstas direcciones a través del RR (*Resource Record*) CERT [3].

La estructura jerárquica del DNS esta dividida en zonas. Cada zona contiene una parte de la estructura y a los servidores de nombres de esa zona llamados *Authoritives Names Server*. Para resolver un nombre a su correspondiente dirección IP, el cliente consulta inicialmente a su servidor de nombre local. Si el servidor conoce la respuesta, podrá retornar el resultado. Si no la conoce, enviará la consulta a los *Root Servers*[4], los cuales están ubicados en la parte superior del árbol. Estos a su vez informarán sobre los servidores de segundo nivel responsables de ese dominio. Este proceso se repetirá con los siguientes niveles del árbol hasta llegar al servidor donde se encuentran los datos sobre el dominio solicitado [19].

Con el objetivo de evitar la sobre carga de los servidores del DNS, el protocolo implementa la posibilidad de hacer *cache* de las consultas realizadas. Así, cada vez que el *resolver*[5] obtiene una referencia sobre un dominio o algún dato sobre éste, lo almacena localmente y en forma temporal. El tiempo de éste almacenamiento es controlado por el TTL (*Time To Live*) asignado a cada RR utilizado en el DNS.

En términos prácticos, se puede mencionar que el funcionamiento del DNS está altamente probado y que el mismo es una precondición para la comunicación en Internet y entre las partes de una PKI.

3.2 Alcance de los nombres de dominio

La estructura de nombres del DNS se divide en cientos de dominios de nivel superior, cada uno de los cuales incluyen todas las direcciones para ese dominio.

3 *RSA Laboratories, division of RSA Data Security Inc.*

4 Existen en la actualidad 13 *root servers* distribuidos geográficamente.

5 Servidor que atiende las solicitudes de los clientes y realiza las consultas a la base de datos del DNS.

Cada dominio se puede dividir en sucesivos subdominios. Los dominios de nivel superior pueden ser genéricos (edu, net, com, mil, org, etc.) a los cuales se los denomina gTLDs (*Generic Top Level Domains*) y de países, definidos en el estándar ISO 3166[6] a los cuales se los llama ccTLDs [13]. Cada recurso se nombra por la trayectoria ascendente en la estructura del árbol hasta la raíz, que es representada por un "." (punto). Por su organización, se puede asegurar que no existirán dos nombres completos[7] iguales bajo dominios diferentes [10].

3.3 Servicio de directorio

El DNS tiene su propia base de datos, la cual es distribuida. Cada dominio puede contener un grupo de r*esources records* [19]. Existen distintos tipos de RR, pero el más común es el que asocia una dirección IP a un nombre. Cuando un *resolver* consulta sobre un dominio, lo que recibirá será los RRs asociados al mismo, los cuales se encuentran en la base de datos del servidor de ese domino. Cada RR consta de 5 atributos: el nombre completo, el ttl, el tipo, la clase y el valor. Dependiendo del tamaño de la respuesta, la misma podrá ser enviada mediante los protocolos UDP o TCP [11].

El nombre completo representa al recurso sobre el cual se necesita información, y es la clave primaria para la búsqueda. El *ttl* es una indicación de la estabilidad del registro en el *cache* de los demás servidores DNS. El tipo referencia de que registro se trata, algunos de ellos son: NS (servidor DNS), A (dirección de IP a un *hosts*), SOA (inicio de autoridad), MX (servidor de correo del domino). La *clase*, en el caso de Internet, siempre estará representado por "IN". El *valor* que puede ser un número IP, un nombre o una cadena ASCII dependiendo del tipo de RR [19].

Se puede notar, que la base de datos del DNS no solo mantiene números IP, por lo que podría ser utilizada para almacenar también certificados. De hecho y como ya se mencionó, en las actualizaciones del DNS se ha definido un tipo de RR llamado CERT [3], para guardar certificados.

Las especificaciones de actualizaciones dinámicas (*Dinamic Updates*) [23] del DNS implementan dos mecanismos de seguridad para agregar, actualizar o eliminar registros, llamados:

- *Secure DNS Transaction and Request Authentication*
- *Secret Key Transaction Authentication*

3.4 Modelo jerárquico de delegación y administración

Los TLDs son delegados a través de los *Root Servers*, según el ente autorizado para la asignación de nombres y direcciones de Internet, de acuerdo a los principios contenidos en [13]. En general la mayoría de las organizaciones en la región que administran los dominios ccTLDs son entidades reconocidas que históricamente se encuentran relacionadas a Internet y a su desarrollo, como ser universidades (CL, CO, MX, PA, PY, UY), redes académicas (BO), dependencias del gobierno (BR, AR, CU) o en organizaciones sin fines de lucro (PE, SV, HN)[8].

Se puede suponer, que si la administración de los ccTLDs fuera delegada en otras organizaciones, éstas serán de similar categoría, asumiendo la labor que realizan y el interés de los usuarios finales acerca del buen funcionamiento de la Internet. Siempre deberá existir alguna entidad responsable de los ccTLDs.

Al igual que en las PKIs, en el funcionamiento del DNS están involucradas distintas entidades. Inicialmente se identifican a las entidades administradoras, que mantienen y operan los servidores de nombres de los ccTLDs o gTLDs. En segundo lugar, se encuentran las organizaciones que delegan sus dominios y por último los usuarios, que utilizan al DNS para buscar y obtener información sobre los recursos a fin de iniciar una comunicación. A continuación se presenta un esquema abreviado del proceso de delegación (ver Figura 2):

- *Solicitud de delegación del dominio (1):* iniciada a pedido de la entidad interesada, la cual es enviada al administrador del ccTLD.

---

6 Código de identificación de países compuesto de dos letras (PY, PE, BR, AR, US, BO, SV, etc.).

7 También conocido como *fully qualified domain name* (FQDN).

8 Según datos extraídos del LacTLD (*Latin American & Caribbean Country Code Top Level Domain Organization*) *http://www.lactld.org/members.html*

- *Verificación de la solicitud(2):* el administrador del dominio verifica los datos incluidos en la solicitud y envía una petición de confirmación de los mismos a la organización interesada (2a).
- *Aprobación de la delegación(3):* una vez confirmado los datos, la delegación deberá ser aprobada según las pautas del administrador. El resultado será notificado a la organización (3a).
- *Actualización de la base de datos(4):* representa la creación y activación de la delegación del nuevo dominio en la base de datos del TLD.

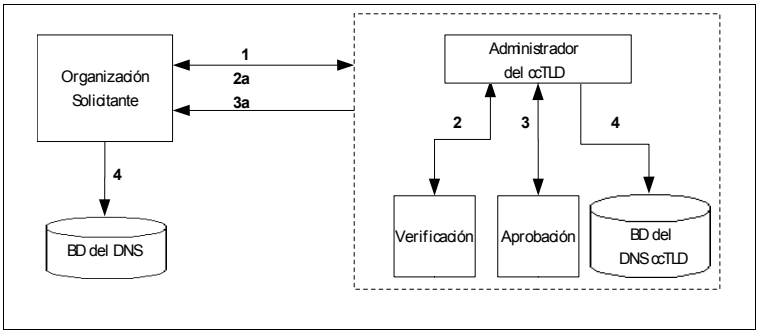

Figura 2:Proceso abreviado de delegación de dominios

En relación a la aprobación, el administrador del dominio realiza la verificación de los datos del solicitante, de forma similar a lo realizado por las CAs. En general, el nivel de verificación de la identificación es definido en cada ccTLD de acuerdo a sus propias pautas de delegación.

Se debe resaltar que en el DNS no se requiere mantener una lista de dominios eliminados o revocados, debido a que los RR asociados al dominio son retirados de la base de datos del DNS, por lo cual, las consultas realizadas sobre ese dominio no podrán ser respondidas.

4 Comparación de LDAP y DNS.

4.1 Servicios de directorios

A los efectos de realizar comparaciones de rendimiento se presenta a LDAP y al DNS como alternativas de almacenamiento, teniendo en cuenta que las implementaciones más comunes de PKI están basadas en LDAP y que a su vez el DNS permite almacenar certificados en su base de datos.

El servicio de directorio para una PKI debe soportar identificación de certificados a través de direcciones Internet, como los nombres de *hosts* o direcciones de correo. Las búsquedas que utilizan nombres comunes para la identificación de certificados carecen de validez en un ámbito general como la red Internet. Así mismo, los datos utilizados para localizar una dirección de red son los nombres de *hosts* o direcciones de correo, los cuales son únicos y están almacenados en el DNS.

Se pueden encontrar referencias sobre las deficiencias de LDAP para almacenar certificados en [2].

4.2 Localización simple

El DNS está definido para resolver un nombre de *host* a una dirección IP [11]. Cuando se contacta con un *host*, el DNS encuentra su número IP asociado, el cual será utilizado para establecer la comunicación. Se debe notar que antes de establecer la comunicación, se sabe con quién se quiere contactar. De la misma manera, pero a través del RR CERT se puede obtener el certificado asociado a ese recurso.

La localización del certificado está dada por clave (nombre de *host*, dirección de correo, etc.) la cual es única y conocida. Además, las aplicaciones no necesitan implementar protocolos distintos para la resolución de nombres y localización de certificados más que el DNS. El DNS es implementado por casi todas las aplicaciones que usan Internet.

En el caso de LDAP, las aplicaciones requerirán rutinas diferentes para la resolución de nombres y para el acceso a los certificados. Además, las CAs y LDAP no tienen definido de forma natural una única estructura raíz como el DNS, por lo que no se sabe a que servidor se debe recurrir para encontrar un certificado en particular.

4.3 Paquetes según protocolo de acceso

El DNS provee un mecanismo simple de localización de direcciones y certificados. Estas características se encuentran directamente relacionadas a la implementación del protocolo y al fin para el cual fue creado (asociar direcciones Internet con nombres de *hosts*). El DNS utiliza los protocolos UDP y TCP. Si el tamaño del paquete excede al soportado por UDP (600 bytes), el protocolo utiliza automáticamente TCP. Un paquete DNS se divide en: *header, question* y tres *answers* [10].

LDAP esta definido para dar acceso a los servicios de directorios X.500 [2], que poseen características mucho más amplias que las del DNS. Los paquetes LDAP utilizan el protocolo TCP y se dividen en: *message id*, b*ind request, bind response, unbind resquest, search request, search result entry, search result done, search result referent, modify request, modify response, controls*, entre otros [21].

Como se puede notar, la estructura de LDAP es mucho más compleja, lo cual es natural debido a los tipos de datos que soporta y al tipo de acceso que requieren sus usuarios. Por ejemplo, en el DNS las consultas no son interactivas y son realizadas por las aplicaciones. En el caso de LDAP, el acceso es interactivo para los usuarios, por lo que soporta mantener sesiones durante las conexiones [21]. En la Figura 3 se muestra el round trip[9] del DNS para realizar una consulta mediante TCP, considerando que el tamaño de los paquetes UDP por lo general no son suficientes para enviar certificados.

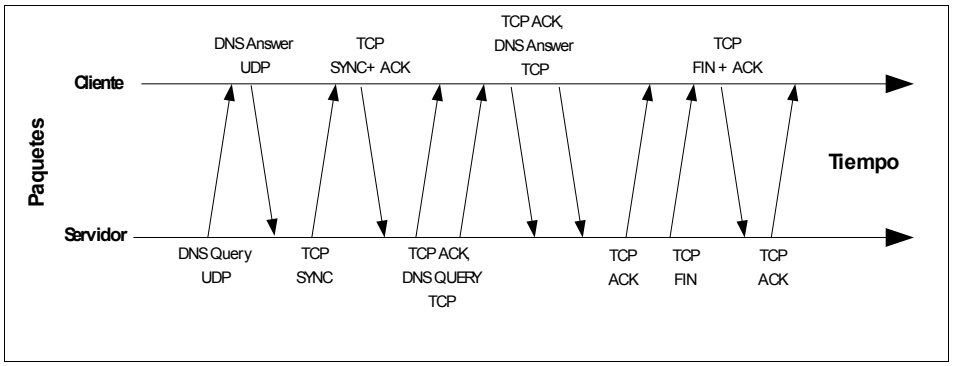

Figura 3:Consulta DNS

Como se puede apreciar, el DNS automáticamente cambia de TCP a UDP. Inicialmente envía una consulta UDP, si la respuesta no es completa, establece una conexión TCP [11].

En el caso de LDAP, luego de establecer la conexión TCP, el cliente envía un "*bind request*" para establecer la sesión, la cual se confirma en con un "*bind result*". La consulta en sí misma se efectúa mediante un "*search request*" y la respuesta se obtiene en los paquetes "*search entry*". El estado de la consulta es enviado al cliente a través de un "*search response*". Para finalizar la conexión el cliente envía un "*unbind request*" y cierra la conexión. En la Figura 4 se muestran los paquetes en una conexión LDAP.

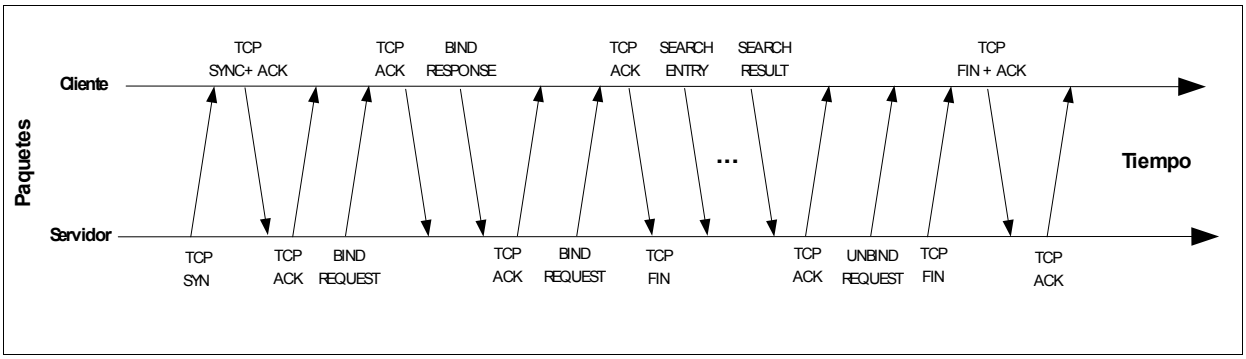

Figura 4: Consulta LDAP

Como se ve, para hacer una consulta LDAP se requieren más paquetes que en una consulta DNS. En la Tabla 1 que se muestra a continuación se resume el número de paquetes utilizados en cada caso.

9 Flujo de paquetes en el tiempo.

Tabla 1: Resumen de los paquetes DNS y LDAP

Protocolo	Cantidad de paquetes
DNS (incluyendo el fall-back)	12
LDAP	15 o más

4.4 Tamaño de los paquetes

La cantidad de paquetes requerido por el DNS para la localización y obtención de un certificado es menor. Si ambos servicios son utilizados bajo la misma infraestructura de red, el DNS también tendrá mejor rendimiento. En la Tabla 2 se muestran los resultados realizados en una red Ethernet, utilizando un certificado RSA de 1024 bits [9].

Tabla 2: Tamaño de los paquetes en DNS y LDAP

Protocolo	Tamaño en bytes
DNS (incluyendo el fall-back)	802
LDAP	852

5 Propuesta de ccTLDs como soporte de una PKI

5.1 Dependencia y uso del DNS

Como se mencionó en la sección 3.1, una PKI usualmente ve, necesita y usa al DNS como un servicio de infraestructura para establecer la comunicación entre sus entidades (CAs, RAs, y usuarios finales). Estrictamente, el DNS es fundamental para el funcionamiento de Internet pero no la PKI.

Los certificados utilizados por las organizaciones para comunicaciones externas no tienen sentido si la misma no posee un dominio (identificación) en Internet.

Así mismo, se deben considerar las funciones de los administradores de los ccTLDs [17], quienes delegan dominios a las organizaciones, las cuales podrían necesitar un certificado, y los procedimientos relacionados a dichas delegaciones, por lo que la delegación de un dominio puede estar asociada a la generación de certificados para dicho dominio.

5.2 Zona de dominio[10] de los ccTLDs

Debido al ámbito en el cuál opera el ccTLD (un país), se asume que será posible y más seguro autenticar la identidad de las organizaciones solicitantes de los dominios delegados y certificados, disminuyendo la posibilidad de errores. Se debe resaltar que una de las referencias utilizadas por las CAs para validar la identificación de las organizaciones, son los datos proveídos por los administradores de los ccTLDs, como en nuestro caso, el NIC-PY.

Así mismo, cabe enfatizar que en dominios como el de PY no existen PKIs nacionales operativas, por lo que se recurre a empresas no nacionales para obtener el servicio. Integrar ambas infraestructuras (ccTLD-PKI) representaría un importante vehículo de promoción de las PKIs y una ventaja para los usuarios.

5.3 Autoridades certificadoras

La confianza en las CAs comerciales se basa en la práctica en la autocertificación de ellas mismas. Debido a su naturaleza comercial, éstas pueden dejar de operar por diversos motivos (económicos, políticas de mercado, etc.) con lo cual los certificados y la seguridad de las conexiones estarían comprometidos.

Como se menciona en el apartado 3.4, la administración de los ccTLD es responsabilidad de organizaciones estrechamente relacionadas al funcionamiento de Internet. Si por alguna razón éstas dejaran de operar, la responsabilidad será delegada a otra organización igualmente comprometida con el desarrollo de Internet.

10 Ámbito de operación y alcance del ccTLD.

5.4 Procedimiento de delegación y certificación

Para que el ccTLD, en este caso el del dominio PY, emita certificados y brinde funcionalidades de una PKI, el presente trabajo propone integrar los procedimientos de certificación a los de delegación de dominios. De hecho, como se describe en los apartados 2.4 y 3.4, los procedimientos de certificación y delegación son similares, pero no iguales. Los procedimientos deben ser ajustados de manera a soportar la transferencia segura de las claves y datos de la solicitud, lo cual puede efectuarse mediante los estándares PKCS u otros recomendados.

Los administradores del ccTLD deben incorporar las CPS a fin de ajustar sus políticas de verificación de identidad de acuerdo a las recomendaciones existentes sobre PKIs [1].

La delegación del dominio puede o no incluir la generación de un certificado, dependiendo del requerimiento de la organización interesada. Se estima que solamente el 1.73% de *hosts* utilizan certificados[11], lo cual no representa una carga adicional muy relevante para el administrador del ccTLD, como tampoco lo es para la base de datos del DNS. En la Figura 5 se muestra un diagrama del procedimiento propuesto:

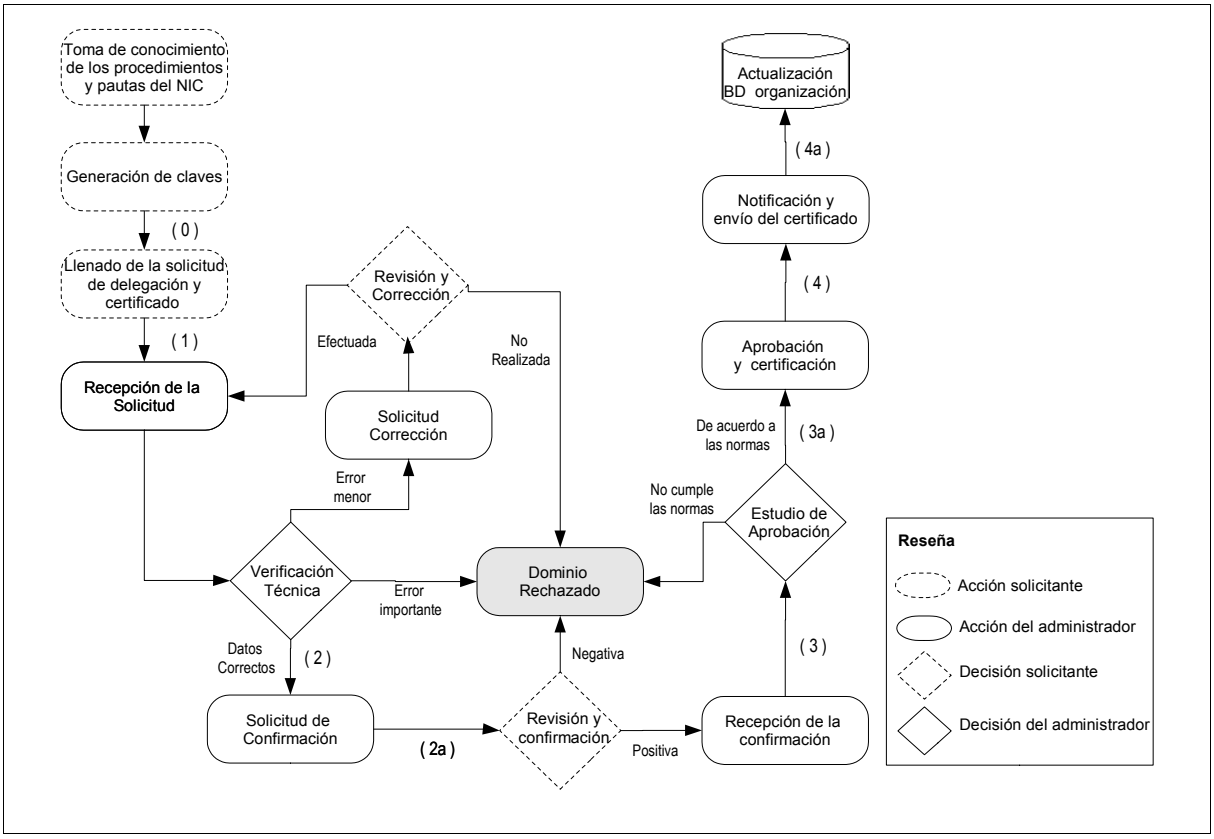

Figura 5: Proceso de delegación y certificación

A continuación se presenta un esquema abreviado acerca de las operaciones de delegación y certificación en un ccTLD:

- *La generación de claves(0):* las entidades subscriptoras generan un par de claves, una pública y otra privada. Almacenan la clave privada en un repositorio seguro. La clave pública será utilizada para la generación del certificado.
- *Solicitud de delegación del dominio y generación del certificado(1):* iniciada a pedido de la organización interesada, la cual es enviada al administrador, adjuntando la solicitud de generación del certificado a través de un medio seguro.

11 Según datos obtenidos de *http://www.securityspace.com*

- *Verificación de la solicitud(2):* el administrador verifica los datos incluídos en la solicitud del dominio y solicita confirmación de los mismos a la organización interesada, como también la confirmación de la clave privada (2a).
- *Estudio de aprobación de la delegación(3):* una vez confirmado los datos, la delegación del dominio deberá ser aprobada según las pautas del administrador (3a). Además, se debe realizar la verificación de la identidad del solicitante acordes a las leyes nacionales y recomendaciones internacionales.
- *Generación del certificado(4):* aprobada la delegación, el resultado es notificado a la organización, el certificado es generado por el administrador y enviado al subscriptor, quien deberá agregar el RR CERT en las tablas de su servidor de dominio.

La eliminación del dominio por cualquier circunstancia, implicará automáticamente la revocación del certificado de la organización, atendiendo a que éste no podrá ser encontrado por los *resolvers* en la estructura jerárquica del DNS. Un certificado no tiene sentido si no existe manera de acceder a él.

5.5 Modelo de certificación

En el *modelo básico* de delegación, a partir de la posesión del dominio, del certificado y de su correspondiente clave privada, la organización podrá solicitar actualizaciones a los datos de su dominio, como ser, el cambio de servidores.

De la misma manera, las organizaciones podrán solicitar certificados para sus *hosts* y cuentas de correos, los cuales una vez generados, deberán ser enviados a la organización solicitante y agregados en sus respectivos servidores de nombres.

Se puede además implementar un *modelo extendido*, en el cual las organizaciones (que poseen un dominio) generan sus propios certificados firmando con su clave privada, por lo que podrán administrar libremente las modificaciones, asignaciones y eliminaciones de los certificados que corresponden a su propia infraestructura.

Gracias a que en el *modelo extendido* las organizaciones generan sus propios certificados, las mismas podrán responder más rápidamente a las modificaciones de nombres de *hosts,* asignaciones IP y direcciones de correo, entre otros. Una desventaja de este modelo, es el costo adicional que implica para las consultas del DNS construir el camino jerárquico de los certificados, dado que se debe verificar el certificado de las organizaciones (que no se encuentran en el *cache*) y luego los certificados por ella firmados.

Como se puede apreciar, la integración DNS-PKI permitirá inclusive definir modelos de certificación más flexibles que posibilitarán a su vez menor tiempo en las actualizaciones y rapidez en las respuestas ante incidentes debido a la cercanía del administrador.

5.6 Revocación y naturaleza de las consultas DNS

Debido a que las consultas a través del DNS se hacen en línea mediante el *resolver* [11], los certificados serán obtenidos desde los servidores al momento que el cliente los necesite y éste podrá almacenarlos localmente para evitar acceso continuo al servidor DNS, controlando el tiempo de vida del certificado. Actualmente las CAs emiten sus listas de revocación a intervalos de tiempo definidos, según lo consideran pertinente.

Para validar la existencia del certificado se necesita simplemente realizar la consulta al *resolver* sobre el RR CERT del DNS nuevamente, por lo tanto se puede prescindir de las listas de revocación (también planteado en [14]) disminuyendo los inconvenientes relacionados a las mismas en cuanto a la operación y administración de las PKIs.

5.7 Interoperabilidad de PKIs

Es casi imposible pensar que una sola CA y su infraestructura puedan soportar el mantenimiento y administración de certificados en un contexto general, no solo por los recursos necesarios, sino también por la diversidad de requerimientos de acuerdo a cada país o región.

En el caso del modelo del DNS cada dominio es administrado internamente, por lo que se tiene una distribución jerárquica bien definida en relación a la infraestructura.

En un modelo más abierto, la confianza podría basarse entre ccTLDs, en cuanto que la responsabilidad de certificación recae sobre quién mejor conoce su zona de dominio.

5.8 Servicio de directorio

Si bien LDAP es completo como servicio de almacenamiento, las PKIs requieren acceso simple a los certificados [5]. El sistema distribuido requerido por las PKIs, presupone la cooperación entre servidores para soportar la escalabilidad. Esto es soportado y utilizado ampliamente en el DNS.

En cuanto a los procesos de adición, modificación, eliminación de los datos, se debe recordar que ambos servicios soportan protocolos seguros de actualización como se plantea en los apartados 2.3 y 3.3. En relación al rendimiento, en el capitulo 4 demuestra que el DNS es eficiente para almacenar certificados.

A estos factores se debe agregar que la gran mayoría de las aplicaciones utilizadas en Internet soportan el DNS, por lo que no requieren implementar otros protocolos para acceder a los certificados.

6 Conclusiones y actividades futuras

A partir de las deficiencias actuales de las PKIs en relación a la infraestructura y al modelo de certificación mayormente centralizados, existen básicamente dos factores muy importantes por los cuales se puede sostener la relación de los ccTLDs con una PKI:

- La dependencia operacional del DNS para el funcionamiento de toda la red
- La eficiencia del servicio de directorio del DNS y la conveniencia de su espacio de nombres

Como se demostró, es completamente factible la integración de los procesos de delegación y obtención de certificados en los ccTLDs, lo que representa una importante ventaja desde el punto de vista de los usuarios. Se debe considerar que los procesos asociados a ambas infraestructuras en realidad son uno solo, ¿ de qué sirve un certificado si no se tiene un dominio ?.

Debido al ámbito nacional en el que opera un ccTLD, los administradores pueden adaptar sus políticas de delegación a las leyes nacionales del país, lo que facilita la relación con los subscriptores. Así mismo se asume que es posible y más seguro autenticar la identidad de las organizaciones solicitantes disminuyendo la posibilidad de errores, teniendo en cuenta que la responsabilidad recae sobre quién mejor conoce su zona de dominio. De hecho, en la actualidad las CAs recurren a los administradores de los ccTLD para validar el espacio de nombres y la autenticidad del solicitante. Asociar el proceso de delegación de dominios y certificación permitirá además promover el uso de las PKIs.

Por otra parte, los usuarios en general y una PKI en particular, necesitan y utilizan al DNS como un servicio de infraestructura para establecer una comunicación. El DNS es fundamental para el funcionamiento de Internet y como servicio de directorio provee un mecanismo simple de localización de direcciones y certificados (el cual está dado por una clave única y conocida) requisito fundamental en la infraestructura de clave pública.

Por la naturaleza en línea de las consultas al DNS, los certificados son obtenidos cuando se realiza la conexión y pueden ser fácilmente actualizados, lo cual implica un mayor grado de seguridad en relación a las listas de revocación, atendiendo que las mismas actualmente son generadas en plazos definidos según las políticas de cada CA.

Además, el protocolo DNS está ampliamente probado, es eficiente, jerárquicamente distribuido, tolerante a fallos e implementado en casi todas las aplicaciones que usan Internet, por lo que no se necesita implementar otros protocolos adicionales para acceder a los certificados.

Como trabajo futuro, los autores esperan especificar y desarrollar los entornos operativos para la administración de los certificados por parte del ccTLD, así como también definir los prototipos de aplicaciones que efectúen consultas tipo CERT en el DNS para posibilitar la integración de este modelo.

Referencias

1. Chokhani S., Ford W., Sabett R., Merrill C., y Wu S. *X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*. IETF, RFC 3647. (Noviembre 2003).
2. Chadwick, D. *Deficiencies in LDAP when usde to support PKI*. Communications of the ACM, Vol. 46, No. 3. (Marzo, 2002).
3. Eastlake, D. *Storing Certificates in the Domain Name System*. IETF, RFC 2538. (Marzo, 1999).
4. Eastlake, D. *Domain Name System Security Extensions*. IETF, RFC 2535. (Marzo, 1999).
5. Gerck, E. *Overview of Certification Systems*, The Bell, Vol. 1, No. 3. (Julio 2000).
6. ITU-T Recommendation. *X.509v3 Information Technology Open Systems Interconnection – The directory: public-key and attribute certificate frameworks*. ITU-T. (Mayo, 2001).
7. ITU-T Recommendation. *X.501 Information Technology Open Systems Interconnection – The Directory: Models*. ITU-T. (1993).
8. Josang, A., Pedersen, I. y Povey, D. *PKI Seeks a Trusting Relationship*. Springer-Verlag. (Julio, 2000).
9. Josefsson, S. *Network Application Securtity Using The Domain Name System*. Master's thesis, Stockholm University. (2001).
10. Mockapetris, P. *Domain Names - Concepts and facilities*. IETF, RFC 1034. (Noviembre, 1987).
11. Mockapetris, P. *Domain Names - Implementation and Specification*. IETF, RFC 1035. (Noviembre, 1987).
12. Myers, J. *Simple Authentication and Security Layer (SASL)*. IETF, RFC 2222. (Octubre, 1997).
13. Postel, J. *Domain Name System Structure and Delegation*. IETF, RFC 1591. (Marzo, 1994).
14. Rives R. *We Can Eliminate Certificate Revocation Lists*. Springer-Verlag. (Febrero, 1998).
15. Nystrom M, y Kaliski B. *PKCS #10: Certification Request Syntax Standard Version 1.7*. IETF, RFC 2986. (Noviembre, 2000).
16. RSA Laboratories. *PKCS #12: Personal Information Exchange Syntax Version 1.0*. RSA Laboratories. (Junio, 1999).
17. Stahl, M. *Domain Name Administrators Guide*. IETF, RFC 1032. (Noviembre, 1987).
18. Stallings, W. *Cryptography and Network Security, 2nd edition*. Prentice Hall. (1999).
19. Tanenbaum, A. *Computer Networks, 3rd edition*. Prentice Hall. (1997).
20. VeriSign. *Normas para el proceso de certificación para los servicios de certificación bajo la VeriSign Trust Network Version 2.0*. CertiSur. (Julio, 2003).
21. Wahl, M., Howes, T. y Kille S. *Lightweight Directory Access Protocol Versión 3*. IETF, RFC 2251. (Diciembre, 1997).
22. Wang, X., Schulzrinne, H., Kandlur, D. y Verma, D. *Measurement and analysis of LDAP performance*. ACM Press. (2000).
23. Wellington, B. *Secure Domain Name System (DNS) Dynamic Update*. IETF, RFC 3007. (Noviembre, 2002).