Universidad del Salvador
Maestría en Auditoría de Sistemas
Trabajo Final

Director: Dr. Fernández
Coordinadora: Lic.Karina Sartor

PKI

INFRAESTRUCTURA DE CLAVE PUBLICA

TRANSACCIONES ELECTRONICAS SEGURAS

Autor: C.P.N. LUIS ANTONIO GODOY

CONTENIDO

Objetivo de la tesis

El objetivo del presente trabajo es realizar una investigación sobre Infraestructura de Clave Pública, conocida por sus siglas en inglés, PKI, estableciendo cuales son sus componentes, el mecanismo de su funcionamiento, llegar con alguna aproximación al estado actual del desarrollo del conocimiento y las posibilidades de aplicación en nuestro medio.

Se trata de un tema sobre el cual se pone, en la actualidad, gran atención por las posibilidades que el mismo brinda para lograr seguridad en las comunicaciones electrónicas, las que van siendo utilizadas, como medio de desarrollo para las operaciones empresarias, en general y para aquellas que pertenecen al ámbito oficial de gobierno.

Existen en la actualidad, trabajos realizados en doctrina sobre el tema, asi como también desarrollos, realizados por las compañias que ofrecen soluciones tecnológicas para su implementación, en Internet o en el ámbito de ésas compañias, las que en algunos casos se encuentran vinculadas a las grandes consultoras de servicios de la especialidad.

Se busca en el presente trabajo, dar una visión coherente de los puntos principales que definen la tecnologia que sustenta el concepto PKI, como asimismo, analizar la posibilidad de aplicación, en nuestro pais, en el área de Administración Tributaria, a partir de la observación del desarrollo en otro pais donde la técnica se utiliza para dar solución a los problemas que plantea la recaudación.

Los aspectos a clarificar, en los que se busca el valor del presente trabajo, además de la posibilidad de aplicarlo en áreas concretas, son los que hacen a su especificidad, intentándose con el desarrollo, brindar una comunicación comprensible de los aspectos de indole técnica, los que tienen gran complejidad.

Es intención del autor brindar un aporte a profesionales, estudiantes o personas interesadas en el tema como una guia de comprensión, para iniciarse en el conocimiento del tema tratado.

Fundamentación y viabilidad de la investigación

La posibilidades y utilidades que surgen de la aplicación de una Infraestructura de Clave Pública (PKI), ha concentrado sobre el tema, una importante cantidad de atención en los últimos años.

La firma digital derivada de la aplicación de la mencionada infraestructura plantea una nueva forma de utilización de la comunicaciones electrónicas. Surge de esta utilización la necesidad de contar con un entorno seguro y confiable para la realización de las mismas.

En nuestro país, se cuenta con resoluciones y decretos, que aceptan la aplicación de la firma digital y un proyecto de ley que cuenta con media sanción y actualmente es analizado para su aprobación definitiva.

La expectativa generada por la aplicación de esta tecnología, tanto en la compañías tecnológicas especializadas en el tema, como en los medios empresarios y administrativos - gubernamentales, es de gran magnitud, lo que le asigna al tema una gran trascendencia y actualidad.

La aceptación de la firma digital y el correspondiente marco legal de resguardo, permitirá la generación y circulación de documentos digitales, seguros y no repudiables, posibilitando la eficientización de las operaciones administrativas en distintos campos de la administración pública y en un futuro inmediato en el ámbito de las empresas privadas.

El autor se identifica con estas corrientes de opinión y en lo personal, dada su formación profesional y su vivencia en el campo laboral, en el que se desempeña en tareas de Auditorías Contables, Asesoramientos Impositivos y Consultoría, considera que una de las aplicaciones, en el ámbito de la Administración Pública, en las cuales la investigación debería intensificarse, es la del área de la administración tributaria. Por este motivo al considerar una posible aplicación ha elegido la mencionada, a partir de la observación de experiencias realizadas en otros países.

La factibilidad de la realización de la presente investigación, es considerada por el autor a partir de la calidad del material bibliográfico obtenido, principalmente a través de Internet y del material que recibió en la maestría en los diferentes módulos y en el específico de Investigación en Auditoría.

Introducción

El auge alcanzado por las comunicaciones electrónicas y consecuentemente por las transacciones económicas, basadas en ellas, derivadas de operaciones comerciales y empresarias, ha conseguido despertar un enorme interés por dotar a las mismas de condiciones fundamentales de seguridad, que las haga confiable y aumentar el volúmen de negocios canalizados por este medio.

También en las esferas vinculadas a los asuntos oficiales de gobierno, en áreas relacionadas con la administración de justicia, con la organización de las recaudaciones tributarias, y para las distintas operaciones de la administración pública, se están volcando esfuerzos e inversiones, para adecuar las normativas legales de sustento y las estructuras operativas.

Estos esfuerzos por hacer más accesibles a las comunicaciones electrónicas en general y dotarlas de seguridad, en las presentes circunstancias, requiere del desarrollo de mecanismos sofisticados y sólidos tecnológicamente hablando.

En la actualidad el acceso a la información tecnológica y a la disposición de poderosas herramientas, se ve facilitado para cualquier persona, interesada en el tema, por su ingreso a la red de comunicaciones, con un equipamiento mínimo y sin grandes recursos o restricciones.

¿Cómo definimos a la seguridad?

ISO define a la seguridad como un concepto que permite minimizar la VULNERABILIDAD.

Podemos entender el concepto seguridad como un atributo de cualquier sistema, informático o no, que significa que ese sistema está libre de cualquier peligro, daño o riesgo y que mantiene porcentajes altos de infalibilidad.

Para mantener un sistema en condiciones de seguridad, hay que garantizar, básicamente los aspectos de **confidencialidad, integridad, disponibilidad y autenticidad.**

La confidencialidad, nos dice que los objetos de un sistema han de ser accedidos solamente por aquellos autorizados a hacerlo.

La integridad, significa que los objetos no serán modificados, eliminados o reducidos por quienes no estén previstos en los esquemas de autorizaciones.

La disponibilidad, indica que los elementos del sistema deben permanecer accesibles a quienes se autorice.

Podemos agregar a este concepto el de:

Autenticidad, la que se refiere a la capacidad de determinar si una lista determinada de personas han establecido su reconocimiento y/o compromiso sobre el contenido de un documento electrónico.

El problema de la autenticidad en un documento tradicional se soluciona mediante la firma autógrafa.

Mediante su firma autógrafa, un individuo, o varios, manifiestan su voluntad de reconocer el contenido de un documento, y en su caso, a cumplir con los compromisos que el documento establezca para con el individuo.

Requisito de no repudio

Existe una diferencia sutil pero muy importante entre el concepto de **autenticidad** y el concepto de **no - repudio.**

Por ejemplo se puede afirmar que un documento fue escrito por una determinada persona, cuando se ha presenciado el acto de la firma.

Si el documento no está firmado autógrafamente, se puede estar absolutamente convencido de su autenticidad, pero no podrá ser probada, ya que sin la firma autógrafa, es imposible establecer el vinculo entre la voluntad de la persona y el contenido del documento.

Si se puede probar a terceros que efectivamente el documento es autentico entonces se dice que el documento es no-repudiable.

Si un documento es **no-repudiable** es **autentico** pero no viceversa.

Requisito de integridad

Una caracteristica básica de un documento auténtico es su integridad. En un documento tradicional como un contrato o cheque, si se aprecian modificaciones o tachones el documento es prácticamente invalidado.

En un documento electrónico en donde por errores de transmisión o fallas en el medio de almacenaje o intencionadamente se modifica el contenido original del documento entonces el documento pierde su integridad y por tanto su autenticidad.

Si un documento es **auténtico** entonces es **íntegro** pero no viceversa.

Correspondencia de conceptos entre el mundo electrónico y el mundo físico

Problema	Solución Física	Solución Electrónica
¿Quién tiene acceso a determinados lugares?	Tarjeta de identidad	Control de Acceso
¿Cómo puedo garantizar que soy quién digo ser?	Fotos en Carnets de Identidad. Firma	Autenticación
¿Cómo se garantiza que sólo aquellos a los que se ha autorizado tienen acceso a la información?	Entrega en mano. Firma del destinatario a la recepción.	Confidencialidad o privacidad.
¿Cómo puedo saber que la información no ha sido manipulada?	Sobres y paquetes sellados.	Integridad
¿Cómo me aseguro que las partes que intervienen en una transacción no nieguen haberlo hecho?	Testigos, notarios, correos certificados.	No repudio.
¿Cómo demuestro cuándo se realizó una transacción?	Fechado de documentos	Sellado de tiempo

Requisito de confidencialidad

En un sistema en donde la forma tradicional de realizar operaciones comerciales esta siendo reemplazado por métodos electrónicos resulta de suma importancia contar

no solo con la tecnología, sino con un marco legal que norme la validez de los documentos electrónicos.

El problema de la confidencialidad no es tampoco un problema estrictamente técnico, también es conveniente estudiar las implicaciones legales del uso de esta tecnología que permite al individuo mantener información confidencial fuera del alcance del Estado, sea esta información licita o ilícita.

En realidad el uso de las técnicas criptográficas, plantea soluciones y problemas no solamente relacionados con el procedimiento técnico matemático, en cuanto a resolver los temas de confidencialidad y autenticidad de los documentos electrónicos.

Un problema de este tipo requiere del trabajo interdisciplinario de criptógrafos, analistas, especialistas en seguridad de datos, abogados, y otros especialistas.

Es importante contar con una base legal que conceda, a los documentos firmados digitalmente, un tratamiento similar a la de los documentos tradicionales firmados autógrafamente.

Vamos a analizar el tema en dos partes, la pimera dedicada al problema de la no-repudación de los documentos electrónicos, la segunda esta dedicada al problema de la confidencialidad.

La tecnica de criptografia

Estos problemas, **confidencialidad, integridad, autenticidad** y **no-repudiación** se resuelven mediante la tecnología llamada "**Criptografía**".

La criptografia es una rama de las matemáticas, que al aplicarse a mensajes digitales, proporcionan las herramientas idóneas para solucionar los problemas antes mencionados.

Al problema de la confidencialidad se le relaciona comúnmente con técnicas denominadas de "encripción" y el problema de la autenticidad mediante técnicas denominadas de "firma digital", aunque ambos en realidad se reducen a procedimientos criptográficos de encripción y desencripción

La criptografia en realidad no es sólo una rama de las matemáticas sino una disciplina que puede reunir otras áreas de la ciencia, sin embargo es en las matemáticas en donde la criptografia moderna encuentra los fundamentos más trascendentes.