Documento Final de Tesis

Esquema de Certificación Digital Masiva para Colombia

Autor: René Francois Vera Roa

Código: 200428219

Asesor: Milton Quiroga

Maestría en Ingeniería de Sistemas y Computación

Universidad de los Andes

Bogotá, Enero 15 de 2007

Tabla de Contenido

I. Introducción

En la actualidad, el gran crecimiento en la utilización de tecnologías de información ha llevado a que cada vez se realicen más comunicaciones a través de medios electrónicos, las cuales han demostrado contribuir al desarrollo de las empresas y entidades que cuentan con estas formas de comunicación, gracias a las diversas ventajas en eficiencia, practicidad, costos, etc. que implica la utilización de medios electrónicos.

Así pues, sería de gran importancia para nuestro país contar con tecnologías de comunicación electrónica ampliamente accesibles para nuestros ciudadanos, y de esta manera proveer a la sociedad en general de los beneficios que implica la utilización de estos medios de comunicación.

Sin embargo, dentro de este entorno de comunicación electrónica masiva, en muchos casos la información que se transmitiría requiere ser protegida por medidas de seguridad (p. ej. información confidencial) y/o contar con los elementos suficientes como para ser reconocida jurídicamente (p. ej. documentos que requieren ser firmados). Es por esto que surge la necesidad de contar con tecnologías ampliamente difundidas y legalmente reconocidas que provean mecanismos para el envío de este tipo de información a través de medios electrónicos con todas las garantías requeridas.

Actualmente, la tecnología más popular que cumple con las condiciones anteriormente mencionadas consta de una PKI (*Public Key Infrastructure*) basada en certificados digitales. Una PKI es una infraestructura que tiene como fin permitir el intercambio seguro de información a través de medios no seguros, utilizando para tal fin criptografía de llaves asimétricas (públicas y privadas). Adicionalmente, cada pareja de llaves (llave pública + su correspondiente llave privada) sirve para identificar a su dueño, y dichas identidades son validadas y refrendadas por una autoridad que se considera confiable. Cuando una PKI se basa en certificados digitales, la autoridad confiable que valida y refrenda las identidades es una Autoridad de Certificación, y a cada usuario del sistema se le asigna un certificado digital, el cual contiene los datos de su dueño, junto con su llave pública.

La tecnología PKI basada en certificados digitales es escalable (de tal manera que pueda ser utilizada en un entorno de comunicación masiva) y está en capacidad de brindar las siguientes garantías en la comunicación:

- ✓ **Confidencialidad:** el contenido del mensaje sólo puede ser conocido por los interlocutores.

- ✓ **Autenticidad:** los interlocutores son quien dicen ser**.** En otras palabras, se puede afirmar que un certificado digital es una forma fiable de identificación en comunicaciones electrónicas.

- ✓ **No Repudiación:** se cuenta con mecanismos para identificar al emisor del mensaje aún después de terminada la comunicación, y de esta manera evitar que dicha persona niegue haber enviado el mensaje. Para contar con esta garantía es necesario que el emisor haya enviado la firma digital del mensaje, la cual es avalada por las leyes de nuestro país como equivalente funcional de una firma manuscrita.

- ✓ **Integridad:** el mensaje no ha sufrido ningún cambio entre su envío y recepción.

En un esquema de esta naturaleza, el certificado digital podría tener diversas utilidades de uso masivo que requieren identificación y/o intercambio de información de manera segura. Ejemplos de estas aplicaciones son: pago de impuestos y servicios públicos, tramitación de documentos, firma de documentos, votación en elecciones, realización de movimientos de dinero y transacciones comerciales, etc.

El presente documento propone los detalles tecnológicos y logísticos para la implementación a gran escala de una PKI basada en certificados digitales en Colombia, de tal manera que cualquier ciudadano de nuestro país tenga acceso a dicho sistema. Para construir un planteamiento razonable y aplicable, se tuvieron en cuenta la realidad, necesidades y restricciones que se presentan actualmente en nuestro país.

Inicialmente, se presentarán los conceptos teóricos relacionados con un esquema de certificación digital, junto con las tecnologías que hacen posible su implementación. Posteriormente, se presentarán antecedentes del esquema planteado en este documento, y luego se procederá a realizar una descripción de las condiciones actuales que se presentan en nuestro país para la implementación del esquema mencionado. A continuación de esto, se presentará la propuesta de implementación, junto con un análisis de vulnerabilidades relacionado con dicha propuesta; y finalmente se enunciarán las principales conclusiones, recomendaciones y trabajos futuros planteados, relacionados con el trabajo realizado.

II. Marco Teórico

A continuación se presentarán los principales conceptos y elementos tecnológicos que hacen parte de la implementación de una PKI basada en certificados digitales. Se iniciará repasando los conceptos y funcionalidades básicas, para luego enfocarse en los servicios adicionales que presta una infraestructura de esta naturaleza. También se realizará un breve repaso sobre el hardware de soporte disponible para esquemas de certificación digital, y finalmente se presentarán los aspectos más importantes a nivel de sistema distribuido en un sistema de esta naturaleza.

Conceptos Generales y Tecnologías Relacionadas

En esta sección se describen los conceptos generales y tecnologías base que hacen parte de una PKI que utiliza certificados digitales.

Un **Certificado Digital** consta principalmente de información que identifica a su dueño, junto con una llave pública. Tanto dicha llave pública como su llave privada correspondiente serán utilizadas para realizar cualquier operación criptográfica que involucre al dueño del certificado digital, incluyendo **Firmas Digitales**. Las firmas digitales, además de cumplir una función equivalente a las firmas manuscritas (refrendar información por parte del dueño de la firma), hacen computacionalmente imposible la modificación de la información refrendada sin invalidar la firma.

Una PKI basada en certificados digitales se implementa a través de una **Autoridad de Certificación**, la cual es una autoridad reconocida y que se considera confiable, que se encarga de emitir y administrar los certificados digitales. La manera en que una autoridad certificadora refrenda un certificado que emite, es firmándolo digitalmente. Estos certificados pueden ser emitidos para usuarios finales (los cuales pueden representar personas, empresas, sistemas informáticos, servidores, etc.) o para otras autoridades de certificación, que se considerarán "subordinadas". Aún cuando una autoridad de certificación no sea subordinada de otra, ésta contará con un certificado digital emitido a sí misma.

Adicionalmente, las autoridades de certificación publican una DPC (Declaración de Prácticas de Certificación), la cual define las políticas de prestación de servicio que tiene la entidad, y en la cual se incluyen las medidas de seguridad a nivel logístico y tecnológico con que cuenta la entidad con el fin de darle mayor credibilidad y confiabilidad a los certificados digitales que expide. Además, en la DPC también se definen medidas de seguridad que deben tomar el dueño del certificado digital y los terceros que deseen comunicarse de manera segura con él a través de su certificado digital.

Así pues, para que un certificado digital mantenga su calidad de confiable, debe cumplir con todas las regulaciones que mencione la DPC de la entidad de certificación que lo expidió. La falla en el cumplimiento de dichas políticas o regulaciones, conlleva a la revocación del certificado digital.

Adicionalmente, para que un sistema informático esté en condición de confiar en un certificado digital, debe realizar las siguientes validaciones:

1. Que el certificado digital se encuentre dentro de su período de validez, el cual es definido por la autoridad de certificación que lo emitió.

2. Que la autoridad de certificación que emitió el certificado digital se encuentre entre su lista de autoridades de certificación confiables. Esto se implementa contando con un repositorio de los certificados digitales de las autoridades de certificación en las que el sistema confía. Si el certificado digital de la autoridad certificadora no se encuentra en dicho repositorio, no se aceptará el certificado digital que se está validando, a menos que la autoridad certificadora que lo firmó sea subordinada de otra, en cuyo caso la aceptación del certificado digital dependerá del resultado de realizar este mismo proceso de validación sobre el certificado digital de la autoridad certificadora en cuestión.

3. Que el certificado digital no se encuentre revocado. Una autoridad de certificación está en capacidad de revocar cualquier certificado digital que haya emitido si el dueño del certificado se lo solicita, o si se cumplen ciertas condiciones que ponen en duda la seguridad de dicho certificado. Una autoridad certificadora siempre ofrece un servicio públicamente accesible en el que se puede hallar si un certificado digital que haya emitido ha sido revocado.

Adicionalmente, toda la información asociada a los usuarios de la autoridad certificadora, se valida, registra y administra de manera independiente por parte de una **Autoridad de Registro**. En muchos casos, el interesado en suscribirse como usuario debe proveer a la autoridad de registro de documentación que soporte la información requerida para facilitar el proceso de validación de la misma.

Es importante tener en cuenta que, en la mayoría de los casos, la autoridad certificadora y la autoridad de registro pertenecen a la misma entidad, por lo cual es muy frecuente que a dicha entidad se le denomine simplemente “autoridad de certificación” o “entidad de certificación”.

Servicios Adicionales que Presta una CA

A continuación se hará un repaso de las tecnologías adicionales más importantes relacionadas con el funcionamiento de una autoridad de certificación.

Validación de Certificados Digitales

Como se mencionó previamente, una autoridad de certificación cuenta con un servicio de validación de certificados digitales, con el fin de identificar los que se encuentren revocados. Para evitar ataques de suplantación, independientemente de la tecnología utilizada para implementar este servicio, los mensajes que se envían al cliente deben ser firmados digitalmente por la autoridad certificadora. Las tres tecnologías más populares que se utilizan para implementar dicho servicio son:

CRL (Certificate Revocation List)

Una autoridad de certificación puede publicar una CRL, la cual es una lista que contiene los números de serie de los certificados revocados, junto con sus fechas de revocación, y opcionalmente la razón para la revocación de cada certificado. Esta CRL es actualizada por la autoridad de certificación a su criterio (pero por supuesto, muy frecuentemente) y publicada en un repositorio de público acceso, cuya ubicación el cliente puede conocer generalmente a través del campo *CRL Distribution Points* del certificado digital de la autoridad de certificación. Luego de que el cliente ubica el repositorio, descarga la CRL y verifica que el número de serie del certificado digital que está validando no se encuentre dentro de la lista.

Debido a que el contenido de una CRL se hará más y más grande a través del tiempo, en algunos casos es particionada bajo algún criterio (generalmente, número de serie de los certificados), para que el cliente sólo tenga que descargar la partición que le pueda llegar a interesar, y así ganar en eficiencia.

OCSP (Online Certificate Status Protocol)

OCSP es un protocolo en línea que le permite a un cliente conocer el estado de validez de uno o más certificados digitales.

Para utilizar este servicio, el cliente realiza una petición a un servidor OCSP (llamado comúnmente "*OCSP Responder*") respecto al estado de validez de uno o más certificados digitales. El servidor retorna el estado de validez de cada certificado digital incluido en la solicitud el cual puede ser:

- *good*: esta respuesta indica que el certificado no ha sido revocado.
- *revoked*: indica que el certificado fue revocado. En este caso, se incluye en la respuesta la fecha y hora de revocación, y opcionalmente la razón de revocación.
- *unknown*: indica que el servidor no tiene información sobre el certificado en cuestión.

Varios protocolos de nivel de aplicación son soportados para transportar los mensajes: HTTP, SMTP, LDAP, entre otros. Adicionalmente, los mensajes que retorna el servidor son firmados digitalmente, utilizando la llave privada que corresponde al certificado digital de:

- La autoridad de certificación o

- Un "*Trusted Responder*" en cuyo certificado digital confía el cliente OCSP o
- Un "*CA Designated Responder*" (también conocido como "*Authorized Responder*") que posee un certificado digital marcado especialmente emitido por la autoridad de certificación. Esta "marca especial" indica que dicho *Responder* puede atender peticiones OCSP en nombre de la autoridad de certificación.

XKMS (XML Key Management Specification)

XKMS es un conjunto de Web services, entre los cuales se ofrece el servicio de consulta del estado de validez de certificados digitales. Estos Web services utilizan las tecnologías *XML Signature* y *XML Encryption*.

Consideraciones Respecto a la Aplicación a Gran Escala

La importancia a nivel de eficiencia, del servicio de validación de certificados digitales, cambia radicalmente cuando el número de usuarios del sistema crece considerablemente. Esto se debe a que en la medida en que se cuente con más usuarios, la cantidad de solicitudes de validación de certificados crecerá exponencialmente, ya que estos usuarios tenderán a comunicarse entre sí.

Por esta razón, es muy importante elegir acertadamente la tecnología de validación de certificados digitales en un sistema a gran escala. La diferencia en cuanto a eficiencia más importante que se puede identificar entre las alternativas más populares, tiene que ver con el tráfico de red que se genera debido a su utilización. A continuación se presenta una descripción del tráfico de red generado por cada una de las tres alternativas más populares para la validación de certificados digitales:

- **CRLs:** las CRLs, aunque se encuentren particionadas, envían al cliente más información de la que desea obtener, ya que enviarán información de revocación de varios certificados digitales en los cuales el usuario no se encuentra interesado. Esto genera una grandísima sobrecarga en el tráfico de red del sistema.

- **XKMS:** el cliente sólo recibe información referente al(a los) certificado(s) digital(es) que desea validar. Sin embargo, esta tecnología genera una sobrecarga importante en el tráfico de red del sistema, porque tiene que dársele un formato XML a todos los mensajes, lo cual aumenta considerablemente el tamaño de cada mensaje.

- **OCSP:** al igual que con XKMS, el cliente sólo recibe información referente al(a los) certificado(s) digital(es) que desea validar. A diferencia de XKMS, los mensajes son transmitidos en un formato bastante simple y plano, lo que evita una sobrecarga en el tráfico de red del sistema. Por lo tanto, OCSP es la alternativa de validación de certificados digitales más conveniente para sistemas a gran escala.

Estampado Cronológico

Este es un servicio adicional opcional que puede prestar una autoridad de certificación, en cuyo caso se denominará también "Autoridad de Estampado Cronológico" o "*timestamping authority*". También se puede dar el caso en el que la *timestamping authority* no es la CA como tal, sino que funciona similarmente a como lo hacen los *CA Designated Responders* para el servicio OCSP.

Este servicio consiste en asignar una estampilla de tiempo al conjunto de datos que el cliente desee. La *timestamping authority* firma digitalmente la pareja conjunto de datos + estampilla de tiempo. De esta manera, la *timestamping authority* está certificando que el conjunto de datos no ha sido modificado después del momento que indica la estampilla de tiempo.

En el mundo real, este conjunto de datos representa generalmente documentos de importancia como pueden ser contratos, reportes, etc. Sin embargo, su aplicación más importante se realiza utilizando firmas digitales como el conjunto de datos, tal como se explicará a continuación: con el fin de garantizar la propiedad de no repudiación en un mensaje, el emisor del mismo envía la firma digital del mensaje como parte de la comunicación, reconociendo así que el mensaje es de su procedencia. Si alguien se encuentra interesado en verificar el origen de dicho mensaje, simplemente tiene que validar la firma digital y verificar que el certificado digital asociado con dicha firma es confiable y válido. Sin embargo, en algunos casos, como puede ser en litigios legales, puede ser necesario realizar la verificación del origen del mensaje en un momento en el que el certificado digital asociado con la firma ya haya caducado o haya sido revocado. Para esto, se puede asociar una estampilla de tiempo a la firma digital en el momento en que se realizó, y de esta manera estar en capacidad de garantizar que la firma digital fue realizada cuando el certificado digital era aún válido. De esta forma se puede garantizar la propiedad de no repudiación sobre un mensaje aún después del período de validez del certificado digital correspondiente a la firma digital realizada.

Hardware de Soporte para el Funcionamiento de una CA

Existen algunos dispositivos de hardware que cumplen exclusivamente funciones de seguridad informática. Cuando estos dispositivos son utilizados dentro de un esquema de certificación digital, contribuyen a un mejor funcionamiento del sistema. Los principales son:

Dispositivos de Hardware Criptográficos

Existen diversos dispositivos de hardware encargados exclusivamente de cumplir funciones criptográficas. Todos se consideran dispositivos de almacenamiento seguro, ya que cuentan con diversos mecanismos de hardware y software que hacen prácticamente imposible

substraer información delicada de ellos sin pasar por un mecanismo de autenticación. Los dispositivos de hardware criptográficos están en capacidad de generar parejas de llaves, y de esta manera proteger llaves privadas a nivel de hardware, lo cual es el máximo nivel de protección del que puede gozar una llave privada. A continuación se presentan los dispositivos de este tipo más importantes:

Dispositivos de Hardware Criptográficos Personales

El dueño de un certificado digital puede proteger su llave privada y utilizar su certificado digital a través de un dispositivo de hardware criptográfico personal. Ejemplos de estos dispositivos son: tokens USB, smart cards, entre otros; siendo los tokens USB los más convenientes en términos de costos y versatilidad, ya que cualquier computador personal moderno cuenta con puertos USB. El mecanismo de autenticación que proveen estos dispositivos con el fin de poder ser utilizados es generalmente el ingreso de una contraseña, sin embargo, algunos cuentan con mecanismos como pueden ser los de autenticación biométrica. Estos dispositivos no únicamente pueden generar parejas de llaves, sino que también están en capacidad de almacenar llaves privadas y otro tipo de información generada por fuera del dispositivo, lo cual puede ser una decisión conveniente bajo ciertas infraestructuras de certificación digital.

Hardware Security Module (HSM)

Son dispositivos de almacenamiento seguro de alto desempeño, diseñados para almacenar múltiples parejas de llaves y realizar gran cantidad de operaciones criptográficas utilizando dichas llaves de manera muy eficiente. Los Hardware Security Modules generalmente hacen parte de la infraestructura de hardware con la que cuenta una CA, en cuyo caso son utilizados para generar y almacenar la llave privada de la CA, y para realizar todas las operaciones criptográficas que requieran su uso, siendo la principal actividad generalmente la firma de nuevos certificados digitales. Algunos HSMs pueden generar nuevas parejas de llaves para los usuarios, firmar el certificado digital correspondiente, y luego exportar dicha información a un dispositivo de hardware criptográfico personal. También existen HSMs que se encuentran en capacidad de trabajar junto con otros HSMs en paralelo, balanceando así la carga.

Dispositivos de Autenticación Biométrica

Estos dispositivos cuentan con mecanismos que autentican una persona a través de la lectura de información única a ella, relacionada con sus características físicas. Inicialmente, estos mecanismos fueron utilizados como mecanismos de autenticación secundarios, dadas las posibilidades realistas de burlarlos.

Dada la naturaleza compleja de la información biométrica, los mecanismos de autenticación biométrica producen a veces falsos positivos y falsos negativos durante el proceso de identificación de la persona. Los falsos negativos generan principalmente incomodidad al usuario, al no reconocerlo y forzarlo a presentar su información biométrica ante un lector

de manera repetida hasta ser reconocido. Por su parte, los falsos positivos traen consecuencias negativas en la seguridad del sistema, ya que permiten a alguien suplantar a un usuario legítimo del sistema. Las tasas que miden la proporción de falsos negativos y falsos positivos en un sistema de autenticación biométrica son la *False Reject Rate (FRR)* y la *False Accept Rate (FAR)*.

El mecanismo de autenticación biométrica que ha tenido más popularidad es el de lectura de huella dactilar, y asimismo se ha convertido en el más conveniente en términos de costos y seguridad, siendo el único a la fecha que cuenta con diversos productos comerciales que incorporan mecanismos avanzados y altamente efectivos para evitar la burla del sistema, la cual en el caso particular de las huellas dactilares se hacía a través de copias sintéticas de la yema de dedos humanos, o con el uso de dedos humanos robados. Adicionalmente, esta tecnología ha evolucionado de tal manera que es posible realizar la lectura correcta de huellas dactilares muy difíciles de leer anteriormente, las cuales correspondían a personas que han sufrido deterioro en las yemas de sus dedos debido a trabajos manuales o accidentes. Por estas razones, el mecanismo de autenticación por huella dactilar puede ser considerado un mecanismo de autenticación altamente seguro a la fecha.

Aspectos Sobresalientes del Sistema Distribuido que Conforma una CA

Una autoridad certificadora es un software de alta capacidad que ofrece servicios a múltiples usuarios. Por esta razón, este software requiere ser instalado en un sistema distribuido. Los aspectos más importantes de la arquitectura de dicho sistema distribuido son:

Balanceo de Carga

La finalidad del balanceo de carga es prestar un servicio de alta calidad en escenarios de alta concurrencia, de manera que dicha concurrencia sea transparente a los usuarios. Debido a que se está planteando un esquema a gran escala, el balanceo de carga se torna en un aspecto técnico vital a tener en cuenta para lograr el funcionamiento adecuado de una CA en este contexto.

Replicación y Consistencia

La implementación de balanceo de carga implica asimismo la implementación de otras prácticas propias de los sistemas distribuidos como lo son la replicación y el manejo de consistencia.

La replicación se refiere a información que necesita ser localizada de manera repetida en diversas ubicaciones, para que cualquier servidor que haga parte de un sistema de balanceo

de carga esté en capacidad de funcionar casi tan bien como si fuera el único servidor que prestara sus servicios. Lo anterior implica replicación a nivel tanto de información volátil como persistente.

El otro gran beneficio de la implementación de replicación en un sistema es el aumento de la confiabilidad y disponibilidad del sistema debido a una mayor capacidad de tolerancia a fallas.

Asimismo, cuando se implementa replicación, es necesario contar con un sistema de manejo de consistencia, para que el servicio se preste con la misma coherencia lógica/funcional que tendría si los datos no estuvieran replicados, a pesar del hecho inevitable de tener en un momento dado diferentes datos en diversas copias que representan la misma información.

Los dos principales esquemas de soporte de replicación y consistencia son:

- Maestro-Esclavos: en este esquema, existe una copia de la información que es considerada la copia "maestra", esta puede ser leída y modificada, mientras que el resto de las copias son "esclavas", y sólo pueden ser leídas. La ventaja de este esquema es el fácil manejo de consistencia ya que las copias esclavas sólo tienen que estar al tanto de los cambios realizados en una copia, la maestra.

- Multi-Maestro: en este esquema, todas las copias de la información son maestras, es decir, pueden ser tanto leídas como modificadas. La ventaja de este esquema es su capacidad de ofrecer mayor disponibilidad de la información para ser modificada, pero su manejo de consistencia es complejo e implica grandes sacrificios en la eficiencia del sistema, ya que cada copia de la información debe estar al tanto de los cambios realizados en el resto de las copias.

Seguridad

Debido a que la función primordial de una CA es prestar servicios de seguridad informática, los sistemas de seguridad que deben proteger una CA deben ser de un altísimo nivel. Las consecuencias en caso de que sea realizado con éxito un ataque al sistema que conforma la CA, son por lo general muy graves, y en ciertos casos pueden llegar a incluir desde la revocación de algunos certificados digitales, hasta la pérdida de la licencia de funcionamiento de la entidad de certificación que administra la CA.

Tolerancia a Fallas y Alta Disponibilidad

Dos de los requerimientos no funcionales más importantes de una autoridad certificadora son la tolerancia a fallas y la alta disponibilidad.

Con la tolerancia a fallas se busca disminuir al máximo la probabilidad de pérdida o modificación accidental de datos: este objetivo es fundamental en una autoridad certificadora, ya que prácticamente toda la información que maneja un sistema de esta naturaleza puede considerarse crítica. La pérdida o modificación de certificados digitales o información que es utilizada para administrar la autoridad certificadora, conllevaría un gran prejuicio para todo el sistema, que podría necesitar desde la generación de nuevos certificados para algunos usuarios, hasta volver a generar absolutamente todos los certificados digitales. En cualquiera de dichos casos, no únicamente se afectaría la capacidad de funcionamiento del sistema, sino que se generaría un impacto altamente negativo sobre la imagen de la autoridad certificadora, lo que conllevaría desde la disminución en el número de usuarios, hasta la cancelación temporal o permanente del uso de este sistema.

Por su parte, la alta disponibilidad permite a los usuarios contar con el servicio en cualquier momento en que lo necesiten, y, teniendo en cuenta que una autoridad certificadora a gran escala podría utilizarse para gran cantidad de transacciones en cualquier momento, es muy importante tener la capacidad de prestar el servicio de manera absolutamente permanente. Adicionalmente, tal como se mencionó anteriormente, la falta de disponibilidad del servicio conlleva un impacto negativo en la imagen de la autoridad certificadora, generando asimismo las posibles consecuencias ya mencionadas.

III. Antecedentes

Durante los últimos años, han empezado a surgir alrededor del mundo diversos proyectos que incluyen la implementación de certificación digital a gran escala, o el uso de tecnologías relacionadas con dicha temática. Los servicios que se ofrecen como parte de estos proyectos se caracterizan habitualmente por tener la capacidad de llegar al público en general. A continuación se describen algunos de dichos proyectos:

Digital Signature Infrastructure For Administrative Simplification And E-Commerce Development (DIGISEC)[1]

El proyecto DIGISEC es la fase de prueba de un proyecto más amplio cuyo objetivo es la masificación de la firma digital en Italia, con el fin de agilizar los procesos administrativos del estado, así como promover y desarrollar ampliamente el comercio electrónico en dicho país.

Durante dicho proyecto, se desarrollará una infraestructura capaz de proveer un servicio completo de Autoridad Certificadora para las Cámaras de Comercio de Italia y sus clientes (empresas), de tal manera que las empresas puedan enviar documentos que hacen parte de sus obligaciones administrativas (por ejemplo, balances) vía Internet a la Cámara de Comercio correspondiente, garantizando autenticación, confidencialidad, integridad y no repudiación en la transacción. Para este fin, sería necesaria la distribución de aproximadamente 2 millones de certificados digitales a través de smart cards.

Durante la fase de prueba, se desarrollaría toda la infraestructura para el soporte de 103 Cámaras de Comercio y 100.000 clientes, y se daría la posibilidad de comparar el uso de las smart cards tradicionales respecto a las Java Cards, para elegir la tecnología que se utilizaría en el proyecto definitivo. Los resultados de dichas pruebas serían analizados para luego realizar nuevas pruebas sobre aplicaciones de comercio electrónico seguro.

Certificados Digitales en Documentos de Identidad

Existen diversos países que han empezado a implementar sistemas altamente modernos en los documentos de identidad; en algunos casos, estos sistemas incluyen la asignación de un certificado digital a cada documento. Ejemplos sobresalientes de estos proyectos son:

[1] Tomado de: *Digital Signature Infrastructure For Administrative Simplification And E-Commerce Development (DIGISEC).* (2005, Junio 14). Recuperado el 20 de Septiembre de 2005, de http://dbs.cordis.lu/fep-cgi/srchidadb?ACTION=D&CALLER=PROJ_IST&QF_EP_RPG=IST-1999-20981

Smart ID Card de Hong Kong[2]

A finales de 2001, el gobierno de Hong Kong decidió la expedición, a partir de mediados de 2003, de un nuevo documento de identidad para sus residentes. Este documento, denominado "Smart ID Card", incluiría todas las aplicaciones no relacionadas con inmigración como son la de licencia de conducción, tarjeta para bibliotecas, etc.

Dada la naturaleza de "smart card" del documento, éste se prestaba para poder almacenar un certificado digital que sirviera como identificación del usuario a la hora de realizar cualquier operación de comercio electrónico. De esta manera se tendría la oportunidad de promover el comercio electrónico aprovechando el proceso de modernización del documento de identidad, el cual involucraba a todos los residentes de Hong Kong (aproximadamente 6,9 millones de personas). Ante esta posibilidad, la autoridad certificadora Hong Kong Post decidió planear un proyecto cuyo fin era la inclusión, de manera gratuita durante el primer año, de un certificado digital en el nuevo documento de identificación. Dicho certificado podría ser solicitado por cualquier persona en el momento de tramitar el reemplazo del documento de identidad antiguo por una Smart ID Card.

A Junio de 2005, Hong Kong Post ha expedido 1,2 millones de certificados digitales, 960.000 de los cuales se encuentran dentro de una Smart ID Card.

DNI Electrónico de España[3]

El DNI Electrónico es el nuevo documento nacional de identidad, el cual, como su nombre lo indica, dejará de ser un documento regular para adquirir capacidades electrónicas adicionales. El DNI electrónico llevará incorporado un chip para acreditar electrónicamente la identidad y permitir la firma electrónica de documentos. El chip contendrá los datos personales de su titular digitalizados (lo que permitirá la identificación electrónica): filiación del titular, imagen digitalizada de la fotografía, imagen digitalizada de la firma manuscrita y plantilla de la impresión dactilar del dedo índice de la mano derecha. El documento tendrá una validez de cinco años cuando el titular no haya cumplido los 30 años; diez años cuando el titular haya cumplido los 30 y no haya alcanzado los 70; y permanente a partir de los 70 años. La activación del chip electrónico será voluntaria y se limita a los mayores de edad.

Renovación de Cédulas de Ciudadanía en Colombia

Las tecnologías de autenticación biométrica pueden llegar a ser muy útiles para aumentar la seguridad o la accesibilidad de un sistema de certificación digital masiva. Es por esto que es

[2] Tomado de: *Case Study Spotlight: Hong Kong Post's e-Cert Smart ID Card Project*. (2005, Agosto). Recuperado el 20 de Septiembre de 2005, de http://www.ptc.upu.int/pi/pi_cstudy.shtml

[3] Tomado de: Gigli, J. (2006, Enero 10). *España: Interior comienza a implantar este año el nuevo DNI electrónico*. Recuperado el 19 de Octubre de 2006, de http://www.gobiernoelectronico.org/node/227

importante repasar un antecedente sobresaliente en esta materia, que actualmente se está poniendo en marcha en nuestro país.

Como parte del proceso de modernización del sistema de identificación colombiano, se está llevando a cabo un proyecto que busca la renovación de las cédulas de ciudadanía de formatos antiguos para que todos los ciudadanos de nuestro país cuenten con su cédula de ciudadanía en el formato más reciente, el cual brinda una mayor seguridad en la identificación de cada persona.

Teniendo en cuenta el gran esfuerzo logístico que requiere esta renovación de documentos, junto con la fecha límite de finalización establecida (31 de Diciembre de 2009), se decidió contar con la ayuda de tecnología altamente moderna para agilizar el proceso. Esta tecnología consta de la instalación de máquinas en 160 municipios de nuestro país, con el fin de ser utilizadas por los ciudadanos para realizar el proceso de solicitud y toma de información para su nueva cédula. En estas máquinas no únicamente se puede ingresar la información biográfica de la persona, sino que se encuentran dotadas de una cámara que toma las fotografías requeridas para el documento, y lectores biométricos capaces de tomar las huellas dactilares de los 10 dedos de las manos de la persona. Así pues, con el fin de brindar alta seguridad en el proceso de autenticación ante el sistema encargado de registrar y realizar las renovaciones, la persona se tendrá que identificar no únicamente con sus datos biográficos, sino también con sus huellas dactilares. El sistema contará muy pronto (Octubre del presente año) con una versión digitalizada de las huellas dactilares de cada ciudadano, lo cual permitirá el proceso de comparación de las huellas tomadas en cada máquina con las registradas en el momento de la expedición de la cédula antigua de la persona, y de esta manera tener total certeza de su identidad.

IV. Condiciones para la Implementación

Con el fin de diseñar un esquema de certificación digital masiva para Colombia, se realizó una investigación sobre las condiciones actuales de nuestro país para la implementación de dicho esquema. Esta investigación incluyó aspectos legales, logísticos y tecnológicos.

Condiciones Legales

A continuación se presentarán los principales elementos jurídicos que soportan la implementación de una PKI basada en certificados digitales en nuestro país. Dicha tecnología está avalada y reglamentada jurídicamente, principalmente por:

- **Ley 527 de 1999 (Ley de Comercio Electrónico):** "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones."[4]. Esta ley define los fundamentos legales que soportan en nuestro país la tecnología PKI basada en certificados digitales. Los aspectos más importantes de esta ley son los siguientes:

  - ***Aplicabilidad de la ley:***
    "La presente ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en los siguientes casos:
    a) En las obligaciones contraídas por el Estado colombiano en virtud de convenios o tratados internacionales;
    b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo."[5]
    A pesar de que la ley tiene como título "Ley de Comercio Electrónico", su aplicación no se limita al comercio electrónico, sino que también abarca "todo tipo de información en forma de mensaje de datos". Esta interpretación de la ley fue posteriormente respaldada por la Corte Constitucional en la Sentencia 831 de 2001, en donde mencionan: "… la Ley 527 de 1999 no se limita al tema del comercio electrónico, aun cuando sus orígenes y su inspiración internacional conciernen fundamentalmente al ámbito mercantil."[6].

[4] Tomado de: *Ley 527 de 1999*. Recuperado el 26 de Octubre de 2006, de http://www.secretariasenado.gov.co/leyes/L0527_99.HTM
[5] Tomado de: *Ley 527 de 1999*, Parte I, Capítulo I, Artículo 1º. Recuperado el 26 de Octubre de 2006, de http://www.secretariasenado.gov.co/leyes/L0527_99.HTM
[6] Tomado de: *Sentencia C-831/01*, Parte VI, Punto 4. (2001, Agosto 8). Recuperado el 6 de Enero de 2007, de http://web.minjusticia.gov.co/jurisprudencia/CorteConstitucional/2001/Constitucionalidad/C-831-01.htm

- ***Definición de Mensaje de datos:*** "Mensaje de datos. La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax;"[7]. Todas las disposiciones jurídicas de esta ley aplican sobre este tipo de mensajes, lo cual incluye, como se puede leer, cualquier tipo de información relacionada con "medios electrónicos, ópticos o similares".

- ***Definición de Entidad de Certificación:*** "Entidad de Certificación. Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales;"[8]. Esta definición reconoce y define desde el punto de vista legal a la entidad de certificación. Menciona las capacidades de dichas entidades para emitir certificados digitales, así como para prestar servicios de estampado cronológico, entre otros.

- ***Reconocimiento jurídico de los mensajes de datos:*** la ley reconoce:
  - A los mensajes de datos como válidos jurídicamente.
  - Un equivalente funcional, bajo ciertas condiciones, entre un mensaje electrónico y uno escrito.
  - A los mensajes electrónicos como elementos de comunicación válidos jurídicamente dentro del proceso de realización de contratos.

- ***Reconocimiento jurídico de las firmas digitales:*** existen diversos apartes de la ley que se pronuncian respecto a este tema. El más importante es: "Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo."[9]. Este aparte le da reconocimiento jurídico a la capacidad de una firma digital de garantizar no repudiación. Adicionalmente, la ley reconoce jurídicamente, bajo ciertas condiciones, la equivalencia funcional entre la firma digital y la firma manuscrita.

- ***Establecimiento de estatutos acerca de las entidades de certificación:*** la ley establece:

[7] Tomado de: *Ley 527 de 1999*, Parte I, Capítulo I, Artículo 2º, Numeral a. Recuperado el 26 de Octubre de 2006, de http://www.secretariasenado.gov.co/leyes/L0527_99.HTM
[8] Tomado de: *Ley 527 de 1999*, Parte I, Capítulo I, Artículo 2º, Numeral d. Recuperado el 26 de Octubre de 2006, de http://www.secretariasenado.gov.co/leyes/L0527_99.HTM
[9] Tomado de: *Ley 527 de 1999*, Parte III, Capítulo I, Artículo 28. Recuperado el 26 de Octubre de 2006, de http://www.secretariasenado.gov.co/leyes/L0527_99.HTM

- A la Superintendencia de Industria y Comercio como ente encargado de autorizar la formación de nuevas entidades de certificación.
- Las actividades que puede realizar una entidad de certificación, entre las cuales es importante mencionar que figura, además de las actividades tradicionales, el servicio de archivo y conservación de mensajes de datos. Esto le da la capacidad a una entidad de certificación de convertirse en una autoridad confiable para el almacenamiento de información, responsabilidad que en ciertos casos los usuarios no desean tener.

➢ ***Establecimiento de estatutos acerca de los certificados digitales:*** los apartes más importantes que se refieren a los certificados digitales son:

- "CONTENIDO DE LOS CERTIFICADOS. Un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente:
  1. Nombre, dirección y domicilio del suscriptor.
  2. Identificación del suscriptor nombrado en el certificado.
  3. El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.
  4. La clave pública del usuario.
  5. La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
  6. El número de serie del certificado.
  7. Fecha de emisión y expiración del certificado."[10]

  Es importante notar que dentro de la información obligatoria básica que figura en este aparte, no aparece ningún tipo de información demasiado específica o difícil de obtener o demostrar, lo que facilitará el proceso logístico de recopilación de información al momento de la creación de un nuevo certificado digital.
- Causales de revocación de un certificado:
  "El suscriptor de una firma digital certificada, podrá solicitar a la entidad de certificación que expidió un certificado, la revocación del mismo. En todo caso, estará obligado a solicitar la revocación en los siguientes eventos:
  1. Por pérdida de la clave privada.
  2. La clave privada ha sido expuesta o corre peligro de que se le dé un uso indebido.

  Si el suscriptor no solicita la revocación del certificado en el evento de presentarse las anteriores situaciones, será responsable por las pérdidas o perjuicios en los cuales incurran terceros de buena fe exenta de culpa que confiaron en el contenido del certificado.
  Una entidad de certificación revocará un certificado emitido por las siguientes razones:

[10] Tomado de: *Ley 527 de 1999*, Parte III, Capítulo III, Artículo 35. Recuperado el 26 de Octubre de 2006, de http://www.secretariasenado.gov.co/leyes/L0527_99.HTM

1. A petición del suscriptor o un tercero en su nombre y representación.
2. Por muerte del suscriptor.
3. Por liquidación del suscriptor en el caso de las personas jurídicas.
4. Por la confirmación de que alguna información o hecho contenido en el certificado es falso.
5. La clave privada de la entidad de certificación o su sistema de seguridad ha sido comprometido de manera material que afecte la confiabilidad del certificado.
6. Por el cese de actividades de la entidad de certificación, y
7. Por orden judicial o de entidad administrativa competente."[11]

Es importante tener en cuenta que este aparte define la posibilidad de la solicitud de revocación de un certificado digital por parte del usuario, así como los casos en los que se encuentra obligado a realizar dicha solicitud. También se mencionan las razones que llevan a una entidad de certificación a tomar la decisión de revocar el certificado. Vale la pena notar que la no revocación de un certificado, cumpliéndose alguna de las causales mencionadas en este aparte, implicaría la presencia de una falla en las medidas de seguridad que deben tomar la entidad de certificación y el dueño del certificado digital.

- **Decreto 1747 de 2000:** "por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales."[12]. Este decreto es la principal disposición jurídica que reglamenta la Ley 527 de 1999. Los aspectos más importantes de este decreto son los siguientes:

  - ***Clasificación de las entidades de certificación:*** el decreto define dos tipos de entidades de certificación: abiertas y cerradas. Define a cada una de la siguiente manera:
    - "Entidad de certificación cerrada: entidad que ofrece servicios propios de las entidades de certificación sólo para el intercambio de mensajes entre la entidad y el suscriptor, sin exigir remuneración por ello."[13]
    - "Entidad de certificación abierta: la que ofrece servicios propios de las entidades de certificación, tales que:
      a) Su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor,

[11] Tomado de: *Ley 527 de 1999*, Parte III, Capítulo III, Artículo 37. Recuperado el 26 de Octubre de 2006, de http://www.secretariasenado.gov.co/leyes/L0527_99.HTM
[12] Tomado de: *Decreto 1747 de 2000 Nivel Nacional.* (2000, Septiembre 11). Recuperado el 31 de Octubre de 2006, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4277
[13] Tomado de: *Decreto 1747 de 2000 Nivel Nacional,* Capítulo I, Artículo 1°, Numeral 8. (2000, Septiembre 11). Recuperado el 31 de Octubre de 2006, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4277

b) Recibe remuneración por éstos."[14]

Dada esta clasificación, sólo se contará con la posibilidad de utilizar entidades de certificación abiertas como parte de la propuesta de implementación, ya que sólo éstas permiten el uso de certificados digitales para la comunicación entre usuarios.

- ***Restricciones sobre la validez jurídica de las firmas digitales:*** el decreto impone, entre otras medidas, la utilización de certificados emitidos por entidades de certificación abiertas para realizar firmas digitales que tengan la validez jurídica de una firma manuscrita.

Condiciones Logísticas

Actualmente, nuestro país ya cuenta con una infraestructura logística suficiente como para incluir a la mayoría de los colombianos como usuarios de un sistema de certificación digital masiva. Existen ciertas restricciones de acceso al sistema que aplican para las personas que viven en sitios menos poblados y de más difícil acceso, dado que la infraestructura y capacidades logísticas actuales de nuestro país no son suficientes para cubrir dichas áreas del territorio nacional.

Durante la investigación se identificaron entidades establecidas, cuya infraestructura es un buen indicador de las condiciones logísticas actuales para implementar un esquema de certificación digital a gran escala. Las principales son:

Certicámara

Certicámara es actualmente la única entidad de certificación abierta autorizada por la Superintendencia de Industria y Comercio. Esta entidad de certificación tradicionalmente ha prestado sus servicios de seguridad informática en proyectos de pequeña y mediana escala. Sin embargo, en el último año, Certicámara ha empezado a mostrar interés por mejorar su infraestructura de servicios de certificación digital, con el fin de adquirir capacidades para atender proyectos de mayor escala. Esto es muy importante ya que se empiezan a sentar precedentes en nuestro país en cuanto a la búsqueda de una infraestructura de servicios de certificación que soporte proyectos de alcance masivo.

Registraduría Nacional del Estado Civil

En nuestro país existen varias entidades que están en capacidad de manejar información básica de todos los colombianos. Sin embargo, la Registraduría Nacional del Estado Civil

[14] Tomado de: *Decreto 1747 de 2000 Nivel Nacional,* Capítulo I, Artículo 1°, Numeral 9. (2000, Septiembre 11). Recuperado el 31 de Octubre de 2006, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4277

es la autoridad reconocida que maneja dicha información. Por esta razón, y sobre todo por la infraestructura logística con la que cuenta la Registraduría gracias a que cumple esta función, ésta entidad es la que está en capacidad de hacer las veces de autoridad de registro para todos los colombianos de la manera más práctica y eficiente.

Ministerio de Comunicaciones – Agenda de Conectividad

La Agenda de Conectividad es un programa del Ministerio de Comunicaciones cuyo fin es fomentar el uso masivo de las tecnologías de información en aras del progreso de nuestro país.[15]. Por esta razón, la Agenda de Conectividad está en capacidad de colaborar con la implementación de un sistema de certificación digital masiva a través de su infraestructura logística y tecnológica, elaborada durante los proyectos que ha desarrollado.

La Agenda de Conectividad cuenta con un proyecto llamado Intranet Gubernamental, que incluye la conexión permanente de las entidades del Estado a una red, con el fin de compartir información. Dicha red es la Red de Alta Velocidad del Estado Colombiano (RAVEC), la cual ya se encuentra en funcionamiento. En la medida en que una amplia mayoría de sedes de la Registraduría se puedan conectar a RAVEC (esto implica proveer de conexión a aquellas sedes que se encuentren en locaciones apartadas de nuestro país, lo cual es un reto logístico importante), se podrá poner en funcionamiento, de una manera mucho más eficiente, una autoridad de registro administrada por la Registraduría.

[15] Tomado de: Agenda de Conectividad. (2006, Diciembre 13). *¿Qué es la Agenda?*. Recuperado el 13 de Enero de 2007, de http://www.agenda.gov.co/BulletinBoard/view_one.cfm?MenuID=5002&ID=146

V. Implementación

A continuación se presentarán los detalles técnicos y logísticos de la propuesta de implementación para el esquema de certificación digital masiva para Colombia, la cual se realizó teniendo en cuenta las condiciones y restricciones que se identificaron en nuestro país. Inicialmente se mencionarán las consideraciones logísticas generales, para luego presentar la arquitectura de todo el sistema planteado, la cual incluye tanto detalles técnicos como logísticos.

Aspectos Logísticos Generales

En esta sección se describirán los aspectos logísticos más importantes a tener en cuenta como parte del esquema propuesto. Estos aspectos están relacionados con la administración de los usuarios y, por lo tanto, con la autoridad de registro del sistema.

Actualmente, la Registraduría Nacional del Estado Civil es el único ente en nuestro país que cuenta con la autoridad e infraestructura adecuadas como para actuar como entidad de registro. Por esta razón, el esquema propuesto asume la asignación de la entidad de registro a la Registraduría.

De esta manera, en el momento en que el ciudadano solicite su cédula por primera vez, la Registraduría contará con su nombre y dirección, y asignará un número de identificación. Recordemos que estos tres datos son la única información requerida por la ley para ser incluida en el certificado digital de su dueño. De esta forma, la Registraduría estaría encargada de no únicamente expedir la cédula de ciudadanía, sino de registrar en la autoridad de registro la información de la persona, para que la autoridad de certificación pueda generar un nuevo certificado digital que corresponda a dicho ciudadano. Asimismo, se revocará el certificado digital una vez la Registraduría tenga conocimiento de la muerte del dueño del certificado.

En cuanto a los ciudadanos que ya cuenten con cédula de ciudadanía antes de la puesta en marcha del sistema, se utilizará la información de la base de datos de la Registraduría para poblar la base de datos de la autoridad de registro, y así estar en capacidad de expedir los certificados digitales correspondientes a este grupo de ciudadanos.

Adicionalmente, se debe tener en cuenta que cualquier usuario tendrá acceso permanente al sistema una vez ingresado al mismo, por lo cual se expedirán los certificados digitales con un período de validez muy largo, de tal manera que no sea necesario expedirle un nuevo certificado digital al usuario en el futuro porque le haya caducado uno anterior.

Como se puede observar en las diferentes afirmaciones realizadas, se está asumiendo que sólo ciudadanos colombianos mayores de edad que cuenten con cédula de ciudadanía

tendrán acceso al sistema. Sin embargo, existen otros tipos de usuarios que deberían estar en capacidad de ser utilizar del sistema:

- Menores de edad: en este caso, la manera más idónea para acceder al sistema sería a través de un mayor de edad en capacidad legal para representar al menor. Por lo tanto, no se considerará la posibilidad de emitir certificados digitales directamente a menores de edad.
- Integrantes de comunidades indígenas: las comunidades indígenas cuentan con regímenes jurídicos especiales, que les permiten tener formas de identificación diferentes a la cédula de ciudadanía. Por esta razón, en el caso de estos usuarios, la identificación que figura en el sistema deberá estar conformada por el nombre de su comunidad, junto con la identificación aceptada por el régimen jurídico que corresponde a su comunidad, la cual generalmente es un nombre.
- Extranjeros: en el caso de los extranjeros, la identificación que figura en el sistema deberá ser el número de su cédula de extranjería o pasaporte.

Arquitectura del Sistema

A continuación se describirá la arquitectura general del esquema de certificación digital masiva. Se iniciará mencionando el tipo de entidad de certificación que debe encargarse del sistema. Posteriormente se realizará un análisis de las alternativas de acceso al sistema y luego se describirá el funcionamiento de un sistema de recuperación de llaves privadas, el cual se decidió implementar debido a las necesidades identificadas durante el análisis de las alternativas de acceso al sistema. Finalmente, se presentará la arquitectura general del sistema distribuido que conforma la CA que hará parte del sistema.

Tipo de Entidad de Certificación

Tal como se mencionó durante el repaso de las condiciones legales para la implementación del sistema, los certificados digitales serán emitidos por una entidad de certificación abierta, ya que sólo éste tipo de entidades de certificación permiten el uso de certificados digitales para la comunicación entre usuarios.

Alternativas de Acceso al Sistema

En la presente sección se describirán y evaluarán las diversas alternativas que se tendrán para acceder al sistema. Es importante tener en cuenta que el usuario será libre de elegir cualquier alternativa, siendo posible elegir más de una. Los puntos de vista a tener en cuenta a la hora de evaluar cada alternativa son:

- Nivel de seguridad que ofrece.
- Conveniencia para el usuario.
- Implicaciones logísticas.

Consideraciones de Accesibilidad del Sistema

Para poder utilizar de una manera adecuada y cómoda los servicios que requieran de una infraestructura PKI, el usuario debe cumplir con dos condiciones:

- **Tener fácil acceso a los medios tecnológicos que permiten utilizar el sistema:** generalmente, esto se traduce en facilidades para acceder a un computador personal. Sin embargo, en un esquema a gran escala en el que todos los ciudadanos contarán con un certificado digital, se presentan diversas condiciones especiales que ameritan contar con una infraestructura tecnológica adicional de acceso público para acceder a los servicios que utilicen el sistema PKI. Esta infraestructura estará compuesta principalmente de cajeros automáticos con servicios adicionados para cumplir con esta función, así como de quioscos especialmente destinados para este fin. Las principales razones que ameritan la implementación de dicha infraestructura son:
  - Una gran cantidad de ciudadanos colombianos aún no tienen fácil acceso a un computador personal.
  - El uso de un computador personal para acceder a los servicios que utilicen el sistema PKI requiere su configuración previa, la cual asimismo requiere de una persona con algunos conocimientos en el tema. Por esta razón, existirían muchos usuarios que, aunque tengan fácil acceso a un computador personal, preferirán acceder a dichos servicios utilizando máquinas preconfiguradas.
  - En ciertos casos, sería muy cómodo y conveniente para algunos usuarios utilizar una infraestructura pública para acceder a diversos servicios, sin necesidad de tener que esperar a tener un computador personal a su disposición.

- **Haber sido capacitado suficientemente para hacer uso correcto de un sistema PKI:** generalmente, esto se traduce en haber recibido capacitación sobre el uso y cuidados que requiere la llave privada del usuario, ya sea que se encuentre almacenada en un dispositivo de almacenamiento seguro como un token USB, o en un archivo en formato de almacenamiento de información privada como puede ser PKCS#12. Adicionalmente, en el caso general, los usuarios de un sistema PKI cuentan con suficientes conocimientos previos sobre tecnologías de información como para que la capacitación mencionada pueda realizarse de manera muy breve.
  Sin embargo, dadas las condiciones del esquema de certificación digital masiva planteado, no es suficiente contar con formas tradicionales de acceso a un sistema PKI, sino que es imprescindible disponer de soluciones de acceso al sistema que sean fáciles de utilizar y que requieran de poca capacitación y conocimientos previos por parte del usuario. Por esta razón, los servicios a ser puestos a disposición públicamente, ya sea utilizando cajeros automáticos, o instalando quioscos para dicho fin, deben ser extremadamente fáciles de usar, contando con una interfaz con el usuario bastante sencilla de utilizar que brinde un alto nivel de orientación.

Mecanismos de Acceso Propuestos

Para utilizar el sistema PKI, el usuario necesita contar con su llave privada y la cadena de certificación correspondiente a su certificado digital. Para cumplir con esta condición, se puede contar con dos alternativas:

1. **El usuario tiene la información mencionada en su poder:** para que esta alternativa sea viable, será necesario que el usuario asuma el costo del dispositivo de almacenamiento en el que se le enviará la información mencionada, para esta alternativa, se tendrán en cuenta dos mecanismos:
    - *La información mencionada está almacenada en un token USB que se le entrega al usuario junto con la contraseña del dispositivo*: de todos los mecanismos de protección de la llave privada por medio de hardware, esta es la opción más económica y también la más flexible, ya que cualquier computador moderno cuenta con puertos USB. Adicionalmente, un puerto USB no sería difícil de instalar en los medios de acceso público mencionados anteriormente. Esta es la opción más conveniente para usuarios que planeen utilizar su certificado digital para realizar operaciones que requieren un altísimo nivel de seguridad, como pueden ser transacciones de altas sumas de dinero, firma de contratos importantes, transferencia de información altamente confidencial, etc.
    - *La información mencionada está almacenada en un archivo en formato PKCS#12 que se le entrega al usuario en un dispositivo de almacenamiento no seguro*: a pesar de las ventajas que ofrece a nivel de seguridad almacenar la información mencionada en un token USB, existirán muchos usuarios que no estarán dispuestos a asumir los costos que implica dicha alternativa. Por esta razón, conviene poner a disposición la opción de contar con la información mencionada en un medio de almacenamiento no seguro, protegiéndola a través de una contraseña que se le entregará al usuario, y de esta manera disminuyendo considerablemente los costos que implica un medio de almacenamiento seguro. Esta es la opción más conveniente para usuarios que planeen utilizar su certificado digital desde su computador personal para realizar operaciones que no requieren un altísimo nivel de seguridad (como por ejemplo, firma de correos electrónicos), y además, no estén dispuestos a asumir los costos que implica la obtención de un token USB.

2. **El usuario recupera de manera segura la información mencionada utilizando un mecanismo de autenticación:** esta opción está especialmente dirigida a las máquinas de acceso público que harán parte del sistema. Esto se debe a que recuperar la llave privada es práctico y seguro únicamente utilizando máquinas preconfiguradas autorizadas y monitoreadas. Dado que almacenar llaves privadas de manera persistente en estas máquinas sería inaceptable en términos de seguridad del sistema, se hace necesario recuperar dicha información cada vez que un usuario utilice estos servicios. Para esta alternativa, se tendrán en cuenta dos mecanismos:

- *Autenticación biométrica por medio de la lectura de la huella dactilar*: este mecanismo representa las mayores ventajas desde el punto de vista de autenticación:
  - ✓ La información biométrica es única a cada persona, además, es intransferible, lo que, junto con las últimas tecnologías de detección de copias falsas en los lectores de huellas dactilares, impediría el robo de dicha información con fines de suplantación.
  - ✓ El usuario no tiene necesidad de memorizar o proteger información de autenticación.

  A pesar de los avances tecnológicos en esta área, los mecanismos biométricos aún manejan una FAR (*False Accept Rate*) que por razones probabilísticas afectaría mucho un sistema con millones de usuarios registrados, identificando como otra persona a diversos usuarios periódicamente. Para evitar este problema, la autenticación biométrica deberá ir precedida por la solicitud del número de cédula del usuario. De esta manera, las probabilidades de ocurrencia de un falso positivo caerían a niveles suficientemente bajos como para no tener en cuenta este problema. Adicionalmente a las máquinas de acceso público, este sistema podrá ser accedido por máquinas previamente autorizadas que presten servicios especiales basados en autenticación por huella dactilar. Ejemplos de estas máquinas pueden encontrarse en sectores como el bancario o en empresas prestadoras de servicios de seguridad general.
- *Autenticación utilizando un número secreto único a cada usuario que sólo es del conocimiento del sistema y del usuario*: por razones de costos y logística, existirán algunos puntos de acceso público que no contarán con mecanismos de autenticación biométrica instalados. Debido a esto, se pondrá a disposición la opción de entregar al usuario un número secreto que lo identifique ante el sistema. De esta manera, el usuario inicialmente ingresará en la máquina su número de cédula, y utilizará el número secreto como contraseña. Este número secreto se entregará impreso en papel, lo que sería altamente beneficioso para el sistema desde el punto de vista de costos.

Evaluación de las Alternativas de Acceso al Sistema

Una vez presentadas las alternativas de acceso al sistema, es momento de entrar a analizar las ventajas y desventajas de cada una bajo diversos puntos de vista.

Consideraciones Generales de Seguridad

El propósito final de un sistema PKI es brindar seguridad a otros sistemas informáticos. Es por esto que el aspecto que se tendrá más en cuenta para evaluar la conveniencia de cada alternativa de acceso será el nivel de seguridad que ofrece. Existen algunas consideraciones generales de seguridad que vale la pena tener en cuenta:

- En caso de que el usuario vaya a tener en su poder de manera permanente su llave privada, es necesario capacitarlo sobre las medidas de seguridad que deben tener

sobre dicha información, las implicaciones de comprometerla y los mecanismos de reporte en caso de comprometerla.

- Si un usuario tiene conocimiento inmediato de que está siendo víctima de un ataque de suplantación, podrá notificar a la autoridad de certificación rápidamente acerca del ataque con el fin de evitar el reconocimiento de las acciones realizadas a su nombre.

- Para contar con un mayor nivel de seguridad en cualquiera de los casos, se realizará cualquier tipo de entrega al usuario se realizará mediante un sobre sellado, requiriendo para la entrega la firma manuscrita del usuario.

- Se considera conveniente mantener las máquinas de acceso público vigiladas permanentemente por cámaras de seguridad para mitigar el riesgo de suplantación de un usuario bajo coacción.

- Los servidores que se encargan de la manejar todo el sistema relacionado con la recuperación de la llave privada a partir de un mecanismo de autenticación, no se encontrarán conectados a Internet, sino únicamente a una red privada a la que se conectará cada máquina de acceso público al sistema, o máquinas adicionales autorizadas previamente.

- La pareja de llaves que se almacena en los tokens USB se genera dentro de los mismos o en un HSM, conectando el token a un puerto USB del HSM para transferir la información. De esta manera se protegerá a nivel de hardware la llave privada, garantizando que nunca se almacenó en texto claro por fuera de dispositivos de almacenamiento seguro.

- Los tokens USB son resistentes a la lectura y modificación no autorizadas de información, sólo se puede intentar destruirla.

- La contraseña que protege un token USB no es vulnerable a ataques de fuerza bruta, ya que el ingreso incorrecto de la misma en un par de intentos bloqueará el dispositivo.

- La llave privada entregada como parte del archivo en formato PKCS#12, será protegida únicamente por la seguridad que ofrezca la contraseña asignada al archivo.

- El mecanismo de autenticación biométrica tiene la gran ventaja de que no genera responsabilidades en cuanto a seguridad por parte del usuario.

- El nivel de protección de la llave privada, en caso de utilizar el mecanismo de autenticación biométrica para recuperarla, será el nivel de seguridad de dicho mecanismo.

- El nivel de protección de la llave privada, en caso de utilizar el mecanismo de autenticación basado en un número secreto para recuperarla, será el nivel de seguridad que el usuario brinde al papel que contiene dicho número.

Los detalles de seguridad de cada alternativa de acceso serán analizados en el Capítulo VI. Análisis de Vulnerabilidades.

Conveniencia para el Usuario

El segundo criterio de mayor importancia luego del nivel de seguridad ofrecido, es la conveniencia para el usuario.

Se presenta a continuación una tabla comparativa de la conveniencia de cada alternativa, respecto a los medios de acceso al sistema:

		Computadores Personales	**Máquinas de Acceso Público**
Token USB		Opción práctica y muy segura para PCs, ya que el PC no requiere almacenar la llave privada.	Estaría disponible esta opción, y no sería complicada de instalar teniendo en cuenta la simplicidad de un puerto USB.
Archivo PKCS#12		Opción práctica y económica para PCs, aunque requieren almacenar la llave privada permanentemente.	No podrá ser utilizado en los medios de acceso público, ya que sería responsabilidad del usuario el ingreso de información confidencial a dichos medios, pero no se puede asumir que el usuario cuenta con mecanismos seguros para ingresar tal información.
Autenticación	**Biométrica**	No es práctico utilizar estas alternativas en PCs, ya que su objetivo final es recuperar la llave privada, y es mucho mejor obtenerla una sola vez y luego mantenerla almacenada.	Esta opción es muy conveniente desde el punto de vista de la capacitación requerida por el usuario, ya que no necesita conocer siquiera de la existencia del sistema PKI. El usuario sólo tiene que saber que necesita autenticarse y que el sistema lo identificará basándose en la información de

			autenticación proveída. Es sencilla de utilizar, a nivel de capacitación bastará con las instrucciones que provea la máquina que el usuario esté utilizando. Además, no genera responsabilidades para el usuario respecto al cuidado de información privada.
	Número Secreto		Esta opción es muy conveniente desde el punto de vista de la capacitación requerida por el usuario, ya que no necesita conocer siquiera de la existencia del sistema PKI. El usuario sólo tiene que saber que necesita autenticarse y que el sistema lo identificará basándose en la información de autenticación proveída. Sin embargo, genera responsabilidades para el usuario respecto al cuidado de información privada.

Tabla 1. Conveniencia de las alternativas de accesibilidad respecto a los medios de acceso al sistema

Implicaciones Logísticas

Las implicaciones logísticas de cada alternativa de acceso son importantes a la hora de pensar en los requisitos de organización, recursos tecnológicos, esfuerzo, tiempo y costos requeridos para el correcto funcionamiento del sistema. Las implicaciones de esta naturaleza más importantes son:

- **Tokens USB:** en caso de que esta sea la única alternativa de acceso elegida por un usuario, el usuario recibirá su token vacío y generará su pareja de llaves dentro del dispositivo. Se requerirá contar con una infraestructura logística que le permita al usuario realizar este procedimiento al mismo tiempo que se conecta a través de Internet con la CA para obtener su certificado digital firmado almacenado dentro de su token.

- **Archivos PKCS#12:** debido a que este archivo debe ser generado antes de ser enviado al usuario, las implicaciones logísticas de esta alternativa incluyen ciertas

complicaciones. Aunque es posible generar en *batch* gran cantidad de archivos PKCS#12, deben existir personas encargadas de almacenar archivo por archivo en un dispositivo de almacenamiento diferente para su posterior envío. La cantidad de personas requerida para hacer este proceso de manera ágil para todos los solicitantes es muy grande.

- **Autenticación Biométrica:** esta es la única opción en la que no es necesario enviarle ningún tipo de información al usuario por medio de un sobre sellado. Esto es una gran ventaja logística y de costos para el sistema. Adicionalmente, a partir de Octubre del presente año, la Registraduría va a contar con la huella dactilar digitalizada de todos los colombianos que posean una cédula, lo cual facilitará inmensamente la puesta en marcha del sistema de autenticación por huella dactilar.

- **Autenticación Basada en Número Secreto:** su ventaja logística radica en que no requiere de la instalación de ningún tipo de hardware especializado en las máquinas de acceso público.

Funcionamiento del Sistema de Recuperación de Llaves Privadas

A continuación se explicará el funcionamiento detallado del sistema encargado de la recuperación de llaves privadas cuando los usuarios decidan acceder al sistema PKI a través de las máquinas de acceso público.

Antes de poder utilizar su certificado digital, el cliente debe contar con su llave privada y su cadena de certificación. Teniendo en cuenta que el sistema planteado contará con una sola CA, la cadena de certificación estará compuesta únicamente por el certificado digital de la CA y el certificado digital del usuario. Por razones de eficiencia, se almacenará en todas las máquinas el certificado digital de la CA, teniéndose que recuperar sólo la llave privada y el certificado digital del usuario de turno.

El sistema de recuperación de llaves privadas será un sistema de servidores que almacenarán información de autenticación (número de cédula de ciudadanía + información biométrica o número secreto), llaves privadas de los usuarios cifradas, y los certificados digitales correspondientes a las llaves privadas.

Para ofrecer un alto nivel de seguridad, toda la información confidencial que intercambien los servidores y las máquinas cliente será cifrada utilizando certificados digitales que representen a cada parte. Adicionalmente, los servidores delegarán todas sus operaciones criptográficas a un sistema de HSMs conectados por red que soporten balanceo de carga, de tal manera que las llaves privadas de los usuarios se encontrarán descifradas únicamente dentro del HSM asignado para la operación.

De esta manera, en el momento de la emisión del certificado digital del cliente, un HSM se encargará de la creación de la pareja de llaves del usuario, la creación y firma del certificado digital correspondiente, y el envío de la llave privada cifrada y el certificado

digital no cifrado a los servidores que contienen la base de datos con la información de autenticación correspondiente.

Todo el proceso de recuperación de la llave privada funcionará de la siguiente manera:

1. El usuario ingresa su información de autenticación en la máquina que esté utilizando.
2. La máquina envía dicha información al sistema de servidores, cifrándola con la llave pública del certificado digital que identifique al sistema de servidores.
3. El sistema de servidores descifra la información de autenticación con su llave privada, y ubica en su base de datos la llave privada cifrada del usuario junto con su certificado digital. La llave privada cifrada es enviada a uno de los HSMs, los cuales son los únicos que contienen la llave de cifrado que puede descifrarla.
4. El HSM encargado de la operación descifra la llave privada del usuario, y la cifra de nuevo utilizando la llave pública de la máquina donde se encuentra el usuario.
5. La máquina donde se encuentra el usuario recibe la llave privada cifrada del usuario más su certificado digital correspondiente.
6. La máquina cliente utiliza su llave privada para descifrar la llave privada del usuario. Además, construye la cadena de certificación del certificado digital del usuario, al contar previamente con el certificado digital de la CA. A partir de este momento el usuario está en capacidad de utilizar su certificado digital. Por razones de seguridad, en ningún momento la máquina cliente almacenará la llave privada del usuario en medios persistentes. Esta llave privada deberá ser totalmente borrada de la memoria de la máquina una vez el usuario abandone la máquina.

Es importante notar que el sistema está diseñado para que la llave privada de los usuarios jamás sea almacenada en texto claro en máquina alguna. De esta manera, el nivel de seguridad con el que cuentan las llaves privadas va a ser muy alto.

Sistema Distribuido que Conforma la Autoridad de Certificación

A continuación se presentarán los aspectos más importantes de la arquitectura del sistema distribuido que conformará la CA. Para este sistema, se asumirá la utilización de la autoridad certificadora EJBCA, la cual es la única autoridad certificadora *open source* que tiene antecedentes de casos de éxito en implantaciones a gran escala. EJBCA es una CA basada en la tecnología de EJBs, perteneciente a la tecnología J2EE.

Balanceo de Carga

Con el fin de identificar las necesidades de balanceo de carga con que cuenta la CA, se procederá inicialmente a identificar los casos de uso de la CA, y luego se plantearán las alternativas de implementación de balanceo de carga en el sistema.

Identificación de Casos de Uso

Inicialmente, es útil identificar los principales componentes de EJBCA y detectar los casos de uso que puedan implicar alta concurrencia y que por lo tanto requerirán de la implementación de balanceo de carga.

A continuación se presenta una arquitectura simplificada para el deployment de EJBCA:

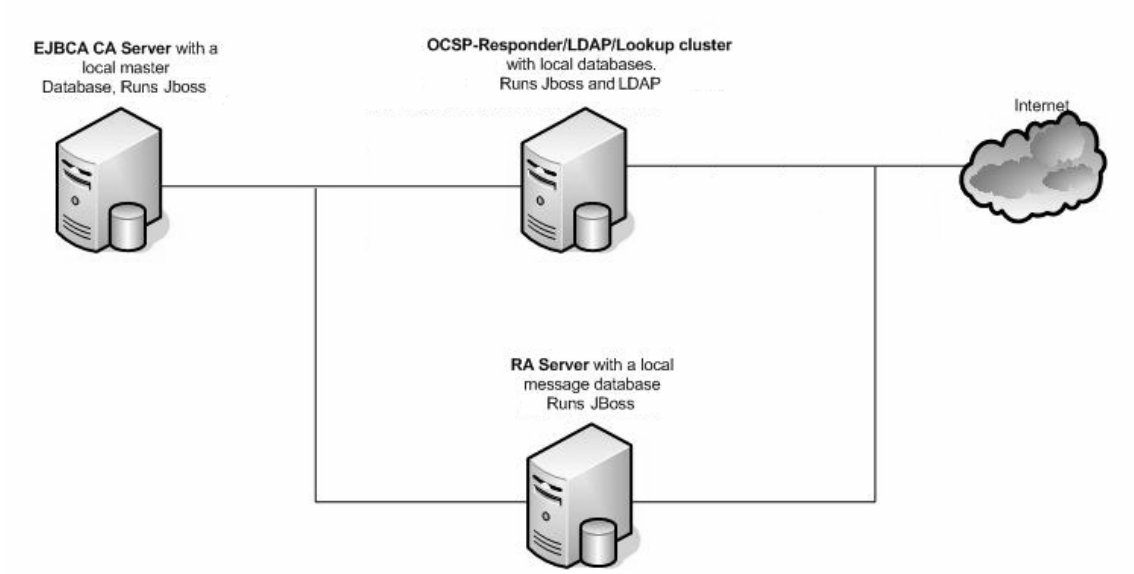

Figura 1. Arquitectura simplificada para el deployment de EJBCA

Como se puede observar en la figura, son tres los principales componentes arquitectónicos de EJBCA, los cuales preferiblemente deben ser instalados en servidores independientes. A continuación se repasarán los principales casos de uso de cada uno de estos componentes, identificando aquellos que impliquen una alta concurrencia en un esquema a gran escala:

- **CA:** su principal función desde el punto de vista de los usuarios es emitir certificados digitales. Para este fin, se utilizarán los HSMs mencionados en el sistema de recuperación de llaves privadas, los cuales harán balanceo de carga entre sí.

- **RA:** implementa dos casos de uso importantes:
  - Registrar una nueva *end entity*: para dicho fin, es accedida por los administradores del sistema. En este caso de uso, la concurrencia no es alta.
  - Consultar la existencia de una *end entity*: para dicho fin, es accedida por la CA para generar los nuevos certificados digitales. Esta operación será realizada en *batch* periódicamente por la CA, por lo cual no requerirá de balanceo de carga.

- **OCSP Responder/LDAP Publisher:** este es el componente de la CA que debe soportar la más alta concurrencia, ya que ofrece el servicio de verificación de la

validez/estado de un certificado digital, el cual es el servicio más solicitado en una CA. Por esta razón, este componente de la CA requerirá de balanceo de carga. Además de tener la tarea de atender las peticiones OCSP, este componente contiene un repositorio LDAP para publicar los certificados digitales del sistema (de ahí su nombre "LDAP Publisher"), el cual funcionará de manera independiente al repositorio utilizado en el sistema de recuperación de llaves privadas.

Alternativas de Balanceo de Carga

Existen alternativas para manejar el balanceo de carga, de acuerdo a criterios no técnicos relacionados con la *end entity* como la ubicación (ciudad, por ejemplo), el tipo (organización, persona, servidor, etc.), entre otros, pero generalmente no es apropiado implementar este tipo de estrategias, ya que hacen el balanceo de carga menos homogéneo y por lo tanto menos eficiente.

Por otra parte, si se implementan alternativas relacionadas con criterios técnicos (capacidades del hardware de cada servidor, ancho de banda de las conexiones entre servidores, etc.), el balanceo de carga se realiza de acuerdo a las capacidades de atención de concurrencia de cada servidor, lo cual es una estrategia que ofrece una alta eficiencia. Este va a ser el criterio a aplicar para el balanceo de carga del sistema, el cual será realizado por parte de HSMs para la CA, y utilizando las funcionalidades de clustering y balanceo de carga con que cuentan JBoss y OpenLDAP para el OCSP Responder/LDAP Publisher. Esto implica la utilización de una granja de servidores en el OCSP Responder/LDAP Publisher.

Replicación y Consistencia

En la presente sección se identificarán los componentes de software que requerirán manejo de replicación y consistencia para lograr un buen funcionamiento de EJBCA a gran escala.

Tomando como punto de partida los requerimientos de balanceo de carga identificados anteriormente, se definirán los requerimientos de replicación y consistencia para cada componente arquitectónico de EJBCA:

- **HSMs en la CA:** realizarán balanceo de carga para la emisión de certificados digitales, la cual, como se mencionó anteriormente, estará conformada los siguientes pasos:
    1. Creación de la pareja de llaves del usuario.
    2. Creación y firma del certificado digital correspondiente.
    3. Envío de la llave privada cifrada y el certificado digital no cifrado a los servidores que contienen la base de datos con la información de autenticación correspondiente.

  Este componente es susceptible a una alta concurrencia en el procesamiento de información (especialmente debido a la generación de parejas de llaves), mas no en el manejo de información persistente (almacena principalmente información de control, la mayoría de la información importante es almacenada en los servidores del sistema de recuperación de llaves privadas y el directorio LDAP). Dadas estas características, sólo será necesario el manejo de replicación y consistencia de

información volátil, lo cual ya viene implementado en las funcionalidades de balanceo de carga de los HSMs.

- **Cluster JBoss y OpenLDAP en los OCSP Responders/LDAP Publishers:** este componente maneja principalmente información persistente: certificados digitales junto con información acerca del estado de validez de los mismos. Esta información tendrá una altísima concurrencia a nivel de lectura (servicio de verificación de la validez/estado de un certificado digital), aunque también a nivel de escritura (cuando la CA envía información actualizada correspondiente al OCSP Responder/LDAP Publisher) pero en menor medida. Dada esta mayor proporción a nivel de lectura, se implementará un esquema maestro-esclavos.
  No obstante, en este caso particular, la alternativa elegida no se adapta idealmente a los requerimientos, ya que de todas maneras se presentará una alta concurrencia a nivel de escritura, lo cual puede generar un cuello de botella. Por esto, se podría pensar en utilizar una estrategia multi-maestro con sólo dos réplicas (ya que mejorarían la eficiencia para escritura, y a la vez, el efecto del manejo de consistencia sobre la eficiencia no sería tan grande), pero esta alternativa generaría complicaciones ya que la publicación de información acerca del estado de validez de los certificados digitales requiere un altísimo nivel de consistencia, lo que obligaría a sincronizar las copias con demasiada frecuencia y, una vez más, perjudicar grandemente la eficiencia del servicio.
  En importante anotar que OpenLDAP cuenta con funcionalidades maestro-esclavos ya implementadas.

Seguridad

Con el fin de prevenir que los servidores de la autoridad certificadora sean víctima de posibles ataques, se utilizarán firewalls e IPSs (Sistemas de Prevención de Intrusos) tal como lo muestra la figura:

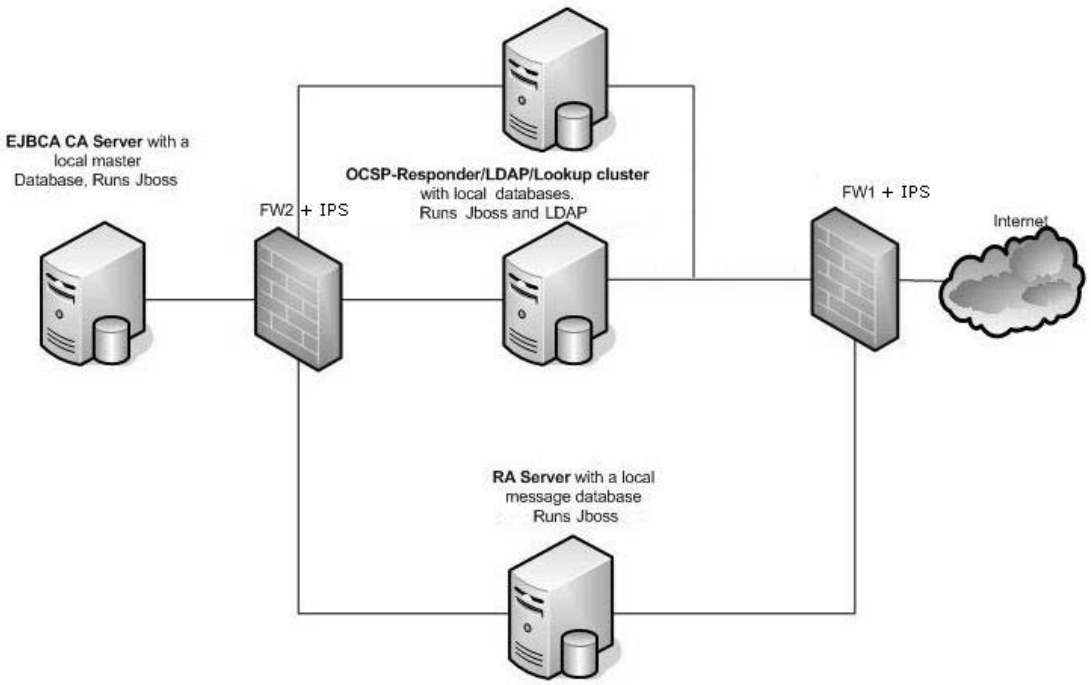

Figura 2. Arquitectura de seguridad de red para el deployment de EJBCA

Algunos detalles de configuración para tener en cuenta son:

- FW1 debe permitir la conexión con el RA Server sólo a las máquinas de los administradores de la RA.
- FW2 no debe permitir la conexión con el CA Server. La manera como el CA Server debe funcionar es consultando los datos del RA Server, y leyendo/escribiendo datos en los OCSP Responders/LDAP Publishers, pero en ningún momento recibiendo peticiones. Por otra parte, FW2 debe también permitir el acceso al RA Server y a los OCSP Responders/LDAP Publishers sólo al CA Server.
- Naturalmente, los firewalls no únicamente deberán restringir acceso por IP, sino por puerto, y los servidores sólo deberán tener abiertos los puertos estrictamente necesarios.
- Los IPS deberán proceder de la siguiente manera cuando detecten un intento de intrusión: Deben realizar un *reset* a la conexión sospechosa, y reconfigurar automáticamente el firewall correspondiente para que impida accesos futuros del sospechoso. Igualmente, los IPS serán configurados para detectar y prevenir ataques de DoS.
- El acceso físico a todos los servidores será posible sólo para los administradores del sistema.
- Los servicios de administración serán posibles sólo por medio de SSL con doble autenticación.

Tolerancia a Fallas y Alta Disponibilidad

A continuación se presentará la arquitectura de tolerancia a fallas y alta disponibilidad para la CA. Primero se hará énfasis en los componentes funcionales del sistema, para luego tratar los componentes no funcionales más importantes, es decir, los dispositivos que actúan sobre la red.

Componentes Funcionales del Sistema

Los componentes funcionales de la autoridad certificadora (CA, RA y OCSP Responders/LDAP Publishers) contienen toda la información altamente crítica para dicho sistema. Por esta razón, es necesario implementar diversos mecanismos de protección sobre estos componentes para permitir que la autoridad certificadora cuente con un altísimo nivel de tolerancia a fallas y disponibilidad. A continuación, se presenta una tabla que describe los tipos de fallas que pueden sufrir estos componentes, junto con la implementación de tolerancia a fallas y alta disponibilidad propuesta para cada una:

Tipo de Falla	¿Cómo Afecta la Información?	Propuesta de Implementación
Fallas de Hardware: Fallas en el funcionamiento correcto de los componentes de hardware de los servidores.	- Modifican o eliminan la información. - Impiden el acceso a la información.	Instalar todos los componentes funcionales de la autoridad certificadora en servidores que cuenten con mecanismos a prueba de fallas de hardware, como manejo de integridad y redundancia. Contar adicionalmente con piezas de hardware de reemplazo listas para dichas máquinas en caso de presentarse daños.
Fallas en el servicio de energía eléctrica.	Impiden el acceso a la información.	Contar con mecanismos que garanticen un flujo de energía eléctrica constante para todos los servidores, como plantas eléctricas y UPSs.
Fallas que son consecuencia de daños a la integridad física de las máquinas: Estas fallas pueden ser resultado de eventos como desastres naturales o intentos de	- Eliminan la información. - Impiden el acceso a la información.	Contar con copias idénticas de los servidores, las cuales se deben encontrar en ubicaciones apartadas entre sí, tanto desde el punto de vista geográfico, como del punto de vista de la red a la

sabotaje al sistema.		que se conectan.
Caídas o fallas en la red a la que se conectan las máquinas.	Impiden el acceso a la información.	Todas las copias deben contar con los mismos mecanismos de seguridad y tolerancia a fallas. En el caso de la CA y la RA, sería suficiente con tener dos copias, mientras que en el caso de los OCSP Responders/LDAP Publishers, si se considera que *n* es la cantidad de servidores necesarios en el cluster para prestar este servicio de manera eficiente, se deberán tener *n* servidores en una ubicación, y *n* en otra.

Tabla 2. Tipos de fallas que pueden sufrir los componentes funcionales de la CA

Nota: Cuando se realizó la propuesta de balanceo de carga para el sistema, se decidió no contar con balanceo de carga en los servidores CA y RA, más allá de que se propuso un sistema de balanceo de carga asociado con el componente CA. Sin embargo, implementar un cluster JBoss para las 2 copias de la CA/RA sería conveniente porque brindaría transparencia respecto a los clientes de estos dos servicios (en un cluster, las máquinas que lo componen actúan como si fueran una sola, lo cual es uno de los objetivos primordiales de un sistema distribuido). Este mismo concepto es útil para las *2n* copias de los OCSP Responders/LDAP Publishers, haciéndolas parte de un solo cluster aunque se encuentren divididas en 2 ubicaciones apartadas. De esta manera, el cluster JBoss se encargaría de la actualización constante de todas las copias, así como de detectar caídas de los servidores que lo componen, ya que cuenta con un sistema de chequeos de salud.

Dispositivos que Actúan Sobre la Red

Una vez planteados los mecanismos de tolerancia a fallas de los componentes funcionales del sistema, es importante diseñar soluciones que garanticen un acceso constante a dichos componentes. Para tal fin, es necesario implementar mecanismos de tolerancia a fallas para los dispositivos que actúan sobre la red (routers, firewalls, IPSs, etc.). El mecanismo más práctico para lograr este objetivo, es contar con dos rutas de acceso diferentes a cualquiera de los componentes funcionales, las cuales deben tener los mismos componentes e idéntica estructura. Adicionalmente, es necesario utilizar un sistema de monitoreo constante de todos los dispositivos de red, el cual debe incluir generación automática de alertas que permitan al administrador de la red enterarse de manera inmediata de las fallas que se presenten.

Debido a que los dispositivos que actúan sobre la red no almacenan información crítica desde el punto de vista funcional del sistema, no es necesario mantener actualizada en tiempo real la información que almacenan. Sin embargo, para los dispositivos de seguridad (firewalls e IPSs), es importante realizar con mucha frecuencia una copia de las reglas de seguridad creadas automáticamente como respuesta a intentos de ataques.

VI. Análisis de Vulnerabilidades

Con el fin de identificar de una mejor manera los niveles de seguridad que provee cada alternativa de acceso al sistema, se realizará el análisis de vulnerabilidades utilizando la metodología STRIDE, que se encarga de clasificar las amenazas de acuerdo a sus efectos, y de esta manera, identificar el nivel de riesgo sobre el sistema que implica cada amenaza. Para esto, se procederá inicialmente a identificar el nivel de riesgo que implica cada tipo de efecto sobre el sistema según STRIDE, para luego enfocarse en los ataques más peligrosos que pueden vulnerar el sistema de certificación digital a través de sus alternativas de acceso.

Nivel de Riesgo de los Tipos de Efectos sobre el Sistema

Antes de analizar las amenazas individualmente, es importante identificar el nivel de riesgo que implica cada tipo de efecto sobre el sistema según STRIDE:

- **Spoofing:** teniendo en cuenta que en el sistema PKI planteado un certificado digital tendría reconocimiento legal como identificador de una persona, en la medida en que un adversario logre perpetrar un ataque de spoofing, éste se encontrará en total capacidad de realizar cualquier actividad en nombre de otra persona. Las consecuencias de dicho ataque dependerían de la aplicación particular que utilice el sistema PKI, pero teniendo en cuenta que el sistema puede ser utilizado para gran variedad de fines que requieran seguridad informática, existirán muchos casos particulares en los que las consecuencias de la suplantación pueden llegar a ser supremamente graves. Ejemplos de estos son: suplantación de la firma en contratos o documentos, autorización de transferencias de dinero, fraude electoral, realización de actos de mala fe en nombre de otra persona, etc.

- **Tampering:** la eliminación de información de autenticación generaría una pérdida temporal del acceso al servicio por parte del usuario afectado, mientras obtiene nuevos datos de autenticación. Esto no representa grandes inconvenientes. Sin embargo, si lo que se afecta es la llave privada, y no existe un mecanismo para recuperarla, el usuario perderá toda la información que haya almacenado cifrada con su llave pública, lo cual puede tener consecuencias muy graves según el caso. Por esta razón, es importante concientizar al usuario de utilizar otro mecanismo de protección de la información almacenada, diferente al cifrado con la llave pública, en caso de que esta información sea muy importante.

- **Repudiation:** todas las operaciones que se realicen con la llave privada tendrán la propiedad de la no repudiación, por esta razón, este tipo de ataques no será posible en el sistema.

- **Information Disclosure:** la obtención de la información de autenticación, o de la llave privada por parte de una persona diferente a su dueño, permitirá a esa persona suplantarlo, conllevando todas las posibles consecuencias ya mencionadas.

- **Denial of Service:** este tipo de ataques afectará únicamente a los usuarios de sistemas que no cuenten con un sistema de respaldo que no utilice tecnología PKI. Para que este sistema de respaldo tenga la misma validez jurídica que el sistema PKI, debe involucrar firmas manuscritas y/o otros medios de identificación legalmente reconocidos.

- **Elevation of Privilege:** las consecuencias de un ataque de este tipo dependen de la aplicación particular que utilice el sistema PKI. Sin embargo, para este análisis, nos estamos enfocando en la parte de autenticación, y en los sistemas de autenticación, un ataque de elevation of privilege siempre implica spoofing, así que se puede asumir que las consecuencias son del mismo tipo en ambos casos.

Luego de repasar el nivel de riesgo que implica cada tipo de efecto de amenaza en el sistema, se puede concluir que las amenazas que generan spoofing son las más peligrosas, mientras que las amenazas que generan otro tipo de efectos tienen repercusiones no muy críticas.

Por esta razón, la única amenaza realmente delicada relacionada con las alternativas de acceso al sistema, es el acceso por parte de otra persona, ya sea temporal o permanente, a la llave privada de un usuario.

Ataques que Pueden Vulnerar el Sistema

Existen diversos ataques que podrían permitir la suplantación de un usuario, según la alternativa de acceso al sistema:

- Un adversario obtiene el token USB de un usuario junto con su contraseña: siempre y cuando el usuario no tenga la contraseña anotada en algún lugar de fácil acceso, este ataque será muy difícil de realizar sin el conocimiento inmediato de la víctima. Teniendo en cuenta la posibilidad que tiene el usuario de asignar esta contraseña, la capacitación de seguridad que recibe antes de obtener el token, y la práctica invulnerabilidad de la contraseña a ataques de fuerza bruta, se considerará necesario por parte del atacante obtener la contraseña, o tener un altísimo conocimiento de las estrategias de asignación de contraseñas de su víctima.

- Un adversario obtiene el archivo en formato PKCS#12 de un usuario, junto con su contraseña: este ataque es más probable que el anterior debido a que esta contraseña es asignada por el sistema, tendiendo así el usuario a anotarla en un lugar accesible más fácilmente. Adicionalmente, las contraseñas de los archivos PKCS#12 sí son vulnerables a ataques de fuerza bruta.

- Un adversario logra acceso a los servidores del sistema de recuperación de llaves privadas: esto requiere alguna forma de acceso a la red privada a la que estarán conectadas estas máquinas, o requeriría de acceso físico a las mismas. No se considerará muy probable este ataque teniendo en cuenta todos los obstáculos que supondrían ambas maneras de acceder a dichos servidores y los mecanismos de protección ante las mismas que se planean tener.

- Un adversario obtiene el número secreto de un usuario para acceder al sistema: este ataque se considerará el más factible de llevar a cabo, teniendo en cuenta que el usuario es responsable de la protección de la confidencialidad de dicho número, existiendo una inmensa mayoría de casos en los que el usuario no está en capacidad de garantizar un buen nivel de seguridad a dicha información. Adicionalmente, para hacer este ataque realidad, el adversario deberá obtener el número de cédula de su víctima, pero esta tarea es aun más fácil que obtener el número secreto.

VII. Conclusiones, Recomendaciones y Trabajos Futuros

En este capítulo final se mencionarán las conclusiones más importantes del trabajo realizado, junto con recomendaciones a tener en cuenta para la implementación del esquema de certificación digital masiva, y trabajos futuros propuestos para complementar dicho esquema.

Conclusiones

A continuación se presentan las principales conclusiones del trabajo realizado:

- Se identificó la presencia en nuestro país, en la actualidad, de suficientes elementos de soporte legales, logísticos, y tecnológicos como para llevar a cabo la puesta en marcha de un esquema de certificación digital masiva.

- Las condiciones particulares identificadas en nuestro país impiden la implementación de esquemas de certificación digital que ofrezcan máximos niveles de seguridad, ya que esto implicaría la asignación de un dispositivo de hardware criptográfico a cada usuario, lo cual es un imposible logístico y económico en el presente.

- Las capacidades del esquema planteado no pueden ser aprovechadas de la mejor manera en el presente, debido a la poca accesibilidad de los colombianos a computadores personales de manera gratuita.

- Los retos más grandes que se pueden presentar en el momento de implementar un esquema de certificación digital a gran escala están relacionados con la parte logística. Asimismo, la parte técnica de la implementación no parece conllevar dificultades importantes.

- Las tecnologías de software con que cuentan las autoridades certificadoras han evolucionado suficientemente como para soportar *deployments* a gran escala, evitándose la necesidad de desarrollar nuevas tecnologías de software para tal fin.

- Las amenazas de seguridad más peligrosas para el sistema son las que permiten lograr la suplantación de un usuario, ya que tendrían consecuencias similares a las que se presentan cuando alguien está en capacidad de suplantar a otra persona a través del documento de identidad y/o la firma manuscrita.

Recomendaciones y Trabajos Futuros

Existe una serie de recomendaciones y trabajos futuros que serían importantes de llevar a cabo para complementar el trabajo realizado:

- Realizar una investigación para identificar las restricciones prácticas de asignar a la Registraduría Nacional del Estado Civil la tarea de administrar la autoridad de registro del sistema.

- Evaluar y trabajar sobre la posibilidad de que el esquema incluya infraestructura que permita acceder al mismo a través de dispositivos móviles de manera masiva.

- Realizar el planteamiento a gran escala de un sistema de archivo y conservación de información de manera segura.

- Realizar pruebas de rendimiento sobre un *deployment* a pequeña escala del esquema de certificación digital propuesto, y proceder con los ajustes necesarios en el planteamiento de la implementación, de acuerdo a los resultados que se presenten en dichas pruebas de rendimiento.

- Realizar un análisis más exhaustivo del esquema planteado desde el punto de vista legal, con la asesoría de abogados expertos en el tema.

- Definir fases de implementación del esquema planteado, incluyendo la cobertura y servicios ofrecidos en cada fase.

- Plantear la implementación de servicios de uso masivo que aprovechen la infraestructura tecnológica y logística que ofrece el sistema PKI de acceso masivo.

Glosario

Autoridad de Certificación Raíz. Autoridad de certificación cuyo certificado digital está firmado por sí misma.

CA. (o AC en español). Acrónimo de "Certificate Authority" o "Autoridad de Certificación" en español.

Cadena de Certificación. (o Ruta de Certificación). Lista de certificados digitales que inicia con un certificado que se quiere validar, y continúa con los certificados digitales de autoridades de certificación intermedias, en las que cada autoridad de certificación firmó el certificado digital de su antecesora en la lista. La lista finaliza con el certificado digital de una autoridad de certificación raíz.

Certificado Raíz. Certificado digital que pertenece a una Autoridad de Certificación Raíz.

End Entity. Entidad que puede recibir, pero no firmar un certificado digital. Estos son los usuarios del sistema como tal, los cuales pueden representar personas, organizaciones, servidores, Web browsers, etc.[16]

IPS. (*Intrusion Prevention System*). Dispositivo encargado de ejercer control de acceso basado en el contenido a nivel de aplicación de los paquetes que viajan por la red, con el fin de proteger contra intrusos un sistema.

PKCS#12. (*Public Key Cryptography Standards #12*). Estándar que define un formato de archivo utilizado comúnmente para almacenar información privada. Su uso más frecuente es el almacenamiento de llaves privadas junto con su cadena de certificación asociada. La información que contiene el archivo se encuentra cifrada, utilizándose frecuentemente una llave criptográfica derivable de una contraseña que ingresa el usuario para descifrar la información.

Protegido por Hardware. Nivel de seguridad de la información, en el cual se considera que dicha información sólo se ha encontrado descifrada dentro de dispositivos de hardware seguros.

RA. (o AR en español). Acrónimo de "Registration Authority" o "Autoridad de Registro" en español.

XML Encryption. Estándar que define mecanismos para el ciframiento de archivos XML.

[16] Tomado de: PrimeKey Solutions AB. Terminology / Abbreviations. *Online Documentation*. Recuperado el 25 de Septiembre de 2006, de http://docs.primekey.se/documentation/en/new-terms.html

XML Signature. (o XMLDsig). Estándar que define una sintaxis XML para firmas digitales, el cual es utilizado generalmente para firmar archivos XML.[17]

[17] Tomado de: *XML Signature*. (2006, Diciembre 25). Recuperado el 14 de Enero de 2007, de http://en.wikipedia.org/wiki/XML_Signature

Referencias

Agenda de Conectividad. (2006, Diciembre 13). *¿Qué es la Agenda?*. Recuperado el 13 de Enero de 2007, de http://www.agenda.gov.co/BulletinBoard/view_one.cfm?MenuID=5002&ID=146

Case Study Spotlight: Hong Kong Post's e-Cert Smart ID Card Project. (2005, Agosto). Recuperado el 20 de Septiembre de 2005, de http://www.ptc.upu.int/pi/pi_cstudy.shtml

Decreto 1747 de 2000 Nivel Nacional. (2000, Septiembre 11). Recuperado el 31 de Octubre de 2006, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4277

Digital Signature Infrastructure For Administrative Simplification And E-Commerce Development (DIGISEC). (2005, Junio 14). Recuperado el 20 de Septiembre de 2005, de http://dbs.cordis.lu/fep-cgi/srchidadb?ACTION=D&CALLER=PROJ_IST&QF_EP_RPG=IST-1999-20981

Gigli, J. (2006, Enero 10). *España: Interior comienza a implantar este año el nuevo DNI electrónico*. Recuperado el 19 de Octubre de 2006, de http://www.gobiernoelectronico.org/node/227

Ley 527 de 1999. Recuperado el 26 de Octubre de 2006, de http://www.secretariasenado.gov.co/leyes/L0527_99.HTM

PrimeKey Solutions AB. Terminology / Abbreviations. *Online Documentation*. Recuperado el 25 de Septiembre de 2006, de http://docs.primekey.se/documentation/en/new-terms.html

Sentencia C-831/01. (2001, Agosto 8). Recuperado el 6 de Enero de 2007, de http://web.minjusticia.gov.co/jurisprudencia/CorteConstitucional/2001/Constitucionalidad/C-831-01.htm

XML Signature. (2006, Diciembre 25). Recuperado el 14 de Enero de 2007, de http://en.wikipedia.org/wiki/XML_Signature

Bibliografía

Agenda de Conectividad. (2006, Diciembre 13). *Intranet Gubernamental - Indicadores de avance*. Recuperado el 13 de Enero de 2007, de http://www.agenda.gov.co/BulletinBoard/view_one.cfm?MenuID=5002&ID=125

Agenda de Conectividad. (2007, Enero 3). *Intranet Gubernamental*. Recuperado el 13 de Enero de 2007, de http://www.agenda.gov.co/BulletinBoard/view_one.cfm?MenuID=5002&ID=121

Certificate authority. (2007, Enero 11). Recuperado el 13 de Enero de 2007, de http://en.wikipedia.org/wiki/Certificate_authority

Certification path validation algorithm. (2006, Febrero 12). Recuperado el 14 de Enero de 2007, de http://en.wikipedia.org/wiki/Certification_path_validation_algorithm

Colombianos con cédula antigua, deben renovarla. Recuperado el 7 de Enero de 2007, de http://www.registraduria.gov.co

DECRETO NUMERO 2170 DE 2002. (2002, Septiembre 30). Recuperado el 6 de Enero de 2007, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4277

Ford, W., Hallam-Baker, P., Fox, B., Dillaway, B., LaMacchia, B., Epstein, J., Lapp, J. (2001, Marzo 30). *XML Key Management Specification (XKMS)*. Recuperado el 28 de Septiembre de 2005, de http://www.w3.org/TR/xkms/

Glossary. Recuperado el 14 de Enero de 2007, de http://www.pki.vt.edu/help/glossary.html

Housley, R., RSA Laboratories, Polk, W., NIST, Ford, W., VeriSign, Solo, D. & Citigroup. (2002, Abril). *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. Recuperado el 14 de Enero de 2007, de http://tools.ietf.org/html/rfc3280

Imamura, T., Dillaway, B., Simon, E. (2002, Diciembre 10). *XML Encryption Syntax and Processing*. Recuperado el 11 de Octubre de 2005, de http://www.w3.org/TR/xmlenc-core/

Information Security Glossary. Recuperado el 28 de Diciembre de 2006, de www.primode.com/glossary.html

Intrusion-prevention system. (2007, Enero 12). Recuperado el 15 de Enero de 2007, de http://en.wikipedia.org/wiki/Intrusion-prevention_system

Mactaggart, M. (2001, Septiembre 1). *Enabling XML security: An introduction to XML*

encryption and XML signature. Recuperado el 13 de Septiembre de 2005, de http://www-128.ibm.com/developerworks/security/library/s-xmlsec.html

Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, C. (1999, Junio). *Request for Comments: 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*. Recuperado el 28 de Septiembre de 2005, de http://www.ietf.org/rfc/rfc2560.txt

nCipher. (2003, Octubre). *NCIPHER netHSM TECHNICAL ARCHITECTURE*. Recuperado el 4 de Diciembre de 2006, de http://www.ncipher.com/uploads/resources/nethsm_arch_issue_1.pdf

nCipher. (2006). *netHSM™ NETWORK-CONNECTED HARDWARE SECURITY MODULE (HSM)*. Recuperado el 4 de Diciembre de 2006, de http://www.ncipher.com/uploads/resources/nethsm.pdf

OSS Nokalva, Inc. (2006). *BioFoundry® Glossary*. Recuperado el 2 de Enero de 2007, de www.biofoundry.com/resources/glossary.html

Preguntas y respuestas frecuentes del Proyecto de Modernización Tecnológica, y renovación de cédulas antiguas. Recuperado el 7 de Enero de 2007, de http://www.registraduria.gov.co/docs/faq_pmt2.doc

Public key infrastructure. Recuperado el 28 de Diciembre de 2006, de http://en.wikipedia.org/wiki/Public_Key_Infrastructure

RSA Laboratories. (1999, Junio 24). *PKCS 12 v1.0: Personal Information Exchange Syntax*. Recuperado el 5 de Diciembre de 2006, de ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf

Sentencia C-662/00. (2000, Junio 8). Recuperado el 6 de Enero de 2007, de http://bib.minjusticia.gov.co/jurisprudencia/CorteConstitucional/2000/Constitucionalidad/C-662-00.htm

Timestamp. (2007, Enero 11). Recuperado el 14 de Enero de 2007, de http://en.wikipedia.org/wiki/Digital_timestamping

Ubuntu Documentation Project. (2006). *Ubuntu Server Guide*. Recuperado el 15 de Septiembre de 2006, de https://help.ubuntu.com/6.06/pdf/ubuntu/C/serverguide.pdf

What is OCSP?. Recuperado el 28 de Septiembre de 2005, de http://www.openvalidation.org/whatisocsp/whatocsp.htm

Williams, P. (1999, Junio 9). *Certificate Validation and the Online Certificate Status Protocol*. Recuperado el 28 de Septiembre de 2005, de http://www.cacr.math.uwaterloo.ca/conferences/1999/isw-june/williams.ppt