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

Maestría en Seguridad Informática

Trabajo Final de Maestría

Tema

Confianza entre organizaciones

Titulo

Intercambio de información entre
Banco Central de Honduras y Sistema Financiero

Autor:

Edy Javier Milla Reyes

Director del Trabajo Final de Maestría:
Ingeniero Hugo Pagola

Fecha de Presentación:
Abril 2015
Cohorte del Maestrando
2012

Declaración Jurada

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

Edy Javier Milla Reyes
No. Documento 14392

Resumen

En el presente Trabajo Final de Maestría se aborda la temática de confianza entre organizaciones y cómo debe ser tomada en cuenta para la relación en función de los intercambios de información. Como una fuente tecnológica, se desarrolla el tema de Infraestructura de llave pública (PKI), cuyo objetivo es la de proveer servicios de autenticación, integridad, confidencialidad y no repudio. Además, se introduce el tema de certificación cruzada como solución de confianza entre organizaciones.

Mediante el estudio de un proceso de negocio, se expone su desarrollo en el contexto de la economía nacional hondureña, cuyo objetivo es la recopilación estadística de la divisa norteamericana, información que es obtenida del sistema financiero mediante el intercambio de archivos, para lo cual se presentan algunas falencias en el aspecto de seguridad de la información.

Se hacen recomendaciones para mejorar los aspectos de seguridad de la información por medio de dos soluciones:

- ISO/IEC 27002:2005 principalmente con sus objetivos de control “Gestión de Operaciones y Comunicaciones” y “Gestión de acceso de usuarios”
- Utilización de certificados digitales a fin de lograr: autenticación, integridad, confidencialidad y no repudio.

Adicionalmente, se muestra una prueba de concepto que permite visualizar técnicamente la ejecución de las recomendaciones planteadas. Fundamentado en la utilización de certificados digitales para asegurar el intercambio de información entre BCH y una institución financiera modelo, obteniendo así un atributos de firma digital y cifrado de archivos utilizando el estándar S/MIME y CMS, cumpliendo de esta manera los objetivos planteados.

Palabras clave: confianza, seguridad, integridad, confidencialidad, disponibilidad, no repudio, certificados digitales, llave pública, llave privada, procesos seguros, intercambio de información, OpenSSL, S/MIME, CMS.

Tabla de contenidos

Declaración Jurada ii
Resumen iii
Tabla de contenidos iv
Nómina de abreviaturas viii
Introducción 1
Objetivos 2
Específicos 2
Alcance 3
Capitulo I. Confianza entre organizaciones 4
Confianza 4
Confianza en los procesos de negocio 5
Elementos importantes para establecer confianza 6
PKI como solución tecnológica para establecer confianza 8
Componentes de la Infraestructura de Llave Pública 8
Certificados digitales 9
Autoridades Certificantes 10
Listas de revocación de certificados 10
Modelos de Confianza 11
Capítulo II. Banco Central de Honduras dentro del marco legal del país 12
Resumen del capitulo 12
Creación del Banco Central de Honduras (BCH) 12
Obligaciones del BCH 13
BCH, comprometido con la seguridad de la información 14
Uso de recursos informáticos en BCH 14
Proceso del Registro de Ingresos y egresos de divisas 15
Descripción general del proceso 15

Descripción detallada del proceso 16
Proceso de creación de la cuenta de usuario de acceso al sitio interno del BCH www.bch.if para las instituciones financieras 16
Proceso de generación y distribución del par de llaves (pública y privada) de BCH utilizando GnuPG 17
Proceso de cifrado de los archivos estadísticos en las Instituciones Financieras 18
Proceso de envío de los archivos cifrados a BCH por parte de las instituciones financieras 19
Proceso de recepción en BCH de los archivos cifrados 19
Capitulo III. Hallazgos y propuestas de mejoras 21
Hallazgos al efectuar el análisis 21
Recomendaciones basadas en el código de practica ISO/IEC 27002:2005 23
10. Gestión de Operaciones y Comunicaciones 23
11. Control de Accesos 34
Herramientas utilizadas en el proceso 37
Mejora en la Confianza entre BCH y el Sistema Financiero 38
Modelo Jerárquico 38
Modelo de Certificación Cruzada 39
Elementos requeridos para la implementación de un modelo de certificación cruzada en BCH 42
Modelo de certificación cruzada en BCH 43
Detalles del proceso de certificación cruzada 44
Gestión de certificados digitales 47
Ciclo de vida de las llaves 47
Protección de llaves criptográficas 48
Proceso mejorado del “Reporte de ingreso y egreso” 49
Registro de usuarios en BCH para otorgar el acceso al proceso 50
Solicitud de la institución financiera: 50
Firma digital de los archivos de reporte 50

Proceso de firma por el Operador 51
Proceso de firma y cifrado por el Autorizador 51
Proceso de envío de los archivos a BCH 51
Proceso de recepción del archivo estadístico en BCH 52
Proceso de descifrado de los archivos estadísticos 52
Firma de Servicio de estampado de tiempo 53
Prueba de concepto 53
Interoperabilidad de certificados PKI 54
Autoridades certificantes Raíz y Subordinada BCH 55
Autoridades certificantes Raíz y Subordinada IF 56
Especificación S/MIME y CMS 56
Conclusiones 58
Glosario 60
Bibliografía 63
Anexos 66
Prueba de concepto proceso de seguridad de archivos 67
Archivos de datos de la Institución Financiera (IF) 67
Firma digital de los archivos 68
Objetivo 68
Roles de usuario 68
Actividad que realiza el Operador 69
Actividad que realiza el Autorizador 70
Cifrado de los archivos 71
Objetivo 71
Actividad que realiza el Autorizador 72
Envío de los archivos 73
Objetivo 73
Actividad que realiza el Autorizador 73
Verificación de la firma digital del Autorizador de la IF para el archivo estadístico 74
Objetivo 74

Actividad que realiza el Analista 74
Descifrado del archivo estadístico 75
Objetivo 75
Actividad que realiza el Analista 75
Verificación de la firma digital del Operador de la IF para el archivo estadístico 75
Objetivo 76
Actividad que realiza el Analista 76
Autoridades certificantes y emisión de certificados digitales con OpenSSL 77
Creación de la CA raíz 84
Creación de directorios 84
Creación de la base de datos de certificados 84
Creación de la solicitud de CA raíz 84
Creación del certificado de CA raíz (autofirmado) 84
Creación de la CRL inicial 84
Creación de la CA email 85
Creación de directorios 85
Creación de la base de datos de certificados 85
Creación de la solicitud de CA email 85
Creación del certificado de CA email (firmado por CA raíz) 85
Creación de la CRL inicial 85
Creación de la cadena de certificación 86
Creación del certificado de usuario Operador 86
Creación del certificado de usuario Autorizador 88
Conexión al servidor SSH utilizando la llave privada/pública del Autorizador 88
Creación del usuario en el servidor remoto 89
Obtención de la llave publica del autorizador 89

Nómina de abreviaturas

AICPA/CICA	American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants
API	Application Program Interface
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
CA	Certification Authority (Autoridad Certificante)
CC	Cross Certification (Certificación Cruzada)
CN	Common Name (Nombre Común)
CMS	Cryptographic Messaje Syntax
CRL	Certificate Revocation List
DNS	Domain Name Systen
EE	End Entity (Entidad final)
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Address
ITU	International Telecommunications Union
MD	Message Digest (Resumen de mensaje, digesto)
SAN	Subject Alternative Name
S/MIME	Secure/Multipurpose Internet Mail Extensions
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infraestructure (Infraestructura de Llave Pública).

RDN	Relative Distinguished Name
RFC	Request for Comments
UPN	User Principal Name
URI	Uniform Resource Identifier

Introducción

A medida que las organizaciones utilizan sistemas de información para potenciar sus actividades de negocios y estrechar sus relaciones en benéfico de su desarrollo competitivo, el reto de mejorar la seguridad de los sistemas de información se acrecienta.

Para el desarrollo de este ámbito, el Banco Central de Honduras (BCH) comprometido con su misión[2], se relaciona con diversas instituciones (financieras y no financieras) que le aportan información a manera de indicadores que por su gran importancia contribuyen a la toma de decisiones del país en materia de economía. Además, la existencia de leyes, reglamentos y normativas vigentes en el país le facultan a requerir que dicha información sea proporcionada con carácter de obligatoriedad, asumiendo a la vez el compromiso que ésta no será divulgada para fines que no correspondan al estudio del comportamiento de la economía.

Debido a que la información de las instituciones se clasifica de acuerdo a su nivel de exposición (en muchas ocasiones de forma confidencial), el BCH está obligado a resguardarla y protegerla, alejándola del alcance de entidades no autorizadas o no involucradas en su procesamiento.

El propósito de este Trabajo Final de Maestría es analizar y mejorar los aspectos de seguridad de uno de los procesos de negocio de la institución que sirve como fuente de indicadores, el “Registro Estadístico de Ingresos y Egresos de Divisas de los Agentes Cambiarios” y que eventualmente, la experiencia de lugar a otras instituciones cuyas funciones o necesidades de negocio sean de similar interés sigan las recomendaciones de este documento.

[2] http://www.bch.hn/mision.php

Objetivos

1. Investigar cómo se desarrollan en la actualidad, las actividades para el intercambio de información para el proceso de negocio “Registro Estadístico de Ingresos y Egresos de Divisas de los Agentes Cambiarios” entre Banco Central de Honduras y Sistema Financiero Nacional.

2. Analizar el proceso de negocio en la búsqueda de posibles debilidades relacionadas con la seguridad de la información.

3. Proponer una mejora a los aspectos débiles que se detecten en el proceso con respecto a la seguridad de la información.

4. Desarrollar una prueba de concepto que permita visualizar las recomendaciones planteadas.

Específicos

1. Fortalecer la seguridad de las actividades de autenticación, autorización, integridad, no repudio y confidencialidad del proceso “Registro Estadístico de Ingresos y Egresos de Divisas de los Agentes Cambiarios”.

2. Alinear el proceso de negocio “Registro Estadístico de Ingresos y Egresos de Divisas de los Agentes Cambiarios” en función de los objetivos de control de la norma ISO/IEC 27002:2005.

3. Mejorar los aspectos de confianza entre BCH y los miembros del Sistema Financiero por medio de la utilización de certificados digitales cruzados.

4. Desarrollar la prueba de concepto que permita mostrar las recomendaciones planteadas, asegurando la información mediante el

uso de certificados y firmas digitales para la autenticación, autorización, integridad y no repudio. Lo anterior, para las operaciones efectuadas por cada usuario que desempeñe un rol en el proceso.

Alcance

Dada la complejidad de los temas abordados y lo extenso de cada uno de ellos, para el desarrollo de este Trabajo Final de Maestría el alcance se desarrolla conforme a lo siguiente:

1. Alinear el proceso de negocio con los objetivos de control que apliquen de la norma ISO/IEC 27002:2005 principalmente a lo que se refiere a:

    a. Gestión de Operaciones y Comunicaciones (apartado 10 de la norma).
    b. Gestión de acceso de usuarios (apartado 11 de la norma).

2. Mejorar los aspectos de seguridad en función de los elementos tecnológicos que se utilizan en el proceso denominado “Registro Estadístico de Ingresos y Egresos de Divisas de los Agentes Cambiarios” del BCH.

3. El desarrollo de este trabajo está basado en el uso de certificados digitales; sin embargo, la temática acerca de la construcción de una estructura de autoridad certificante (CA) y todos los elementos que la deben constituir, es limitada y se aborda brevemente, por lo que dada su complejidad, el lector debe indagar acerca de este tema. Se recomienda el material bibliográfico “PKI, Implementing and managing E-Security” que aborda esta temática en profundidad. [1]

Capitulo I. Confianza entre organizaciones

Resumen del capítulo: En este capítulo se definen algunos conceptos de confianza, confianza en las organizaciones, además se presentan algunos elementos importantes para obtener confianza y se describe a las infraestructuras de llave pública (PKI) como solución tecnológica para establecer confianza. Además, se enunciar los componentes de una PKI.

Confianza

La nueva palabra de moda (buzzword) para el siglo veintiuno es: “confianza” [2]. Se habla mucho de confianza en nuestro entorno cotidiano, confianza en la fabricación de productos que se consumen, confianza en los servicios que se brindan y confianza en las operaciones que se intercambian entre entidades.

La RAE define confianza como [3]: “1. Esperanza firme que se tiene de alguien o algo”, “2. Seguridad que alguien tiene en sí mismo”, en el presente documento se habla de confianza en el intercambio de información entre organizaciones, por lo que este concepto se amplía a: “Seguridad que una organización tiene en sí misma, que el intercambio de información que se efectúa hacia otra organización se ha operado de forma segura”.

En el mundo digital en que vivimos, la confianza debe aplicarse de acuerdo al contexto de las organizaciones. El riesgo de pérdida de información debido al uso de sistemas informáticos es extremadamente alto, en un solo incidente relacionado con el uso de tecnologías de información se pueden experimentar grandes pérdidas de datos. De acuerdo a los reportes publicados por DataLossDB.org (DataLossDB: proyecto de investigación que tiene como propósito documentar y reportar los incidentes relacionados con la pérdida de datos a nivel mundial), cada incidente revela una pérdida de información importante (>6000 registros). En los últimos incidentes reportados aparecen las empresas eBay (2014-05-21) y Adobe Systems (2013-10-03) con 152M y 145M de registros fueron expuestos [4].

Lo anterior conlleva a que las organizaciones estén expuestas a una serie de consecuencias como ser: la disminución en la confianza y reputación. Por lo tanto, implica que los controles relacionados con el nivel de confianza entre entidades deban ser elevados.

Debido a que el nivel de confianza varía dependiendo del enfoque al cual se aplica (contexto en el que se desarrolla). Los elementos de control que se establecen en una operación financiera de alto valor, difiere de los controles que se aplican a operaciones de bajo valor, por lo que cada organización, debe definir los controles más apropiados de acuerdo a la política, criterio de clasificación de la información y análisis de exposición al riesgo.

Confianza en los procesos de negocio

Las organizaciones utilizan procesos de negocios en los que no siempre se consideran elementos que incluyan el intercambio seguro de la información, (Por procesos se entiende como el conjunto de actividades que se llevan a cabo para la consecución de un objetivo) bien sean procesos que involucren o no a las tecnologías de información (TI). Estas actividades deben estar enmarcadas en principios que aseguren la información en al menos los siguientes aspectos: confidencialidad, integridad, disponibilidad y no repudio.

En ocasiones se observa que TI no está alineado con las estrategias del negocio, provocando una ruptura en la armonía de las organizaciones en relación a los procesos de negocio. En algunas oportunidades, se hacen esfuerzos separados que no contribuyen al desarrollo integral de los procesos, repercutiendo en baja efectividad y eficiencia en los servicios que se ofrecen a las partes interesadas.

Cuando se trata del intercambio de información entre organizaciones, deben establecerse controles que permitan generar cierto grado de confianza entre ellas. Los entornos de negocios están conformados por personas, procesos y tecnología, por lo que TI no provee una solución integral que cubra todos estos aspectos, por lo tanto, cada cual debe ser sujeto de análisis, procurando al mismo tiempo mantener niveles de seguridad que permitan

proporcionar a la información los resguardos adecuados conforme a su clasificación (confidencial, sensible, pública, etc.).

Elementos importantes para establecer confianza

De acuerdo a Kapil [2] la confianza tiene tres elementos importantes:

> ***Predictibilidad**: la habilidad para producir consistentemente un resultado (positivo) esperado, evita en el cliente la necesidad de mantener constantemente un alto grado de vigilancia. La seguridad, servicio y calidad de las organizaciones, al ser más predecible, mayor facilidad que el cliente adquiera (consuma) sus servicios.*
>
> ***Activos**: La confianza no es un factor importante, a menos que haya activos (físicos o lógicos) importantes en riesgo de pérdida o daño. A mayor valor, se requiere un nivel mayor de confianza. Sitios web como eBay (un sitio de subastas en línea), utiliza socios de servicios de custodia para las operaciones de mayor valor (generalmente más de EE.UU. $ 500) como un método para aumentar la confianza en las transacciones entre dos personas desconocidas.*
>
> ***Incertidumbre**: La confianza se requiere, cuando hay un grado de incertidumbre en la capacidad de verificar una operación o resultado. En general, si toda la información se conoce sobre las partes y la transacción, entonces se reduce en gran medida la necesidad de confianza. Sin embargo, la mayoría de las transacciones, presentan un nivel de incertidumbre, incluyendo la historia desconocida*

del comprador o vendedor, la calidad desconocida de servicios o productos, y así sucesivamente.

Considere el siguiente caso el relación al uso de certificados digitales: cuando una organización deposita los certificados que pertenecen a la jerarquía de la CA Symantec/Verisign en su almacén de autoridades de certificación raíz de confianza y en el almacén de autoridades de certificación intermedias (en general estos certificados son parte de la estructura de los sistemas operativos y/o navegadores web), todos los certificados emitidos por estas CAs pasan a ser certificados de confianza, incluso los emitidos para otras organizaciones. Symantec/Verisign ha ganado un gran nivel de confianza a nivel mundial, por lo que las organizaciones y muchos individuos confían en sus certificados emitidos.

De esta manera, los usuarios de servicios que utilizan certificados emitidos por Symantec/Verisign en sus aplicaciones de negocio, al ver un resultado consistente (predictibilidad), la protección de los recursos (activos) en riesgo de pérdida y al ofrecer la capacidad de verificar la identidad de las partes (bajar la incertidumbre), genera un alto grado de confianza.

También, la confianza se gana cuando las organizaciones forman parte de iniciativas que buscan fortalecer la seguridad de los entornos en Internet, Symantec/Verisign, DigiCert, Inc. y Comodo CA Ltd (entre otros) son miembros de The Certification Authority Browser Forum [5], una organización voluntaria que aglutina a los líderes en autoridades certificantes y vendedores de navegadores de internet y otras aplicaciones. Los miembros que tienen una CA emisora de certificados o una CA Raíz deben cumplir con la auditoria para CAs: WebTrust (AICPA/CICA), ETSI 102042 o ETSI 101456 [6] para jerarquías de certificados sean considerados a ser incluidos en los navegadores web de mayor despliegue a nivel mundial.

En el ámbito financiero, la norma ISO 21188 y 15782 establecen un marco de requisitos para la gestión de una PKI a través de las políticas de los

certificados, declaraciones de prácticas de certificación y la gestión de certificados digitales en el sector de servicios financieros.

Como podemos observar, si queremos implementar ámbitos tecnológicos que generen confianza, se debe recurrir a elementos y recursos apropiados que permitan visualizar entornos seguros y que garanticen su efectividad en las organizaciones.

PKI como solución tecnológica para establecer confianza

Una Infraestructura de Llave Pública (PKI), está orientada a fortalecer los servicios confidencialidad, integridad, autenticación y no repudio de la información. Es una combinación de software, tecnologías de cifrado, y servicios que permiten a las organizaciones proteger la seguridad de la información, de sus comunicaciones, y sus operaciones de negocio [7]. PKI integra certificados digitales, criptografía de llave pública, y autoridades certificantes dentro de una arquitectura de seguridad en la red de toda la organización. La PKI de una organización permite llevar a cabo transacciones con la confianza de que: La entidad que origina la transacción es quien dice ser; la entidad que recibe la transacción es realmente el destinatario y la integridad del dato no ha sido comprometido [8]. Típicamente una PKI incluye la emisión de certificados digitales a entidades finales (EE).

El RFC 2828 Glosario Seguridad en Internet [9] define PKI como un sistema compuesto por CAs (y, opcionalmente, Autoridades de Registro RAs y otros servidores de soporte y agentes) que efectúan tareas de administración de certificados, gestión de archivos, gestión de Llaves y funciones de gestión de tokens dirigido a una comunidad de usuarios para aplicaciones de criptografía asimétrica.

Componentes de la Infraestructura de Llave Pública

Las organizaciones implementan ambientes de PKI para establecer confianza en sus entornos. Si esta PKI se diseña de acuerdo a lineamientos, marcos normativos y estándares, ésta implementación gozará de plena

confianza a los usuarios y organizaciones que tienen relación con la infraestructura.

Dependiendo de la complejidad en las necesidades de las organizaciones, los componentes de una PKI pueden variar. Básicamente se encuentran los siguientes componentes:

- Certificados Digitales
- Autoridades Certificantes
- Listas de revocación de certificados

Certificados digitales

Los certificados [8] son el fundamento de una PKI. Son representaciones digitales de computadoras, dispositivos de red o servicios y usuarios, estos últimos denominados como entidad final (EE). Éstos son respaldados por una autoridad certificante (CA). Tienen asociado un par de llaves denominadas pública y privada. Únicamente la llave pública se almacena en el certificado en la extensión “public key”. La especificación RFC 5280 cubre dos clases de certificados: Certificados de CA y Certificados de entidad final.

Contienen una colección de información (generalmente de 2 a 4 kilobytes) digitalmente firmada que típicamente incluye lo siguiente [7]:

- Información acerca de la EE (identificado por la extensión asunto o subject) que es dueño de las llaves pública y privada.
- Información acerca del emisor (CA).
- La llave pública correspondiente al par de llaves asociadas al certificado (el certificado no contiene la llave privada).
- Los nombres de los algoritmos de cifrado y resumen soportados por el certificado.
- Un listado de extensiones del estándar ITU X.509. [10]
- Información que permite determinar el estado de revocación y validez del certificado.

Para emitir un certificado digital, se debe asegurar la identidad del solicitante. Similar a un documento de identificación personal, el emisor (conocida como la autoridad de registro) debe solicitar la documentación que considere pertinente para identificar a la EE.

Cuando se emite un certificado digital por medio de una CA operativa, ésta firma digitalmente el certificado con su llave privada. La firma evidencia que el certificado fue firmado por una CA y permite determinar si ha habido cambios posteriores a su emisión. Al ser comprobado (utilizando la llave pública de la CA emisora) cualquier cambio, se evidencia que el certificado ha sido alterado y por consiguiente debe considerarse inválido.

Autoridades Certificantes

Emiten certificados para otras CAs y usualmente listas de revocación de certificados (CRLs). También efectúan una serie de tareas administrativas. Las CA generalmente son delegadas como las Autoridades de Registro (RA).

Validar y comprobar la identidad de un solicitante del certificado digital, emisión del certificado y hasta gestionar la revocación del certificado (en el caso de compromiso de la llave privada) son algunas de las funciones que desempeña una CA.

Algunas organizaciones implementan más de una CA con el propósito de mejorar la gestión de los certificados. Las CAs se organizan en jerarquías iniciando por una raíz y varias subordinadas que pueden ejercer diversas funciones e incluso estar destinadas a generar tipos de certificados para determinados fines.

Listas de revocación de certificados

Debido a que los certificados están expuestos a una serie de riesgos, debe existir un mecanismo de revocación (archivos CRL o protocolos en línea OCSP) que permita informar a los usuarios de la PKI que un certificado ha sido comprometido. La lista de revocación de certificados o CRL es generado

por una CA, es un archivo que contiene los números de serie, fecha y razón de revocación de los certificados que han sido reportados por las EE. El archivo se publica periódicamente y las aplicaciones que utilizan los certificados deben consultar esta lista con el propósito de comprobar su estado (si aparece en la lista, el certificado ha sido revocado) antes de efectuar cualquier operación. OCSP en un protocolo en línea que devuelve a través de una consulta realizada particularmente, el estado de un certificado, a diferencia de la CRL que se debe descargar todo el archivo de revocación cada vez que se requiere saber el estado en un solo certificado.

Modelos de Confianza

Cuando las organizaciones crean sus PKI, la confianza se establece solamente en los certificados emitidos por su propia PKI. La interacción entre organizaciones, crea la necesidad para que el marco de confianza interno sea extendido, logrando de esta manera establecer confianza para el uso de aplicaciones entre organizaciones, por ejemplo un servidor web, aplicaciones firmadas, etc.

Es importante considerar que para que opere una PKI, se deben definir los requisitos legales, acuerdos de uso, acuerdos de nivel de servicio (SLA), procedimientos de operación, etc.

En este trabajo se describen los siguientes modelos para establecer confianza en PKIs:

- Modelo Jerárquico
- Modelo Certificación Cruzada

Cada modelo se referencia en el capítulo III. Se describe con mayor énfasis el modelo de certificación cruzada ya que éste permite establecer confianza entre organizaciones que tienen establecidas sus PKI, de esta manera no es requerido generar CAs nuevamente para establecer un punto de confianza.

Capítulo II. Banco Central de Honduras dentro del marco legal del país

Resumen del capitulo

Este capítulo describe la situación del Banco Central de Honduras como institución en el entorno en el que se desarrolla, creación e interacción que tiene con las entidades del sistema financiero que operan legalmente en el país.

Se hace un enfoque en el sistema financiero que producto de la legislación del país, debe acatar las disposiciones de Ley del Banco Central de Honduras. Es del interés en particular abordar la temática del reporte del origen de la divisa norteamericana que las instituciones financieras reciben por parte de las personas naturales y jurídicas legalmente constituidas en el país.

Se describe el proceso que se lleva a cabo entre BCH y las entidades financieras para el intercambio de información, por medio de sistemas informáticos. Estos sistemas se han desarrollado con el fin cumplir de manera efectiva la entrega de la información requerida a las instituciones financiera.

Creación del Banco Central de Honduras (BCH)

El Banco Central de Honduras (BCH) se crea el 3 de febrero de 1950 aprobada mediante decreto legislativo No. 53, e inicia operaciones el 1 de julio de ese mismo año. En el año 1996, el soberano Congreso Nacional reforma la Ley del BCH mediante decreto No.228-96, que incluye reformas encaminadas a armonizar las actividades de la institución en relación a las condiciones y exigencias del mercado financiero.

El BCH se rige por su Ley y los reglamentos que dicte su Directorio, cuerpo colegiado con funciones estrictamente profesionales y técnicas de banca central. Este órgano superior, que se desempeña a tiempo completo en la entidad, es el que determina y dirige la política monetaria, crediticia y cambiaria del Estado.

Dentro de algunas de las funciones del BCH se tiene la responsabilidad de “Habilitar los agentes cambiarios que podrán negociar divisas en el territorio nacional” y “Determinar el tipo de cambio de la divisa en función de la oferta y demanda”.

Paralelamente, el Banco Central de Honduras mantiene una política de observación y revisión de los límites de tenencia de divisas asignado a los agentes cambiarios, con el objetivo que estos puedan satisfacer oportuna y eficientemente la demanda de divisas de sus clientes.

Asimismo, de conformidad con lo establecido en el Artículo 25 de la Ley del Banco Central de Honduras [11], reformado mediante Decreto 111-2004, publicado en el Diario Oficial La Gaceta el 22 de septiembre de 2004, toda persona natural y jurídica con residencia o domicilio en el territorio hondureño, sean nacionales o extranjeros, están obligados a proporcionar la información que las dependencias del Banco Central de Honduras les soliciten en el ejercicio de las atribuciones que le confiere la Ley. Dicha información será tratada confidencialmente y utilizada única y exclusivamente para fines estadísticos y de análisis económico y financiero.

En cumplimiento de lo anterior, el BCH ha creado el “Instructivo para el registro estadístico de ingresos y egresos de divisas de los agentes cambiarios” [12], que permite identificar claramente a la persona natural o jurídica que realiza la transacción de compra o venta de divisas, así como su origen o destino.

Obligaciones del BCH

Conforme a las funciones del BCH, cierta información que maneja debe ser declarada bajo reserva que debido a su naturaleza, de ser ofrecida al público es susceptible de ocasionar perjuicios a la economía y seguridad del Estado. En observancia a la Ley de Transparencia y Acceso a la Información Pública, el Instituto de Acceso a la Información Pública (ente responsable de garantizar y proteger el derecho de los ciudadanos de acceder a la información pública) aprobó la solicitud del BCH de clasificar como reservada la

información e indicadores por empresas y agentes cambiarios sobre ingresos y egresos de divisas (entre otros). El Directorio del BCH hace del conocimiento mediante sesión del 3 de febrero de 2011, Acuerdo No.01/2011 [13].

BCH, comprometido con la seguridad de la información

Comprometido con las instituciones con las que se relaciona, el BCH ha decidido implementar la norma ISO/IEC 27001:2005 que describe un sistema de gestión de seguridad de la información (SGSI), a su vez utilizar el ISO/IEC 27002:2005 como código practica para alinear su operatividad. Por lo que a través de la política autorizada por los miembros del Comité de Tecnologías y Seguridad de la Información (CTSI), se elevó la solicitud de aprobación ante el Directorio del BCH como la máxima autoridad de la institución, misma que resolvió aprobar la "Política de Seguridad de la Información".

Uso de recursos informáticos en BCH

En BCH se ha encontrado en los recursos informáticos una oportunidad a los problemas que se presentaban tradicionalmente al intercambiar información. Anteriormente, se recurría al intercambio de la información mediante documentos o reportes en impresos, con todos los problemas que implícitamente tiene esa forma de intercambio, por ejemplo, en general la pérdida de éstos repercute en divulgación de la información, provocando en las organizaciones disminución de la confianza ante el público en general al conocerse ese extremo. Otro ejemplo común es el reproceso de la información y consumo de tiempo que ocasiona tener una persona digitando todo el contenido de los reportes, repercutiendo además en el incremento de la frecuencia de errores de cálculo en los sistemas de información debido a la interacción humana.

Con la ayuda de los recursos informáticos se han superado muchas de estas situaciones (se acelera la entrega y disminuyen los errores), sin embargo, aún quedan algunos aspectos a considerar y que deben seguirse en los procesos de negocios con el fin de proteger la información, considerada

el activo más valioso para las organizaciones (después del recurso humano). Bases de datos de clientes, planes de negocios y propiedad intelectual son algunos de los ejemplos de cómo la información es una fuente de vida de muchas organizaciones [14]. No tener la información disponible en el momento necesario, implica que se tomen malas decisiones. También, la información en manos de la competencia puede convertirse en una desventaja para las organizaciones.

Actualmente existe una variedad de maneras de llevar a cabo el intercambio de información utilizando herramientas informáticas, facilitando y agilizando las operaciones de negocio de las instituciones. La red SWIFT es un ejemplo de estos casos que por medio de una plataforma propietaria de comunicaciones, productos y servicios, permite a los socios conectarse e intercambiar información financiera de forma segura y confiable [15].

Proceso del Registro de Ingresos y egresos de divisas

Para facilitar a los Agentes Cambiarios del Sistema Financiero el envío de la información para el “Registro Estadístico de Ingresos y Egresos de Divisas de los Agentes Cambiarios”, el BCH ha implementado servicios tecnológicos utilizando recursos informáticos que son accedidos mediante enlaces de datos (con los agentes cambiarios) para que la transferencia de la información sea oportuna, además, se incluyen controles que permiten tener cierto grado de control en lo que se refiere a seguridad de la información.

Descripción general del proceso

Para este proceso, los Agentes Cambiarios (sistema Financiero) elaboran el reporte (informe) describiendo todas las actividades económicas respecto al origen y destino de la divisa norteamericana siguiendo los lineamientos emitidos por el BCH. Posteriormente en sus equipos, ejecutan un proceso batch que cifra el o los lotes de archivos estadísticos por medio de criptografía simétrica/asimétrica (simétrica para el cifrado del archivo y asimétrica para el cifrado de la contraseña aleatoria) utilizando la llave pública de BCH por medio de la herramienta GNUPG. Posteriormente acceden a la plataforma web de BCH que les permite subir el archivo estadístico a un

repositorio destinado para uso de cada institución. Finalmente en BCH cada Analista descarga y descifra los archivos (utilizando la llave privada de BCH) recibidos de cada repositorio por institución, verifican que el formato del archivo corresponda a lo solicitado y seguidamente se incorpora la información en el sistema denominado BALCAM.

Descripción detallada del proceso

Proceso de creación de la cuenta de usuario de acceso al sitio interno del BCH www.bch.if para las instituciones financieras

El acceso al sitio web es necesario para que la institución financiera pueda proveer el reporte de ingreso y egreso de divisas de forma rápida y efectiva. Por lo que es importante para la institución financiera seguir el siguiente proceso:

1. El representante legal de la institución financiera envía una carta dirigida al departamento de Internacional de BCH solicitando la creación de la cuenta de usuario que le permite el acceso al sitio www.bch.if.

2. El departamento de Internacional remite al departamento de Tecnología y Comunicaciones (TYC) la solicitud de creación junto con la autorización respectiva.

3. El TYC crea la cuenta de acceso (en la plataforma de gestión de usuarios de ese sistema) que se forma mediante el código de la institución financiera (IF) a la que pertenece el agente cambiario, es decir el código de la institución financiera es la cuenta de usuario, eje. 101 pertenece a Banco Sogerin.

4. El TYC informa al agente cambiario que la cuenta ha sido creada mediante memorándum a través del departamento de Internacional; la contraseña es proporcionada al solicitante a través de llamada telefónica. Así mismo, se le pide que cambie la contraseña inicial.

5. En la institución financiera, el agente ingresa al sitio www.bch.if (el sitio únicamente se puede acceder por medio de la red entre BCH e IF) y cambia la contraseña inicial.

Proceso de generación y distribución del par de llaves (pública y privada) de BCH utilizando GnuPG

1. En BCH se genera el par de llaves pública/privada mediante el GnuPG. El TYC junto con el Analista efectúan la actividad de creación de llaves. El Analista define y asigna una contraseña que protege el almacén de llaves del GnuPG, donde se resguarda la llave privada. Solamente se genera un par de llaves que es utilizado por todos los analistas.

2. El TYC extrae la llave pública del BCH para ser distribuida a las Instituciones Financieras (agentes cambiarios), de manera que éstos puedan cifrar la información que será remitida.

3. El TYC distribuye la llave privada en los equipos de los analistas (un total de cinco) del BCH que reciben los archivos cifrados de las instituciones financieras. Esta llave es utilizada para descifrar los archivos. Cada institución financiera tiene asignado un analista del BCH que verifica los datos de los archivos enviados.

4. Entre los cinco analistas se comparten la contraseña del almacén de llaves donde se resguarda la llave privada. Cada vez que un nuevo analista es incorporado en sustitución de otro, se le comparte la misma contraseña.

Proceso de generación y distribución del par de llaves (pública y privada) del agente cambiario utilizando GnuPG

A continuación se describe el proceso que siguen los agentes cambiarios de acuerdo a la guía “2004-12-21 - Guía Rápida de Uso de GnuPG” para la creación del par de llaves:

1. Personal técnico de BCH se presenta a las instalaciones donde se encuentra ubicada la institución financiera. En algunas instituciones se ha capacitado personal técnico de informática par que efectúe el proceso.
2. Generan el par de llaves pública y privada mediante el GnuPG. Se solicita al agente que asigne una contraseña que protege el almacén denominado anillo de llaves (keyring) donde se resguardan.

3. Incorporan al almacén de llaves local de GnuPG la llave pública de BCH.
    a. Verifican que el "fingerprint" de la llave pública recibida por parte BCH corresponda al mismo dato proporcionado en la guía.
    b. Incorporan la llave en el anillo de llaves GNUPG.

4. Almacenan en el equipo local, el archivo batch que le permite al agente realizar el proceso con facilidad.

Proceso de cifrado de los archivos estadísticos en las Instituciones Financieras

1. Preparan los archivos de acuerdo al formato especificado por BCH. El archivo corresponde al formato establecido de tal manera que los campos de datos contengan la información de acuerdo a lo esperado.

2. Colocan los archivos de reporte (archivos a cifrar) en la carpeta "Cifrar y Firmar" de acuerdo a lo especificado en la guía. Se utiliza el disco duro local como medio de almacenamiento.

3. Ejecutan el batch (proporcionado a cada institución) que automatiza el proceso de cifrado.
    a. Colocan la contraseña del almacén de llaves cuando es requerida.

b. Mediante el proceso batch se comprimen los archivos contenidos en la carpeta “Cifrar y Firmar”, se genera un solo archivo y luego se cifra utilizando la llave pública de BCH.
c. El archivo cifrado de salida es colocado en la carpeta “Reportes Compra Venta” conforme se requiere en la guía.

Proceso de envío de los archivos cifrados a BCH por parte de las instituciones financieras

1. Ingresan a la página www.bch.if donde se le pide el código de institución y la contraseña correspondiente.

2. Seleccionan mediante el botón “Examinar” el archivo comprimido que contiene el archivo cifrado y que se encuentra ubicado en la carpeta “Reportes Compra Venta”.

3. Presionan sobre el botón “Subir” para que el archivo sea colocado en el repositorio designado a cada institución. La asignación de su propio repositorio por institución, limita que otras instituciones puedan acceder a los archivos que no les pertenecen.

Proceso de recepción en BCH de los archivos cifrados

1. Cada analista procede a descargar los archivos cifrados que han sido enviados por las instituciones financieras y que le corresponden revisar según la asignación. Esto se logra ejecutando el batch que se encuentra en cada equipo de los analistas.

2. Al ejecutar el batch se les requiere el usuario y contraseña de la conexión al servidor de archivos.

3. El batch hace una conexión SSH utilizando la utilidad PSCP (protocolo SCP) al servidor de archivos utilizando el protocolo SSH. El usuario y contraseña para la conexión SSH es el mismo utilizado por todos los analistas.

4. Los archivos cifrados se descargan al equipo del analista. Ejecutan el proceso que les permite descifrar los archivos descargados; Ingresan la contraseña que protege la llave privada y seguidamente los archivos son descifrados y colocados en una carpeta local.

5. Verifican que el contenido del archivo corresponda al formato requerido [16].

6. Si la prueba de verificación es superada, el archivo se ingresa en el sistema estadístico denominado BALCAM.

7. Posteriormente, borran los archivos que se almacenaron en el disco local.

Capitulo III. Hallazgos y propuestas de mejoras

Resumen del capítulo: En este capítulo se describen los hallazgos en seguridad de la información de las situaciones y aspectos débiles del proceso, además, se siguen dos líneas de acción para la mejora en la seguridad, la primera se encamina a las recomendaciones del ISO/IEC 27001:2005 particularmente a los objetivos de control Gestión de Operaciones y Comunicaciones y Control de Accesos. La segunda, en la mejora de la confianza entre BCH y el Sistema Financiero a través de los modelos de confianza en infraestructuras de llave pública (PKI), certificación cruzada e interoperabilidad de certificados digitales emitidos por distintas plataformas [17]. También, se expone para el intercambio de información la utilización de la especificación Secure/Multipurpose Internet Mail Extensions (S/MIME) y Cryptographic Message Syntax (CMS), logrando así contar con elementos de seguridad que permiten la autenticación del usuario, integridad del mensaje, no repudio (prueba de origen de la actividad de preparación y envío del archivo estadístico) y confidencialidad de la información.

Hallazgos al efectuar el análisis

A pesar que el proceso de “Registro Estadístico de Ingresos y Egresos de Divisas de los Agentes Cambiarios” cuenta con algunos controles que le aportan seguridad, se entiende que hay aspectos que pueden mejorarse en función de la seguridad de la información, que por cumplimiento de normas y regulaciones el BCH debe seguir (compromiso de mantener la información en forma confidencial). Principalmente se han revisado algunos de los objetivos de control de Gestión de Operaciones y Comunicaciones y Control de Accesos contenidos en el Código Práctica del ISO/IEC 27002:2005; de esta manera, se ha logrado tener un panorama que ha permitido enfocarse en seguir las recomendaciones de mejores prácticas contenidas en la norma.

En el análisis realizado al proceso actual, se han localizado algunas situaciones que deben normalizarse en función de los procesos que se deben llevar a cabo para asegurar la información. De no seguirse las recomendaciones, posibilita la exposición de la información en alguna parte

de su ciclo, misma que puede ser alcanzada por terceras partes que no tienen relación con el proceso.

A continuación se presenta una matriz que relaciona cada debilidad con foco en su atención por institución y recursos.

No.	Debilidades	Institución		Recursos		
		BCH	Financiera	Persona	Proceso	Tecnología
1	No se identifica físicamente al usuario que accede al sistema por medio de una autoridad de registro.	●			●	
2	Se utiliza una sola cuenta de usuario por agente para acceder a www.bch.if		●		●	●
3	Certificado SSL caducado https://www.bch.if	●			●	●
4	Los usuarios comparten la cuenta de acceso y contraseña	●	●	●	●	●
5	No se cambia la contraseña de acceso al sitio http://www.bch.if de la cuenta de usuario.	●	●	●	●	●
6	No se puede determinar la identidad del usuario que prepara el archivo estadístico.	●	●		●	●
7	No se puede determinar la identidad del usuario que envía el archivo estadístico.	●	●		●	●
8	No existe evidencia que el archivo estadístico ha sido procesado y aceptado.	●	●		●	●
9	El archivo estadístico es enviado sin evidencia de autorización.		●		●	●
10	No se verifica la integridad del archivo estadístico.	●			●	●
11	No se autentica ni verifica que el emisor sea genuino.	●			●	●
12	Una vez que se ha procesado el archivo estadístico, no se hace borrado seguro del mismo.	●	●		●	●
13	No se lleva registro de la destrucción de los archivos.	●	●	●	●	●
14	La llave privada de BCH se comparte entre los cinco analistas.	●	●	●	●	●
15	No se cambia la contraseña del almacén que protege la llave privada.	●	●	●	●	●
16	El par de llaves de BCH se ha mantenido por nueve años.	●			●	●
17	Al haber rotación del personal, no se generan nuevas llaves (privada/publica).	●	●	●	●	●
No.	**Debilidades**	**Institución**		**Recursos**		

		BCH	Financiera	Persona	Proceso	Tecnología
18	En el acuerdo de intercambio no se tiene un límite de responsabilidades.	●	●		●	
19	No existe un rotulado indicando que la información contenida en los archivos es sensible	●	●		●	●
20	No existe una práctica de revisión regular de los listados de usuarios de envío y recepción autorizados	●	●	●	●	
21	No hay un ciclo de verificación de versiones de productos utilizados en el proceso.	●				●

Recomendaciones basadas en el código de practica ISO/IEC 27002:2005

Los objetivos de control que se han considerado en las recomendaciones, son los que se relacionan directamente con el proceso de "Registro Estadístico de Ingresos y Egresos de Divisas de los Agentes Cambiarios". Los controles que están contenidos en la norma y que no se mencionan, se debe a que están contenidos en políticas, normas y procedimientos de mayor alcance donde está contenido el proceso en estudio. Con la aplicación de los siguientes objetivos de control del ISO/IEC 27002:2005, permite una mejora en la seguridad de la información para el proceso:

10. Gestión de Operaciones y Comunicaciones

Objetivo de control:

10.7 Manejo de los medios

10.7.3 Procedimientos para el manejo de la información

Hallazgos:

a. No se tiene el mantenimiento de un registro formal de los receptores autorizados de los datos: Se ha detectado que en ocasiones (a pesar que se tiene disponible un canal de datos propio para el intercambio de información), se ha utilizado el correo electrónico como medio de

intercambio; por tal razón, se ha destinado la información a personas que ya no intervienen en el proceso.

b. Debido a que no se sigue el control en a)., no se tiene un listado de distribución y de receptores autorizados que se pueda revisar a intervalos regulares.

Recomendación:

- Llevar el mantenimiento de un registro formal de los receptores autorizados de los datos.
- Revisar periódicamente el listado de distribución y receptores autorizados.

Alcance: El control debe implementarse en ambas instituciones (emisor y receptor) por las áreas de negocio.

Objetivo de control:

10.8 Intercambio de información

10.8.1 Políticas y procedimientos de intercambio de información.

Hallazgos:

a. Se utilizan procedimientos diseñados para proteger la información intercambiada de la intercepción, copia, modificación y destrucción. Únicamente los usuarios autorizados tienen acceso a la información.

b. Se hace uso de técnicas criptográficas para proteger la confidencialidad de la información mediante el uso de herramientas de cifrado.

c. La directriz de retención de la información recibida de la IF indica que una vez recibido y procesado el archivo estadístico sea eliminado

Recomendación:

- Para fortalecer la protección de la información, se recomienda el uso de procedimientos de borrado seguro al momento de destruir la información contenida en los archivos estadísticos una vez que se ha descifrado y ha sido utilizada en la siguiente etapa del proceso.
  Alcance: El control debe implementarse en ambas instituciones (emisor y receptor) por las áreas de negocio. En la IF, una vez que la información ha sido aceptada por BCH. En BCH una vez que la información ha sido ingresada en el sistema BALCAM.
- Mantener en archivo histórico, la versión que se ha recibido de la IF y que se encuentra en forma cifrada por el tiempo que determina la ley. Se debe asegurar además que la llave privada que corresponde tenga el mismo tratamiento.
  Alcance: El control debe implementarse en ambas instituciones (emisor y receptor)
- Fortalecer el uso de las técnicas criptográficas para proteger la integridad, autenticidad y no repudio de la información.
  Alcance: En la IF, se debe firmar digitalmente el archivo estadístico por las partes involucradas en el proceso. En BCH, debe verificarse la firma digital.

Objetivo de control:

10.8 Intercambio de información

10.8.2 Acuerdos de intercambio.

Hallazgos: En el acuerdo de intercambio no se tienen las condiciones de seguridad en relación a:

a. Procedimientos para asegurar la trazabilidad y no repudio.

b. Responsabilidades y obligaciones en caso de incidentes de seguridad de la información.

c. Uso de un sistema de rotulado acordado para la información sensible.

d. La propiedad y las responsabilidades por la protección de los datos. Mención explícita en el uso de licencias del software.

e. Controles especiales para la protección de llaves criptográficas.

Recomendación:

- Agregar al acuerdo de intercambio lo relacionado a los hallazgos. **Alcance:** El control debe implementarse en ambas instituciones.

Objetivo de control:

10.8 Intercambio de información

10.8.4 Mensajería electrónica.

Hallazgos:

a. La disponibilidad del servicio se puede ver afectada por eventuales caídas del enlace de telecomunicaciones entre instituciones o del servidor que recibe la información estadística.

b. Consideraciones legales

Recomendación:

- Disponer de contingencia apropiada para el enlace de comunicaciones y el servidor que recibe la información estadística.
  Alcance: El control debe implementarse en BCH.
- Dado que se está recomendando el uso de firma digital para fortalecer la autenticación y no repudio de la información, deben considerarse aspectos de tipo legal que no contravengan las leyes y reglamentos en función del uso de esta tecnología.
  Alcance: El control debe implementarse en ambas instituciones.

Objetivo de control:

10.8 Intercambio de información

10.8.5 Sistemas de información del negocio.

Hallazgos: Las instituciones financieras no tienen acceso a sistemas de información derivados del proceso en estudio, por lo que los hallazgos en este apartado se ven limitados a:

a. Políticas y controles apropiados para gestionar como se comparte la información.

b. Categorías del personal, que tienen permitido el uso al servidor de archivos

Recomendación:

- Establecer políticas y controles apropiados que permitan un manejo adecuado de la información compartida.

  Alcance: El control debe implementarse en BCH.
- Establecer las categorías de personal que tienen acceso al servidor de archivos, como ser los analistas del departamento de Internacional.

Objetivo de control:

10.9 Servicios de comercio electrónico

10.9.1 Comercio electrónico.

Hallazgos: El proceso en estudio, no se relaciona con el comercio electrónico propiamente dicho; sin embargo, se han visualizado algunos controles de este apartado que pueden ser de beneficio:

a. El proceso de autenticación que se lleva a cabo, está limitado a la institución financiera y no al usuario propiamente dicho. Por lo que no se tiene la certeza de la identificación del usuario que finalmente se autentica.

b. No se tienen establecidos procesos de autorización asociados al envío de información.

c. Determinación de requerimientos de integridad y no repudio, prueba de envío y recepción de los archivos estadísticos.

d. Responsabilidades asociadas con cualquier error u omisión al proveer la información.

Recomendación:

- Establecer procesos de autorización asociados al envió de información. Se recomienda definir al menos los roles de Operador (ente que prepara la información estadística) y Autorizador (ente que verifica y envía la información estadística a BCH). Éstos deben además ser identificados en por medio de la Autoridad de Registro correspondiente:

  Alcance: El control debe implementarse en BCH
- Establecer un control por medio del uso de certificados digitales para obtener la integridad y no repudio utilizando firma digital y prueba de envío y recepción utilizando el concepto de firma digital de recibo (RFC 2634).

  Alcance: El control debe implementarse en ambas instituciones
- Establecer en el acuerdo de intercambio de archivos (10.8) la responsabilidad de la IF en caso de proveer información inapropiada. Ej., sanciones.

  Alcance: El control debe implementarse en ambas instituciones

- Usar métodos de autenticación seguros por medio de certificados y firmas digitales.
  Alcance: El control debe implementarse en ambas instituciones

Objetivo de control:

10.9 Servicios de comercio electrónico

10.9.2 Transacciones en línea.

Hallazgos: El proceso en estudio, no se relaciona con el comercio electrónico propiamente dicho; sin embargo, se han visualizado algunos controles de este apartado que pueden ser de beneficio:

a. No se utilizan firmas digitales para las partes involucradas.

b. El certificado digital utilizado en la página www.bch.if se encuentra caducado, de manera que se muestra una advertencia al usuario de la IF quien hace caso omiso de tal advertencia. A pesar de ello el canal se mantiene encriptado.

c. Se detectó el uso del protocolo SSL v3. Como parte de la suite de protocolos de cifrado.

d. Se utiliza autenticación segura sin certificados digitales.

Recomendación:

- Se recomienda el uso de firma digitales para cada etapa del proceso donde un ente interactúe con el archivo estadístico.
  Alcance: El control debe implementarse en ambas instituciones
- Se recomienda seguir un ciclo de gestión de certificados digitales que contribuya al proceso desde la creación de un certificado hasta su destrucción.
  Alcance: El control debe implementarse en ambas instituciones para que incluyan los certificados de EE para cifrado de canal de datos y personas.
- Debe incluirse en el ciclo de gestión de vulnerabilidades el servidor que soporta este proceso.
  Alcance: El control debe implementarse en BCH
- Debe habilitarse la autenticación segura a través del uso de certificados digitales

Alcance: El control debe implementarse en ambas instituciones

Objetivo de control:

10.10 Seguimiento y control

10.10.1 Registro de auditoria

Hallazgos: Debido a la falta de autorización, esta parte del proceso no pudo ser analizada; sin embargo, dada la importancia de este control, se recomienda seguir la guía de implementación de acuerdo a la guía de implementación de la norma

Recomendación: Se recomienda que las auditorias de las sesiones incluyan cuando correspondan:

a) Identificación de los usuarios;

b) Fechas, tiempos y detalles de los eventos principales, como el inicio y cierre de sesión;

c) La identidad de la computadora o la ubicación si es posible;

d) Registros de intentos de acceso al sistema exitosos y rechazados;

e) Registros de intentos de acceso a los datos u otro recurso, exitosos y rechazados;

f) Cambios a la configuración del sistema

g) Uso de privilegios;

h) Uso de utilitarios y aplicaciones del sistema;

i) Archivos accedidos y el tipo de acceso;

j) Direcciones de redes y protocolos;

k) Alarmas ejecutadas por el sistema de control de acceso;

l) Activación y desactivación de los sistemas de protección, tales como antivirus y sistemas de protección de intrusos.

Alcance: El control debe implementarse en BCH

Objetivo de control:

10.10 Seguimiento y control

10.10.3 Protección de la información de los registros de actividad

Hallazgos: Los registros no son extraídos a una localidad diferente a donde se originan los eventos.

Recomendación: Para que la información de registro este protegida contra la manipulación y accedida por procesos no autorizados, se recomienda proteger:

a) Los registros contra cambios no autorizados.

b) Que los archivos de sesión se editen o eliminen.

c) Que la capacidad de almacenamiento del medio del archivo de sesión se exceda, resultando en la falla para registrar los eventos o sobrescribir eventos registrados del pasado.

d) La extracción de los registros hacia un servicio de recolección de eventos (plataforma SIEM).

e) Clasificar los registros por tipo actividad y extraer solo aquellos que son de utilidad para el seguimiento de eventos importantes.

Alcance: El control debe implementarse en BCH

Objetivo de control:

10.10 Seguimiento y control

10.10.4 Registros de actividad de administrador y operador

Hallazgos: El acceso a la base de datos (control de acceso) está definido por una sola cuenta de acceso, lo que dificulta deducir la responsabilidad de cada rol al momento de presentarse un incidente relacionado con éstos.

Recomendación: Llevar el registro de actividades de éstos dos roles.

a) Creación de cuentas de acceso para cada rol que desarrolla actividades en la base de datos.

b) Fecha y hora de ocurrencia del evento.

c) Información acerca del evento

d) Procesos involucrados

e) Revisar periódicamente los eventos registrados para cada rol

Alcance: El control debe implementarse en BCH

Objetivo de control:

10.10 Seguimiento y control

10.10.6 Sincronización de reloj

Hallazgos: Se determinó que la sincronización de reloj es adecuada ya que se utiliza el servicio NTP; sin embargo, se determinó que no se autentica la fuente utilizada para sincronización (NTP authentication keys)

Recomendación: Configurar los servicio de NTP de tal manera que se autentique el servicio por medio de llaves previamente definidas.

Alcance: El control debe implementarse en BCH

11. Control de Accesos

Objetivo de control:

11.2. Gestión de accesos de usuarios

11.2.1 Registro de usuarios

Hallazgos:

El repositorio de archivos tiene una sola cuenta de acceso para subir el archivo estadístico por institución que no está vinculada a un usuario particular, por lo que no se tiene certeza de persona que efectúa las acciones. El usuario únicamente conoce sus derechos de acceso por las actividades que desarrolla. El usuario no firma ninguna declaración indicando que comprende las condiciones de acceso. Al tener un solo usuario por institución, no se hace mantenimiento de un registro formal de todas las personas que utilizan el servicio. No se puede desvincular la cuenta si una persona deja de ejercer el rol o tarea.

Recomendación:

a) Hacer un registro de cuentas de usuario que vinculen a las personas que efectúan las operaciones en el repositorio de archivos

b) Establecer un control que permita verificar que el usuario tiene autorización del dueño para uso del sistema o servicio de información.

c) Entregar al usuario una declaración escrita de sus derechos de acceso

Se recomienda agregar el rol de supervisor cuya actividad permita llevar un control de la trazabilidad de flujo de los archivos. Eje, cuando se enviaron, si se recibieron, quien los recibe.

d) Establecer un control para el mantenimiento de un registro formal de todas las personas que utilizan el servicio.

e) Al implementar el control del literal a), se debe bloquear inmediatamente el usuario que ha dejado de ejercer el rol o tarea en el proceso.

Alcance: los controles deben implementarse en BCH.

Objetivo de control:

11.2. Gestión de accesos de usuarios

11.2.2 Gestión de privilegios

Hallazgos:

A pesar que se tiene identificados los privilegios asociados a sistema operativo y base de datos, a nivel de este último se utiliza un usuario genérico para agregar, modificar y eliminar los accesos que se definen a los usuarios de la institución financiera.

Recomendación:

a) Identificar los usuarios que requieran estar asociados a otorgamiento de privilegios.

Alcance: El control debe implementarse en BCH.

Objetivo de control:

11.2. Gestión de accesos de usuarios

11.2.3 Gestión de contraseñas

Hallazgos:

Al rotarse el personal en las instituciones financieras, las contraseñas de acceso al repositorio de archivos se “heredan” sin mayor control o cambio de las mismas. La solicitud de reinicio de contraseña, no se apega al proceso de identificación del usuario antes de proveerle una contraseña nueva. Las contraseñas iniciales son genéricas y por lo tanto se puede adivinar. Los usuarios no tienen recibo de recepción de contraseñas.

Recomendación:

a) Apegarse al proceso de gestión de usuarios donde se incluye el ciclo de vida que permite el desarrollo de un adecuado manejo de contraseñas,

Alcance: los controles deben implementarse en BCH.

b) Descartar la contraseña genérica y cambiar

c) En vista que en el proceso se está recomendando el uso de certificados digitales, se recomienda a la vez que los procesos de autenticación sean efectuados utilizando tarjetas inteligentes.

Alcance: El control debe implementarse en BCH.

Objetivo de control:

11.2. Gestión de accesos de usuarios

11.2.4 Revisión de los derechos de acceso

Hallazgos: Debido a que se utilizan usuarios genéricos por institución, no se puede determinar que usuario tiene derechos particulares en el uso del sistema.

Recomendación: Seguir la indicación en 11.2.1 para que posteriormente se puedan hacer revisiones de derechos de acceso conforme a lo siguiente:

a) Los derechos deben revisarse a intervalos regulares.

b) Reasignación de derechos de acceso a los usuarios cuando realicen el traslado de un puesto a otro.

c) Los derechos con mayores privilegios deben revisarse con mayor frecuencia.

d) Verificación de las asignaciones de privilegios a intervalos regulares para asegurar que no se han obtenido privilegios no autorizados.

Alcance: El control debe implementarse en BCH.

e) Llevar un registro de los cambios a cuentas privilegiadas

Herramientas utilizadas en el proceso

En relación a las herramientas informáticas utilizadas, el uso del GNUPG [18] que es una implementación basada en el estándar de Open PGP RFC 4880 permite cifrar y firmar datos. Incorpora un sistema de almacén de llaves protegido por una contraseña que permite asegurar y agregar o quitar llaves. Otro aspecto relevante es que su funcionamiento es a nivel de línea de comandos, lo que permite la creación de rutinas de automatización e integración con otros productos o aplicaciones.

El producto GnuPG en la versión 1.4.0 utilizada en el proceso de negocio actual es del año 2004, ha sido retirado de la línea de soporte técnico por parte de la comunidad, razón por la que el proceso se expone a una diversidad de errores que eventualmente no podrán ser resueltos. Esto supone aspectos impredecibles que a futuro puede comprometer la seguridad que el proceso requiere para resguardar la información. Por lo que es esencial mantener plataformas actualizadas [19].

La herramienta puede ser reemplazada por una versión más reciente; sin embargo, un problema que se ha encontrado para la continuidad de su uso, es el soporte local de las empresas en relación a provisión de smart cards compatibles para el uso de este producto, limitando las posibilidades de poder tener un elemento externo (doble factor) que pueda almacenar las llaves de forma segura. Si bien, hay soluciones en el mercado mundial como: The OpenPGP card y The Fellowship Smartcard, no existen representaciones locales de estos productos. Por lo anterior, no se recomienda mantener esta implementación en el BCH.

Se está proponiendo cambiar a una base que utilice certificados digitales provistos por una PKI dada la posibilidad de funcionamiento de la infraestructura para entornos corporativos donde se requiere mayor control en el uso de tecnologías criptográficas (en contraste con PGP que se basa en redes de confianza [7]), además, de la reciente iniciativa del BCH en relación a normar el uso de los certificados digitales y que éstos sean emitidos por

BCH. Igualmente, las Instituciones Financieras deben generar los suyos, siempre bajo un esquema formal de proceso de generación. Posteriormente, se debe concretar un proceso de certificación cruzada (en una sola dirección IF hacia BCH) entre Instituciones Financieras y BCH. Las IF deben proveer al BCH el certificado de la autoridad certificante subordinada que se ha elegido para emitir los certificados de los usuarios finales (EE) para que se efectué el proceso de certificación cruzada entre instituciones.

Mejora en la Confianza entre BCH y el Sistema Financiero

Debido a que las organizaciones tienen que intercambiar información para el desarrollo exitoso de sus negocios, la relevancia de éste tema representa un particular interés en aquellos que requieren efectuar el intercambio de forma segura. Las nuevas necesidades de negocio, regulaciones y cumplimiento de normativas, en ocasiones llevan a las organizaciones a implementar una Infraestructura de Llave Pública (PKI). Con el propósito de aprovechar estas infraestructuras, el modelo de certificación cruzada puede ser utilizado para que dos o más organizaciones puedan interactuar, permitiendo restringir los certificados que se pueden aceptar entre ellas. En las siguientes secciones se explican los modelos jerárquicos y certificación cruzada.

Modelo Jerárquico

En este modelo, el punto de confianza inicia en la CA Raíz, por consiguiente, todas las CAs que sean firmadas por esta CA forman parte de una jerarquía de confianza. En un escenario donde dos organizaciones requieran que exista confianza entre las CAs, se debe establecer una CA Raíz que sea común. En figura 1 se muestra el modelo:

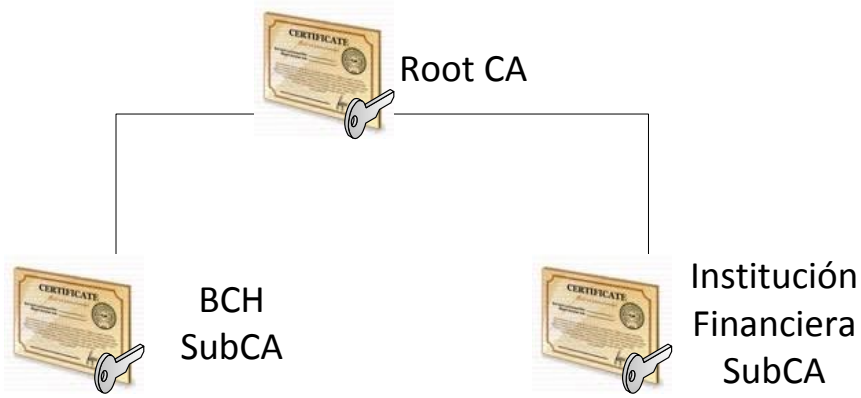


Figura 1. Modelo Jerárquico

En el ejemplo la “Root CA” representa la autoridad certificante común para la CA subordinada de BCH y las de las Instituciones Financieras (denominadas subordinadas por depender del CA Root), Al existir una CA común, todos los certificados emitidos por “Institución Financiera SubCA” son de confianza para BCH y viceversa. Si se quiere implementar este modelo en organizaciones que tienen sus PKI operando con CAs Raíz diferentes (CA Raíz y CA subordinadas con certificados emitidos para diversas aplicaciones), implica que se deben revocar todos los certificados emitidos para sus aplicaciones, servicios y usuarios para establecer nuevamente las CAs necesarias junto con los certificados requeridos para operar nuevamente. Además, se debe planificar las condiciones de operación para que una vez establecida la relación, se utilicen restricciones (constraint) adecuadas para limitar los certificados que la SubCA va a permitir utilizar de la otra SubCA en su entorno de confianza. Si a futuro se rompe la relación de negocios, esto provocaría en que las empresas deban revocar todos sus certificados y volver a generar CAs individuales. El otro problema que se visualiza es tomar la decisión de ubicar físicamente la CA Raíz, el ubicarla en una u otra de las instituciones deja lugar a que se efectúen emisiones de certificados sin que la otra se entere de tal situación.

Modelo de Certificación Cruzada

En este modelo, cada institución tiene una estructura jerárquica como el mostrado en la figura 2, por lo que no se tiene ninguna vinculación entre ellas (salvo el certificado cruzado). Este modelo permite que la dos (o más)

organizaciones puedan establecer el punto de validez de su asociado, firmando el certificado en el nivel que se desee. En la representación gráfica se muestra que las dos instituciones poseen su propia jerarquía, la institución financiera envía el certificado de la SubCA a la jerarquía de la BCH (ambas en el segundo nivel). La SubCA de BCH al firmar éste certificado, mismo que además tiene reglas de nombre y de aplicación, pasa a ser un certificado de la jerarquía de BCH.

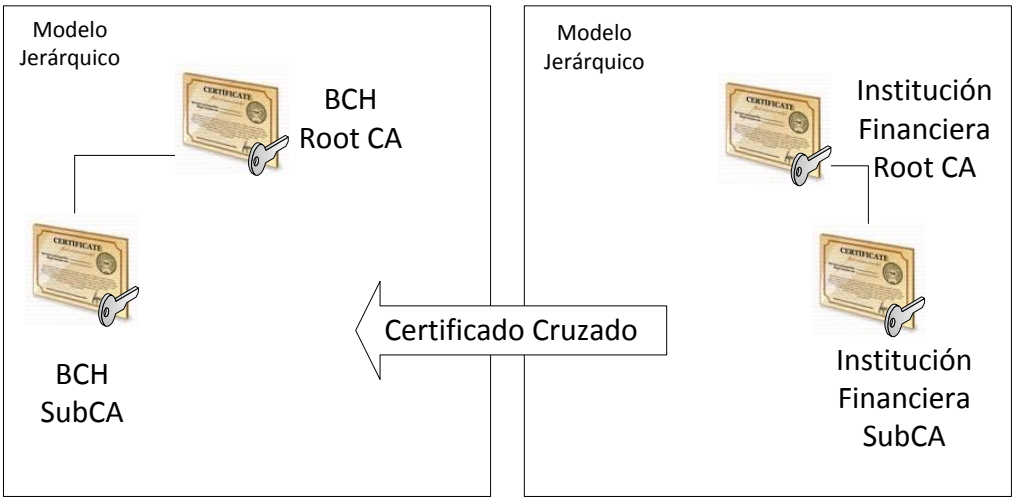


Figura 2. Modelo Certificación Cruzada

Cuando las APIs criptográficas del sistema operativo reciben la solicitud de comprobación de un certificado EE emitido por la IF, se construye la cadena de confianza que incluye el certificado cruzado, que al haber sido firmado por la SubCA del BCH, se comprueba que el certificado de EE pasa a ser un certificado de confianza en la jerarquía de BCH. (El certificado cruzado debe guardarse en el almacén de certificados intermedios de confianza en el caso de un equipo con sistema operativo Windows).

Las APIs criptográficas comprueban además, que los certificados de EE de la institución financiera cumplan con las reglas de nombre o aplicación definidas en el proceso de certificación cruzada.

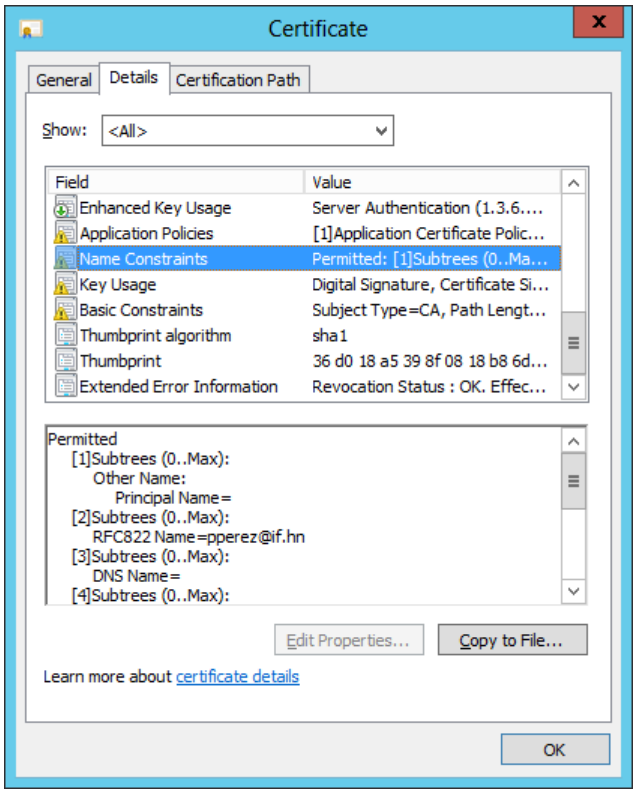


Figura 3. Restricciones de nombre

En la figura 4. se muestra la lista de propósitos utilizados en este certificado cruzado, corresponden a los OIDs 1.3.6.1.5.5.7.3.1 para autenticación de servidor, 1.3.6.1.5.5.7.3.2 para autenticación de cliente, 1.3.6.1.5.5.7.3.3 para autenticación de código y 1.3.6.1.5.5.7.3.4 para autenticación en email.

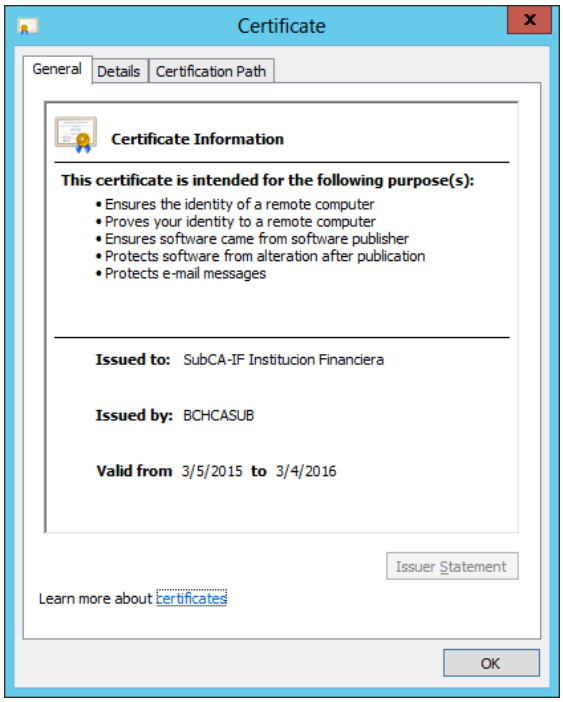


Figura 4. Propósitos de uso de certificado

Elementos requeridos para la implementación de un modelo de certificación cruzada en BCH

Para efectuar la certificación cruzada, se requiere que el certificado de la CA subordinada de la institución financiera sea firmado por el certificado de la CA subordinada de la BCH, esto se logra utilizando la Subordinación Calificada [20] (Qualified Subordination) permitiendo establecer confianza entre CAs que se encuentran en jerarquías separadas. La certificación cruzada no está limitada a CAs subordinadas, por lo que pueden establecerse confianza entre la CA Raíz y la subordinada. En el proceso de "Reporte de ingresos y egresos de divisas de los Agentes Cambiarios" la confianza se establece en un solo sentido, permitiendo que en BCH se confíe en los certificados emitidos por las Instituciones Financieras que envían la información a BCH.

Mediante la Subordinación Calificada, se deben establecer reglas que permitan validar los certificados que son aceptados entre jerarquías, esto limita los certificados que son aceptados para determinada jerarquía. BCH requiere que únicamente los certificados de las Instituciones Financieras cuyo asunto refleje el nombre del usuario sea aceptado, de esta manera se logra la

aplicación del principio del menor privilegio. Lo anterior se logra utilizando la extensión “Name Constraints”.

Las reglas de nombres pueden aplicarse a los siguientes campos:

- RDN: Identifica los nombres de objetos almacenados en directorios como un LDAP. Ejemplo: DirectoryName = "O = Institucion Financiera, DC = IF, DC = HN".
- DNS: Identifica los nombres de objetos (dispositivos de red, equipos, etc.) en el formato del Sistema de Nombres de Dominio (DNS). Ejemplo: DNS = websrv.if.hn
- URI: Identifica los nombres de recursos que utilizan el formato Uniform Resource Locator (URL), File Transfer Protocol (FTP) y Hypertext Transfer Protocol (HTTP). Ejemplo: URL = http://www.if.hn
- Correo electrónico: Identifica los nombres utilizando el formato de correo electrónico. Ejemplo: email = @if.hn
- UPN: Identifica en la extensión nombre alternativo de asunto (subject alternative name) dominios o direcciones IP. Ejemplo: websrv.if.hn o IPADDRESS=255.255.18.172,255.255.255.0

Adicionalmente se pueden definir los propósitos de aceptación de certificados, esto permite establecer políticas de aplicación (Aplication Policies) utilizando los OID de certificados digitales de manera que únicamente los propósitos destinados para cierta aplicación sean válidos. Por ejemplo los OID 1.3.6.1.5.5.7.3.1 para autenticación de servidor, 1.3.6.1.5.5.7.3.2 para autenticación de cliente y 1.3.6.1.5.5.7.3.4 para autenticación en email pueden incluirse en el certificado cruzado para permitir únicamente los certificados de EE que fueron emitidos para estos propósitos.

Modelo de certificación cruzada en BCH

El modelo de certificación cruzada permitirá una mejora en la confianza entre las Instituciones Financieras y BCH. En la emisión de certificados del lado de la institución financiera, cada cambio debe ser reportado por medio

del nuevo certificado, ya sea, porque el mismo ha expirado o sea revocado por alguna razón de seguridad. De esta manera la responsabilidad de la emisión del certificado del agente cambiario recae sobre las Instituciones Financieras y no en BCH.

La emisión de certificados de agente cambiario en períodos cortos de tiempo, permite ciclos de recertificación de usuarios con el beneficio de asegurar que solo los usuarios autorizados pueden enviar información e ingresar al sitio web del BCH. Por tanto, el servidor de BCH debe estar configurado para permitir la autenticación de usuarios únicamente con los certificados que tengan la siguiente información:

- Vigencia dentro de los límites de la emisión y caducidad.
- Las extensiones “Asuntos” y “Nombres Asuntos Alternativos” ligadas al usuario de la IF.
- La extensión “Nombres Asuntos Alternativos” valida a través de la extensión “Restricción de Nombres” (Name Constraint) del certificado cruzado utilizando el campo “Email” (estándar RFC 822) con la información de la IF.
- Verificación de las extensiones “Protección de correo electrónico” y “Autenticación de cliente”.

Detalles del proceso de certificación cruzada

Para la emisión del certificado cruzado, se propone que las políticas a seguir para los criterios de aceptación de los certificados de las Instituciones Financieras sea el siguiente:

1. La duración de la relación entre instituciones sea acordada su revisión de forma periódica, con el propósito de verificar su adecuado funcionamiento. A medida se hacen movimientos de personal en la IF y dependiendo de las restricciones definidas, el certificado cruzado debe cambiarse. Eje.: en la restricción se define explícitamente el email del usuario autorizado, cada vez que el usuario sea sustituido, debe emitirse un nuevo certificado que incluya la nueva dirección de email.

Además, reportar al BCH el cambio conforme al reporte de usuarios autorizados para envío de información.

2. La aceptación del certificado de usuario final (EE) sea emitido para el propósito OID 1.3.6.1.5.5.7.3.2 Autenticación de cliente y OID 1.3.6.1.5.5.7.3.4 protección de correo electrónico (para firma digital).
3. En la extensión Asunto (subject) el certificado debe haberse emitido para el usuario registrado en el formulario de control respectivo de acceso al sistema.
4. En la extensión Subject Alternative Name se debe colocar la dirección de email del usuario de IF.
5. La profundidad jerárquica (depth path) del certificado cruzado no debe ser mayor a 0, con el propósito de evitar que certificados de usuario final de una CA por debajo de la SubCA cruzada emita certificados que puedan considerarse válidos.
6. El dominio de BCH debe ser excluido de las restricciones permitidas con el propósito de evitar que la IF emita certificados con los datos de BCH y estos sean aceptados por omisión.

A continuación se muestra el archivo de políticas Policy.inf para una certificación cruzada efectuada para una Autoridad Certificante Microsoft Windows Server 2012.

```
[Version]
Signature = $WindowsNT$

[NameConstraintsExtension]
Include = NameConstraintsPermitted
Exclude = NameConstraintsExcluded
Critical = true

[NameConstraintsPermitted]
Email=usuario@if.hn

[NameConstraintsExcluded]
Email=@bch.hn

[BasicConstraintsExtension]
PathLength = 0

[ApplicationPolicyStatementExtension]
Policies =AppClientAuth,AppEmailProtection
critical = true

[AppClientAuth]
OID = 1.3.6.1.5.5.7.3.2
[AppEmailProtection]
OID = 1.3.6.1.5.5.7.3.4

[RequestAttributes]
CertificateTemplate = CrossCA
```

Gestión de certificados digitales

Deben definirse procedimientos para la gestión de certificados digitales, deben ser debidamente documentados y los interesados deben seguir las disposiciones con el propósito de evitar (en la medida de lo posible) incidentes de seguridad.

Los procedimientos para la gestión de certificados digitales deben adecuarse a cada situación institucional, por lo que se recomienda seguir un ciclo de vida para una adecuada gestión.

Ciclo de vida de las llaves

THALES e-security propone un modelo relacionado con el ciclo de vida de las llaves [21] desde la generación hasta la destrucción. El modelo permite una administración sistemática de las llaves que puede ser utilizado en certificados digitales. El modelo consiste en:

- Generación: Proceso por el cual una nueva llave se genera.
- Registro: Proceso por el cual una llave es asociada a un usuario, aplicación o servicio.
- Almacenamiento: Proceso por el cual la llave es almacenada en un lugar seguro o inaccesible por entes no autorizados.
- Respaldo y restauración: Proceso por el cual la llave debe ser respaldada para evitar que en un desastre ésta se pierda afectando las operaciones del negocio.
- Distribución/Instalación: Proceso por el cual una llave se distribuye o se instala para su posterior uso. Este proceso debe estar acompañado de una validación apropiada del ente que va utilizar la llave al momento de la entrega.
- Uso: Proceso por el cual la llave es utilizada
    - Rotación: Proceso por el cual la llave se redefine o se rota de acuerdo a una política de riesgo, evitando una ventana muy amplia de ataque por uso prolongado.

    - Revocación: Proceso por el cual la llave se revoca debido a un incidente.
- Suspensión: Proceso por el cual se determina que la llave ha culminado su vida operacional y debe ser reemplazada.
- Destrucción: Proceso por el cual la llave es destruida si no se requiere más su existencia.

Al utilizar certificados cruzados, éstos deben ser manejados con extrema precaución, ya que estos permiten o limitan el acceso a determinados servicios o aplicaciones. Para que un certificado cruzado preste los servicios adecuadamente, las aplicaciones o servicios deben ser capaces de determinar la validez de la cadena de certificación que emitió el certificado.

Los sistemas operativos incluyen APIs criptográficas que acceden al almacén de certificados de confianza y verifican el hash del certificado cruzado (o cualquier certificado) que ha sido cifrado utilizando la llave privada de la CA subordinada (o cualquier CA de la jerarquía). La verificación se hace descifrando el hash por medio de la llave pública de la CA subordinada (quien es la única que puede descifrar lo que la llave privada cifró) verificando la validez de los certificados.

Dicho lo anterior, es importante que el almacén de certificados de confianza sea protegido para evitar que se guarden certificados cruzados (y cualquier otro en general) que ponga en riesgo el proceso de comprobación. Se recomienda hacer una labor de inspección periódica para verificar que únicamente los certificados subordinados o intermedios autorizados se mantengan es estos almacenes de consulta.

Protección de llaves criptográficas

El uso de certificados digitales asociado a los procesos de firma y cifrado de archivos, deben tener un método seguro de resguardar la información (si la llave privada se mantiene en la custodia adecuada). Un método seguro de almacenar y utilizar la llave privada en los procesos diarios de negocio es por medio de un módulo de seguridad HSM (Hardware Security

Module). El uso de éste dispositivo permite ejercer un mayor control sobre las actividades de cifrado/descifrado y firma digital de la información en las instituciones.

Cuando se trata de actividades de uso masivo de criptografía, conviene utilizar un net HSM. La empresa THALES ofrece un equipo de seguridad que gestiona llaves criptográficas utilizando un juego de tarjetas PCB con CHIP incorporado, pudiendo ser asignadas a varios usuarios. Las tarjetas deben ser utilizadas en el orden apropiado (y tiempos definidos según la política de uso) para poder tener acceso a la llave privada que es capaz de descifrar el o los archivos. Utilizando el principio de cuatro ojos en el proceso (dos o más usuarios), garantiza que entidades individuales puedan acceder a la información sin la autorización correspondiente.

Proceso mejorado del "Reporte de ingreso y egreso"

Para el proceso mejorado, se recomienda hacer uso de los siguientes elementos que permita obtener mayor seguridad en el manejo de la información:

- Seguir un proceso de registro de usuarios
- Designar una entidad denominada autoridad de registro en BCH cuya función sea la de comprobar los datos del solicitante.
- Almacenar los certificados emitidos en dispositivos de seguridad criptográficos (HSM token).
- Segregar funciones para la institución financiera
    - Operador (prepara el archivo estadístico)
    - Autorizador (revisa y envía el archivo estadístico a BCH)
- Firma digital de los archivos estadísticos por cada rol que se va a desempeñar.
- Cifrado de los archivos estadísticos
- Envió de los archivos por medio del sitio seguro
    - Autenticación al sitio utilizando el certificado digital contenido en un token criptográfico.
- Autenticación, integridad y no repudio de los archivos

- Borrado seguro de los archivos

Registro de usuarios en BCH para otorgar el acceso al proceso

El registro de usuarios en BCH debe llevarse a cabo bajo el seguimiento estricto y cumplimiento del proceso. Los siguientes pasos del proceso se deben seguir con el objetivo de asegurar el acceso adecuado a los usuarios finales:

Solicitud de la institución financiera:

1. El representante legal de la institución financiera debe enviar una solicitud indicando el propósito del acceso junto con el formulario de registro dirigido al departamento de Internacional.
2. El formulario de registro de usuarios debe incluir los siguientes datos:
    a. Institución solicitante
    b. Fecha de solicitud
    c. Nombres
    d. Apellidos
    e. Numero de documento de identidad
    f. Cargo que desempeña
    g. Rol dentro del proceso:
        i. Operador
        ii. Autorizador

Se recomienda que los formularios con los datos proporcionados por la institución solicitante sean validados por un tercero con el propósito de confirmar que los registros son íntegros.

Firma digital de los archivos de reporte

Se recomienda que para asegurar el origen de la información, las personas designadas por la institución financiera involucradas en el proceso, firmen digitalmente el archivo estadístico de la siguiente forma:

- Firma del Operador
- Firma del Autorizador

Proceso de firma por el Operador

De forma general, en esta parte del proceso se persigue la autenticación, integridad y no repudio de la información contenida en los archivos estadísticos, mismos que son generados en la misma institución financiera. Además, se recomienda que la firma de los archivos estadísticos sea comprobada por el Autorizador.

El Operador firma cada archivo que contiene la información estadística en el siguiente orden:

- Obtiene el hash del archivo estadístico.
- Inserta el token que contiene su llave privada
- Firma el hash utilizando su llave privada.
- Obtiene estampado de tiempo de un TTP

Proceso de firma y cifrado por el Autorizador

En esta parte del proceso además de la autenticación, integridad y no repudio se persigue la confidencialidad la información a ser enviada a BCH. Además, los archivos deben ser comprobados por el Autorizador.

El Autorizador verifica que el archivo fue firmado por el Operador y lo cifra en el siguiente orden:

- Comprueba que el hash del archivo estadístico corresponda a la firma del Operador (hash cifrado con la llave privada del Operador).
- Genera el hash del archivo estadístico.
- Firma el hash utilizando su llave privada.
- Cifra el archivo utilizando la llave publica del analista del BCH.
- Genera el hash del archivo cifrado.
- Firma el hash utilizando su llave privada.
- Obtiene estampado de tiempo de un TTP.

Proceso de envío de los archivos a BCH

Los archivos deben ser enviados por la institución financiera a BCH siguiendo el siguiente orden:

- El Operador ingresa al sitio www.bch.if (este sitio es alcanzable únicamente por medio de la Red de Interconexión Financiera que aglutina a los miembros del sistema financiero de Honduras).
- El sitio solicita al Autorizador, el certificado digital para efectuar el proceso de autenticación.
- El Autorizador inserta en el puerto USB de su equipo el token asignado y que contiene la llave privada que corresponde al certificado digital emitido a su persona.
- Si el certificado digital es válido, se muestra la página con las opciones para agregar el archivo cifrado al repositorio asignado a la institución financiera.
- Sube el archivo.
- Obtiene del sitio web el recibo de confirmación que el archivo fue subido satisfactoriamente.

Proceso de recepción del archivo estadístico en BCH

El analista asignado a cada institución financiera descarga los archivos cifrados y procede a descifrarlos, posteriormente los registra en el sistema BALCAM. Los pasos a seguir son los siguientes:

- Se conecta al servidor de archivos por medio de un cliente de transferencia de archivos utilizando el protocolo SSH
- Para el proceso de autenticación utiliza su certificado digital.
- Descarga y almacena los archivos a un repositorio de su equipo local.

Proceso de descifrado de los archivos estadísticos

Descargados y almacenados los archivos estadísticos cifrados por la institución financiera, el analista procede a descifrar los archivos ejecutando el siguiente proceso:

- Ejecuta el batch que procesa cada archivo cifrado
- Comprueba el estampado de tiempo
- Procede a descifrar los archivos utilizando su llave privada.
- Comprueba que el archivo fue firmado, para la comprobación utiliza llave pública del Autorizador y Operador designado por la institución financiera.

- Verifica que los archivos contienen el formato según la guía.
- Procesa los archivos en el sistema BALCAM.
- Elimina los archivos locales utilizando la herramienta de borrado seguro.

Firma de Servicio de estampado de tiempo

En cada parte del proceso donde se aplica una firma del Operador y Autorizador, se debe tener el estampado de tiempo conforme al estándar IETF RFC 3161.

El estampado permite confirmar que para el momento en que se ejecutó el proceso de firma digital, el certificado del firmante era válido. Por lo que en un futuro, de requerirse validar el proceso de firma, aunque el certificado del firmante haya expirado, el estampado de tiempo confirma la validez del evento de firma (momento en que la firma fue ejercida). La fuente de tiempo debe ser obtenida de una tercera parte confiable (Trusted Third Party).

Prueba de concepto

La prueba de concepto se fundamenta en lo expresado en este documento con el propósito de verificar la funcionalidad de lo recomendado. Consiste en las siguientes actividades:

- Creación de la Autoridad Certificante Raíz
  - BCH e
  - IF
- Creación de la Autoridad Certificante Subordinada
  - BCH e
  - IF
- Creación de un certificado (en la CA Subordinada de BCH) para la publicación de un sitio seguro.
- Creación de un certificado de usuario (en la CA Subordinada de BCH) para ejercer las actividades del analista de BCH.
- Creación de un certificado de usuario (en la CA Subordinada de IF) para ejercer las actividades del Operador de la IF.

- Creación de un certificado de usuario (en la CA Subordinada de IF) para ejercer las actividades del Autorizador de la IF.
- Desde el equipo de la IF, se han efectuado:
    - Firmado digital del archivo estadístico; el Operador utiliza su llave privada para firmar el archivo.
    - Verificación de la firma digital; el Operador utiliza su llave pública y comprueba que la actividad se efectuó correctamente.
    - Obtiene estampado de tiempo de un TTP.
    - Verificación de la firma digital; el Autorizador utiliza la llave pública del Operador y comprueba que la actividad de firma y estampado de tiempo se efectuó correctamente.
    - Firmado digital del archivo estadístico, el Autorizador utiliza su llave privada para firmar el archivo.
    - Verificación de la firma digital, el Autorizador utiliza su llave pública y comprueba que la actividad fue correcta.
    - Obtiene estampado de tiempo de un TTP.
    - Cifrado del archivo estadístico, el Autorizador cifra el archivo estadístico utilizando la llave pública del Analista correspondiente del BCH.
    - Opcionalmente: Firmado del archivo cifrado, el Autorizador utiliza nuevamente su llave privada para firmar digitalmente el archivo, con esto se logra que el Analista compruebe (antes de descifrar el archivo) que ha sido enviado por determinada institución financiera (prueba de origen). Además, se logra una capa de protección adicional denominada Triple Wrapping, siguiendo las recomendaciones del RFC 2634

Interoperabilidad de certificados PKI

El estándar ITU-T X509 y RFC 5280, 6810 de IETF que define el formato de certificados digitales, permite a los fabricantes que soportan esta tecnología, apegarse a lineamientos, reglas, formatos, etc. establecidos con el fin de garantizar la interoperabilidad independientemente de la plataforma que se utilice. En este trabajo se han realizado prácticas de laboratorio utilizando dos sistemas operativos, Microsoft Windows y la distribución de

Linux Ubuntu Debian, comprobándose de esta manera que a pesar que los sistemas operativos son diferentes, la certificación cruzada (APIs criptográficas, aplicaciones) ha logrado interoperar sin presentarse mayores problemas.

En las pruebas de concepto, en el ambiente Microsoft Windows se ha utilizado el servicio de autoridad certificante (Active Directory Certificate Services), generándose certificados raíz y subordinado. Así mismo, en el ambiente Linux Ubuntu, se ha utilizado la herramienta OpenSSL [22] para la generación de certificados raíz y subordinado. En ambos sistemas se han utilizado certificados que han logrado interoperar, confirmándose de esta manera que las actividades mínimas que se requieren para efectuar la certificación cruzada funcionen adecuadamente.

Dada la interoperabilidad entre plataformas, las extensiones en los certificados deben cumplir con el estándar antes mencionado, de manera que las aplicaciones puedan reconocer los valores que deben ser validados y aplicados independientemente de la plataforma.

Autoridades certificantes Raíz y Subordinada BCH

Del lado de BCH se crearon las autoridades certificantes mediante el sistema operativo Windows Server 2012, La autoridad certificante raíz y subordinada se virtualizan por medio del producto VMWare Workstarion 9. Por medio de la autoridad certificante subordinada se emitieron los certificados de usuario final. Para el Analista, se ha generado un certificado digital con el propósito de descifrado de la información. Esto debido a que el analista no ejerce ninguna labor de firmado de operaciones, únicamente recibe el archivo cifrado de la IF que contiene los datos estadísticos. Un tercer equipo es virtualizado, para este caso se ha utilizado Linux Ubuntu v.14.04 LTS y utilizando la herramienta OpenSSL para realizar las operaciones de comprobación y descifrado de la información.

Autoridades certificantes Raíz y Subordinada IF

Del lado de IF se crearon las autoridades certificantes mediante el sistema operativo Linux Ubuntu v.14.04 LTS utilizando la herramienta OpenSSL. Un solo equipo virtualizado mediante VMWare 9 permite cumplir con la ejecución de la autoridad certificante raíz y subordinada, además, de las actividades de firma y cifrado de la información estadística. No se recomienda que en un ambiente productivo se realicen todas las actividades en un solo equipo. Los certificados del Operador y Analista se utilizan únicamente para las actividades de firma digital.

Especificación S/MIME y CMS

En el desarrollo de esta investigación, se ha encontrado que la especificación Secure/Multipurpose Internet Mail Extensions (S/MIME), que de acuerdo al RFC 5751 [23] permite las características de autenticación, integridad del mensaje, no repudio con prueba del origen y cifrado de la información, apoyándose en un objeto Cryptographic Message Syntax (CMS) RFC 5652 [24] para los mensajes con formato Multipurpose Internet Mail Extensions (MIME) [25] utilizando gestión de llaves basados en certificados como la definida por PKIX, infraestructura de llave pública X.509 . CMS es derivado de la especificación PKCS #7 versión 1.5 originalmente publicado como una nota técnica de los laboratorios RSA en 1993. Como almacén criptográfico, el CMS define seis tipos de contenido: data, signed-data, enveloped-data, digested-data, encrypted-data, and authenticated-data.

Contenido data

Datos arbitrarios, cualquier tipo de dato en texto o binario.

Contenido signed-data

Hash del mensaje cifrado con la llave privada del emisor. Puede haber más de una firma.

Contenido enveloped-data

Datos arbitrarios con contenido cifrado y llaves de sesión cifradas para los destinatarios. Puede haber varias llaves de sesión para varios destinatarios.

Contenido digested-data

Hash del mensaje, típicamente es utilizado para proveer integridad de datos.

Contenido encrypted-data

Datos arbitrarios con contenido cifrado, a diferencia del enveloped-data, no tiene destinatarios ni llaves de sesión. Una aplicación típica de este tipo de contenidos es la de almacenamiento local donde la llave se ha derivado de una contraseña.

Contenido authenticated-data

Es un código de autenticación de mensaje (MAC) y llaves cifradas para uno o más destinatarios. La combinación de MAC y una llave de cifrado para autenticación se requieren para que el destinatario verifique la integridad del contenido.

Dado el potencial de esta especificación que permite la seguridad de mensajes y archivos, la prueba de concepto se apoya en su utilización, logrando así su desarrollo mediante el uso de herramientas como el OpenSSL basadas en la especificación anteriormente mencionada. En el anexo se detallan las actividades que se realizaron a fin de lograr una aproximación técnica de lo recomendado.

Conclusiones

El uso del marco de referencia en la norma ISO/IEC 27002:2005 orientado a la seguridad de la información, nos ha posibilitado visualizar una problemática del proceso “Reporte de ingreso y egreso de divisas de los agentes cambiarios” hasta el momento desconocida, permitiendo mejorar la seguridad en los aspectos débiles que pueden llegar a impactar negativamente a la institución.

A la vez, la aplicación de los controles del marco de referencia es una tarea que puede llegar a consumir muchos recursos en el proceso de implementación (humanos, económicos, tiempo, etc.), por tanto, recomiendo iniciar con metas cortas realizables en espacios de tiempo razonables e ir mejorando a medida que se hacen evaluaciones periódicas del funcionamiento de los controles utilizando el ciclo de Deming (PDCA) contenido en el ISO/IEC 27001:2005.

El uso de herramientas tecnológicas, facilitan la automatización de algunas partes de los procesos, evitando la aparición de los errores comunes que se presentan frecuentemente debido a la intervención humana y logrando procesos eficientes y efectivos, por lo que siempre es recomendable visualizar esta alternativa.

Para lograr altos niveles de seguridad de la información, se ha recurrido al uso de la PKIs que dada su complejidad, al afrontar un proyecto de esta magnitud se requiere que las instituciones orienten una diversidad de recursos para lograr el objetivo de implementación. Las decisiones que se tomen al momento de la implementación de una PKI afectaran en el futuro de ésta y los sistemas que dependerán de ella (operativamente hablando como el momento de emisión de los certificados, CRLs, renovación de CAs, etc.), es necesario contar con una fuente de información y de mucha solides que permita la implementación de un buen diseño.

Las lecciones aprendidas que a otras entidades les han costado el consumo excesivo de recursos (humanos, económicos, tiempo, etc.), se deben aprovechar para no cometer los mismos errores al momento de hacer las implementaciones, logrando resultados favorables en tiempos cortos, con niveles de riesgo marginales.

El conocimiento que he adquirido al haber cursado cada una de las materias de la Maestría en Seguridad Informática, han permitido ampliar el panorama de ésta disciplina, por lo que ahora tengo la capacidad de considerar con amplio criterio una variedad de alternativas de solución a los problemas de seguridad que se presentan en los entornos empresariales y cotidianos.

Glosario

Activo	(Inglés: Asset). En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Según [ISO/IEC 13335-1:2004]: Cualquier cosa que tiene valor para la organización.
Amenaza	(Inglés: Threat). Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
Analistas	Empleado de BCH que efectúa las actividades de revisión de la información enviada por los agentes.
Autenticación	(Inglés: Authentication). Segú [Magerit:1997]: Característica de dar y reconocer la autenticidad de los activos del dominio (de tipo información) y/o la identidad de los actores y/o la autorización por parte de los autorizadores, así como la verificación de dichas tres cuestiones..
Autenticidad	(Inglés: Authenticity). Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.
Autoridad de Registro	Ente de validación de la identidad y otros datos de los suscriptores de certificados.
Confidencialidad	(Inglés: Confidenciality). Acceso a la información por parte únicamente de quienes estén autorizados. Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.
Control	Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel

	de riesgo asumido. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida.
Disponibilidad	(Inglés: Availability). Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Según [ISO/IEC 13335-1:2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.
Gestión de llaves	(Inglés: Key management). Controles referidos a la gestión de llaves criptográficas.
Incidente	Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Integridad	(Inglés: Integrity). Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.
Interoperabilidad de certificados	La operación valida entre certificados emitidos por distintas plataformas.
No repudio	Según [CCN-STIC-405:2006]: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Según [OSI ISO-7498-2]: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).
Prueba de Concepto	Una prueba de concepto o PoC (por sus siglas en inglés) es una implementación, a menudo resumida o incompleta, de un método o de una idea, realizada con el propósito de

	verificar que el concepto o teoría en cuestión es susceptible de ser explotada de una manera útil
Riesgo	(Inglés: Risk). Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.
Trazabilidad	(Inglés: Accountability). Según [CESID:1997]: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Bibliografía

[1] A. Nash, W. Duance y C. J. D. Brink, PKI, Implementing and managing E-Security, Berkely California: RSA Press, 2001.

[2] K. Raina, PKI Security Solutions for the Enterprise, Indianapolis, Indiana: Wiley Publishing, Inc., 2003.

[3] Real Academia Española, «Diccionario de la lengua española,» Real Academia Española, [En línea]. Available: http://www.rae.es/rae.html, http://www.rae.es/drae/srv/search?id=ttIyhpiT7DXX2p26VbYf. [Último acceso: 7 6 2013].

[4] DATALOSSdb, «DATALOSSdb,» Open Security Foundation, 02 02 2015. [En línea]. Available: http://datalossdb.org/. [Último acceso: 02 02 2015].

[5] Certisur, «Certisur,» [En línea]. Available: https://www.certisur.com/eventos-y-noticias/201207-Nuevas-Normativas .

[6] Certification Authority Browser Forum, «CA/Browser Forum,» CA/Browser Forum, [En línea]. Available: https://www.cabforum.org/forum.html. [Último acceso: 13 07 2013].

[7] J. A. Buchmann y E. Karatsiolis, Introduction to Public Key Infrastructures, Springer, 2013.

[8] R. Kuhn, V. C. Hu, T. Polk y S.-J. Chang, Introduction to Public Key Technology and the Federal PKI Infrastructure SP 800-32, National Institute of Standards and Technology, 2001, p. 15.

[9] The Internet Engineering Task Force, «Internet Security Glossary,» [En línea]. Available: https://www.ietf.org/rfc/rfc2828.txt. [Último acceso: 04 04 2015].

[10] International Telecommunication Union, «ITU-T Recommendations by series,» [En línea]. Available: http://www.itu.int/ITU-T/recommendations/index.aspx?ser=X. [Último acceso: 15 12 2013].

[11] Banco Central de Honduras, «Ley del Banco Central de Honduras,» Banco Central de Honduras, [En línea]. Available: http://www.bch.hn/download/Leybch.pdf. [Último acceso: 03 09 2014].

[12] Banco Central de Honduras, «Instructivo para el registro estadístico de ingresos y egresos de divisas de los agentes cambiarios,» Banco Central de Honduras, [En línea]. Available: http://www.bch.hn/download/instructivo.pdf. [Último acceso: 03 09 2014].

[13] Banco Central de Honduras, «Acuerdo No.1/2011,» Banco Central de Honduras, [En línea]. Available: http://www.bch.hn/transparenciabch/download/acuerdo_no_%2001_2011.pdf. [Último acceso: 03 09 2014].

[14] B. Honan, «ISO27001 in a Windows Environment: The Best Practice Handbook for a Microsoft Windows Environment,» de *ISO27001 in a Windows Environment: The Best Practice Handbook for a Microsoft Windows Environment*, It Governance Ltd; 2 edition, 2010.

[15] SWIFT, «SWIFT Company Information,» [En línea]. Available: http://www.swift.com/about_swift/company_information/company_information. [Último acceso: 30 07 2014].

[16] Banco Central de Honduras, «Formulario e Instructivos Compra y Venta de Divisas,» Banco Central de Honduras, [En línea]. Available: http://www.bch.hn/download/nota_agentes_cambiarios2009.pdf. [Último acceso: 30 07 2014].

[17] E. Milla, «Trabajo Final de Especialización: Certificación Cruzada, Confianza entre organizaciones,» Buenos Aires, 2013.

[18] The GNU Privacy Guard, «The GNU Privacy Guard,» [En línea]. Available: https://www.gnupg.org/. [Último acceso: 15 01 2015].

[19] M. Osborne, How to cheat at managing information security, Rockland, MA: Syngress, 2006.

[20] Microsoft Corporation, «Qualified subordination overview,» Microsoft Corporation, 2005 Enero 2005. [En línea]. Available: http://technet.microsoft.com/en-us/library/cc786077(v=ws.10).aspx. [Último acceso: 14 07 2013].

[21] R. Moulds, Key Management For Dummies, Hoboken: Wiley, 2001.

[22] OpenSSL Project, «OpenSSL Project,» [En línea]. Available: https://www.openssl.org/. [Último acceso: 14 06 2014].

[23] Internet Engineering Task Force , «Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2,» [En línea]. Available: https://tools.ietf.org/html/rfc5751. [Último acceso: 31 03 2015].

[24] Internet Engineering Task Force, «Cryptographic Message Syntax (CMS),» [En línea]. Available: https://tools.ietf.org/html/rfc5652. [Último acceso: 23 03 2015].

[25] Internet Engineering Task Force, «Multipurpose Internet Mail Extensions,» [En línea]. Available: https://tools.ietf.org/html/rfc2045. [Último acceso: 03 04 2015].

[26] B. Ballad, «Access Control, Authentication, and Public Key Infraestructure,» de *Access Control, Authentication, and Public Key Infraestructure*, Jones & Barlett Learning, 2011.

[27] B. Komar, Windows Server 2008 PKI and Certificate Security, Redmond, Washington: Microsoft Press, 2008.

[28] Comisión Nacional de Bancos y Seguros, «Comisión Nacional de Bancos y Seguros,» 30 Junio 2003. [En línea]. Available: http://www.cnbs.gob.hn/circulares/2003/C0392003.htm. [Último acceso: 13 Octubre 2014].

[29] Microsoft Corporation, «Developer Network,» Microsoft Corporation, [En línea]. Available: http://msdn.microsoft.com/en-us/library/ms524668(v=vs.90).aspx. [Último acceso: 15 06 2013].

[30] El portal de ISO 27001, «El portal de ISO 27001,» [En línea]. Available: http://www.iso27000.es/glosario.html. [Último acceso: 09 10 2013].

[31] Internet Engineering Task Force , «https://www.ietf.org/about/,» [En línea]. [Último acceso: 22 01 2014].

Anexos

Prueba de concepto proceso de seguridad de archivos

La prueba de concepto está basada en el uso de la herramienta OpenSSL. Esta herramienta tiene las siguientes aplicaciones (argumentos):

1. smime: Efectúa las operaciones de cifrado, descifrado, firma y verificación de mensajes MIME 1.0. RFC 2045. Puede procesar mensajes con formato PKCS#7 (RSA Labs).

2. cms: Cryptographic Message Syntax, sucesor de PKCS#7 (RSA Labs) efectúa las operaciones de cifrado, descifrado, firma y verificación de mensajes S/MIME versión 3.2 (2010 Request for Comments: 5751). Se encuentra soportado por el RFC 5652.

Para el ejercicio se utiliza el argumento cms ya que provee una mayor cantidad de opciones que el argumento smime. Para mayores detalles consulte la documentación de Open SSL para estos dos argumentos:

- https://www.openssl.org/docs/apps/smime.html
- https://www.openssl.org/docs/apps/cms.html

Una de las características interesantes de la especificación CMS, es que contiene un objeto Hora de firma (signingTime OID 1.2.840.113549.1.9.5). Este objeto almacena la hora en que se efectuó la operación de firma. Sin embargo; la fuente de la hora es el mismo equipo donde se realizan las actividades de firma y no un tercero confiable (TTP). Para efectos de la prueba de concepto se utiliza éste objeto. Sin embargo, para un ambiente productivo, se recomienda utilizar un TTP.

Archivos de datos de la Institución Financiera (IF)

El archivo de entrada, es un archivo que contiene la información que será enviada a BCH. Para esta etapa del proceso se persigue obtener cuatro elementos importantes en relación a la información:

1. Autenticación: Permite tener la certeza que la información proviene del Operador y Autorizador.
2. No repudio: El Operador y Autorizador de la IF no pueden negar haber manipulado el archivo ya que al ejercer la operación de firma digital demuestran tener posesión de la llave privada que acompaña su certificado digital. Ellos son los únicos que tienen (y deben tener) en custodia sus respectivos certificados digitales.
3. Integridad: Una vez que los archivos de datos se han firmado, debe poder comprobarse que los archivos no han sufrido ningún cambio mientras estuvieron en tránsito.
4. Confidencialidad: Mantener los archivos de tal forma que aún en tránsito su contenido no puedan ser visto por terceros. Únicamente el Analista de BCH que tiene la llave privada puede accederla.

Firma digital de los archivos

Con la firma de los archivos de datos se obtienen los tres primeros elementos: autenticación, no repudio e integridad.

Objetivo

Cada usuario de la IF (Operador y Autorizador) que efectúa una actividad, debe firmar digitalmente el archivo de datos.

Roles de usuario

Son actividades destinadas a la ejecución de una etapa del proceso. Se determina que para las actividades a realizar, deben existir dos roles:

- Operador: Se encarga de preparar el archivo de datos por lo que es responsable de que el contenido de éste tenga el formato solicitado por el BCH
- Autorizador: Es el encargado de verificar que el archivo contiene la información solicitada por el BCH y a la vez debe comprobar que el Operador lo haya firmado digitalmente. A la vez él debe firmar digitalmente el archivo.

- Analista: Es el receptor de la información en BCH al que pertenece la llave privada, cuya actividad es la de procesar el archivo cifrado recibido de las instituciones financieras.

Actividad que realiza el Operador

Una vez que se ha preparado el archivo estadístico de acuerdo al formato establecido por el BCH, el Operador debe proceder a:

1. Firmar digitalmente
2. Verificar

Firmar digitalmente utilizando el estándar S/MIME y CMS

Comando a ejecutar:

openssl cms -sign -in Mensaje-Operador.txt -text -out Mensaje-Operador.sig -signer Operador.crt -inkey Operador.key

Donde:

Mensaje-Operador.txt: Archivo conteniendo la información

Mensaje-Operador.sig: Archivo de salida firmado conteniendo el formato S/MIME y CMS. Además, se incluye en el archivo el certificado con la llave pública del Operador.

Operador.crt: Archivo que contiene el certificado con la llave pública del usuario Operador.

Operador.key: Archivo que contiene la llave privada del Operador con la que ejerce la firma.

Verificación: El Operador debe comprobar que el archivo fue firmado correctamente

openssl cms -verify -in Mensaje-Operador.sig -CAfile ifchain.pem -out Mensaje-Operador.sig.txt

Donde:

Mensaje-Operador.sig: Archivo que ha sido firmado por el Operador. Además, se incluye en el archivo el certificado con la llave pública del Operador.

ifchain.pem: Archivo que contiene la cadena de certificación de la IF

Mensaje-Operador.sig.txt: Archivo con estructura S/MIME y CMS que tiene los datos que fueron firmados.

Nota: El argumento “-out” puede omitirse para visualizar la salida directamente en pantalla.

El mensaje de salida de verificación es: **Verification successful**

Actividad que realiza el Autorizador

Una vez que el Operador ha preparado los archivos y los ha firmado, el Autorizador procede a revisar los archivos de datos y posteriormente:

Verificación: El Autorizador debe comprobar que el archivo fue firmado correctamente

openssl cms -verify -in Mensaje-Operador.sig -CAfile ifchain.pem -out Mensaje-Operador.sig.txt

Donde:

Mensaje-Operador.sig: Archivo que ha sido firmado por el Operador. Además, se incluye en el archivo el certificado con la llave pública del Operador.

ifchain.pem: Archivo que contiene la cadena de certificación de la IF

Mensaje-Operador.sig.txt: Archivo con estructura S/MIME y CMS que tiene los datos que fueron firmados.

Nota: El argumento “-out” puede omitirse para visualizar la salida directamente en pantalla.

El mensaje de salida de verificación es: **Verification successful**

Firmar digitalmente utilizando el estándar S/MIME y CMS

Comando a ejecutar:

openssl cms -resign -in Mensaje-Operador.sig -out Mensaje-Autorizador.sig -signer Autorizador.crt -inkey Autorizador.key

Donde:

Mensaje-Operador.sig: Archivo firmado por el Operador conteniendo el formato S/MIME y CMS. Además, se incluye en el archivo el certificado con la llave pública del Operador.

Mensaje-Autorizador.sig: Archivo firmado por el Autorizador conteniendo el formato SMIME/CMS. Además, se incluye en el archivo el certificado del Autorizador.

Autorizador.crt: Archivo que contiene el certificado del usuario Autorizador.

Autorizador.key: Archivo que contiene la llave privada del Autorizador con la que ejerce la firma.

Verificación: El Autorizador debe comprobar que el archivo fue firmado correctamente:

openssl cms -verify -in Mensaje-Autorizador.sig -CAfile ifchain.pem -out Mensaje-Autorizador.sig.txt

Donde:

Mensaje-Autorizador.sig: Archivo que se ha firmado

Ifchain.cer: Cadena de certificación de la IF

Mensaje-Autorizador.sig.txt: Archivo con estructura SMIME/CMS que guarda los datos que fueron firmados.

Nota: El argumento “-out” puede omitirse para visualizar la salida directamente en pantalla.

El mensaje de salida de verificación es: Verification successful

Cifrado de los archivos

Con el cifrado de los archivos de datos se obtienen el tercer elemento: Confidencialidad. Además, al hacer las verificaciones utilizando el certificado cruzado, podemos realizar la autenticación de origen, no repudio e integridad.

Objetivo

El usuario Autorizador de la IF debe cifrar el archivo de datos utilizando la llave pública (certificado digital) del Analista de BCH que está encargado de recibir los archivos. Seguidamente debe volver a firmar digitalmente, esta vez en el archivo cifrado. A esta técnica se le denomina Triple Wrapping RFC 2634.

Actividad que realiza el Autorizador

El Autorizador procede a cifrar los archivos:

Cifrado utilizando la herramienta OpenSSL con el algoritmo Advanced Encryption Standard (AES)

Comando a ejecutar:

openssl cms -encrypt -in Mensaje-Autorizador.sig -out Mensaje-Autorizador.sig.enc -aes128 Analista.crt

Donde:

Mensaje-Autorizador.sig: Archivo conteniendo la información firmada por el Operador y Autorizador

Mensaje-Autorizador.sig.enc: Archivo conteniendo la información firmada por el Operador y Autorizador cuyo contenido ha sido cifrado utilizando el certificado del Analista de BCH.

Aes128: Algoritmo de cifrado simétrico.

Analista.cer: Certificado del usuario Analista de BCH.

Firmar digitalmente de nuevo utilizando el estándar S/MIME y CMS

Comando a ejecutar:

openssl cms -sign -in Mensaje-Autorizador.sig.enc -out Mensaje-Autorizador.sig.enc.sig -signer Autorizador.crt -inkey Autorizador.key

Donde:

Mensaje-Autorizador.sig.enc: Archivo conteniendo la información firmada por el Operador y Autorizador cuyo contenido ha sido cifrado utilizando el certificado del Analista de BCH.

Mensaje-Autorizador.sig.enc.sig: Archivo firmado nuevamente por el Autorizador conteniendo el formato S/MIME y CMS. Además, se incluye en el archivo el certificado del Autorizador.

Autorizador.crt: Archivo que contiene el certificado del usuario Autorizador.

Autorizador.key: Archivo que contiene la llave privada del Autorizador con la que ejerce la firma.

Verificación: El Autorizador debe comprobar que el archivo fue firmado correctamente:

openssl cms -verify -in Mensaje-Autorizador.sig.enc.sig -CAfile ifchain.pem -out Mensaje-Autorizador.sig.txt

Donde:

Mensaje-Autorizador.sig.enc.sig: Archivo que se ha firmado

Ifchain.cer: Cadena de certificación de la IF

Mensaje-Autorizador.sig.txt: Archivo con estructura S/MIME y CMS que guarda los datos que fueron firmados.

Nota: El argumento "-out" puede omitirse para visualizar la salida directamente en pantalla.

El mensaje de salida de verificación es: Verification successful

Envío de los archivos

Para el envío de los archivos se utiliza el protocolo SCP (Secure Copy Protocol). Este protocolo utiliza el protocolo SSH (Secure Shell) como un medio de transmisión seguro. De esta manera, se le agrega una capa de seguridad a los archivos en tránsito de un extremo a otro.

Objetivo

El usuario Autorizador de la institución financiera debe enviar los archivos que se han firmado y cifrado al servidor de BCH. Para autenticarse, debe utilizar la llave publica/privada que ha utilizado en las operaciones de firma digital. Para esta prueba de concepto se utiliza el protocolo SSH por medio de la herramienta SCP. El usuario Autorizador se ha definido en el servidor de BCH asociando su llave pública.

Actividad que realiza el Autorizador

El Autorizador procede a efectuar la conexión al servidor de BCH cuyo repositorio ha sido previamente configurado para permitir su autenticación y el acceso a subir archivos:

Conexión, autenticación y copia de archivos al servidor

Comandos a ejecutar:

scp Mensaje-Autorizador.sig.enc.sig autorizador@192.168.10.11: Mensaje-Analista.sig.enc.sig

Donde:

Mensaje-Autorizador.sig.enc.sig: Archivo conteniendo la información cifrada y firmada digitalmente por el Autorizador.

autorizador: Usuario login definido en el servidor remoto

192.168.10.11: IP del servidor remoto.

Mensaje-Analista.sig.enc.sig: nombre del archivo en el repositorio remoto

Nota: Dado que la autenticación del usuario Autorizador al servidor remoto se lleva a cabo mediante el uso de la llave pública contenida en el certificado, la contraseña que se solicita es la que protege la llave privada.

Verificación de la firma digital del Autorizador de la IF para el archivo estadístico

El Analista de BCH debe verificar la firma digital del usuario Autorizador de la IF. Utilizando el certificado cruzado (puesto que éste contiene las restricciones que se definieron para hacer válida la relación) que se emitió entre instituciones, debe comprobarse la validez de la firma digital.

Objetivo

El usuario Analista de BCH debe verificar que el archivo firmado digitalmente corresponde al usuario Autorizador de la IF.

Actividad que realiza el Analista

El Analista procede a verificar la firma digital del archivo:

Verificación utilizando la herramienta OpenSSL

Comando a ejecutar:

openssl cms -verify -in Mensaje-Autorizador.sig.enc.sig -CAfile CrossChain-bch-if.cer -out Mensaje-Autorizador.sig.enc

Donde:

Mensaje-Autorizador.sig.enc.sig: Archivo conteniendo la información firmada digitalmente por el Autorizador de la IF.

CrossChain-bch-if: Archivo que contiene el certificado cruzado entre BCH e IF.

Mensaje-Autorizador.sig.enc: Archivo de salida que contienen el Mensaje con la información estadística en forma cifrada.

El mensaje de salida de verificación es: Verification successful

Descifrado del archivo estadístico

El descifrado del archivo estadístico se lleva a cabo por el Analista de BCH, quien tiene la llave privada que corresponde a la llave pública que fue utilizada para cifrar los archivos por parte del Autorizador de la IF.

Objetivo

El usuario Analista de BCH debe descifrar el archivo estadístico utilizando su llave privada.

Actividad que realiza el Analista

El Analista procede a descifrar los archivos:

Descifrado utilizando la herramienta OpenSSL

Comando a ejecutar:

openssl cms -decrypt -in Mensaje-Autorizador.sig.enc -recip Analista.pem -inkey Analista.key -out Mensaje-Analista.sig

Donde:

Mensaje-Autorizador.sig.enc: Archivo conteniendo la información cifrada por el Autorizador

Analista.pem: Certificado del Analista

Analista.key: Llave privada del Analista de BCH

Mensaje-Analista.sig: Archivo conteniendo la información descifrada por el Analista de BCH.

Verificación de la firma digital del Operador de la IF para el archivo estadístico

El Analista de BCH debe verificar la firma digital del usuario Operador de la IF. Utilizando el certificado cruzado (puesto que éste contiene las restricciones que se definieron para hacer válida la relación) que se emitió entre instituciones, debe comprobarse la validez de la firma digital.

Objetivo

El usuario Analista de BCH debe verificar que el archivo firmado digitalmente corresponde al usuario Operador de la IF.

Actividad que realiza el Analista

El Analista procede a verificar la firma digital del archivo:

Verificación utilizando la herramienta OpenSSL

Comando a ejecutar:

openssl cms -verify -in Mensaje-Analista.sig -CAfile CrossChain-bch-if.cer -out Mensaje-Analista.txt

Donde:

Mensaje-Analista.sig: Archivo conteniendo la información firmada digitalmente por el Autorizador de la IF.

CrossChain-bch-if: Archivo que contiene el certificado cruzado entre BCH e IF

Mensaje-Autorizador.txt: Mensaje conteniendo la información estadística.

El mensaje de salida de verificación es: Verification successful

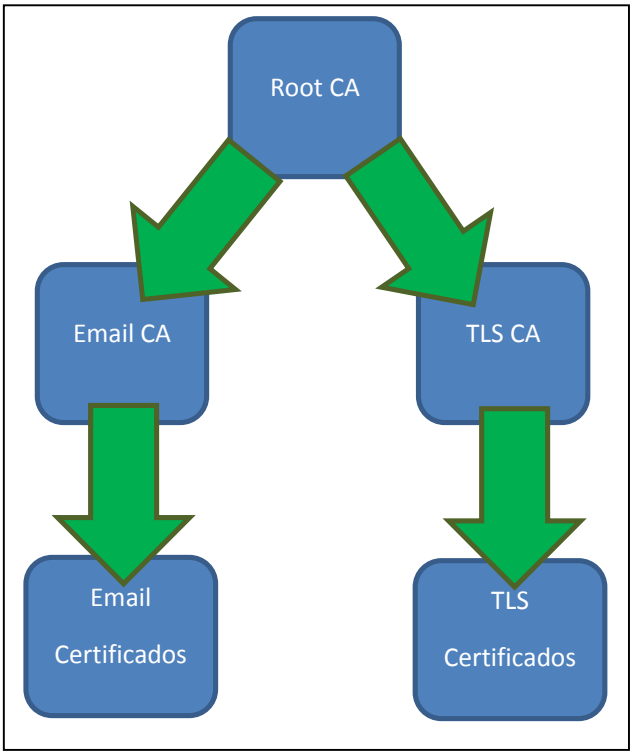
Con el archivo de salida del paso anterior **Mensaje-Autorizador.txt,** el Analista procede a revisar que el archivo recibido contiene la información en el formato solicitado, de ser así, se procesa en el sistema BALCAM. Posteriormente debe utilizarse una herramienta de borrado seguro de la información que ya no es útil.

Autoridades certificantes y emisión de certificados digitales con OpenSSL

Para la creación de autoridades certificantes en Linux Ubuntu se ha utilizado la herramienta OpenSSL. Los scripts que se utilizaron provienen del sitio: https://pki-tutorial.readthedocs.org/en/latest/index.html

Se han efectuado adaptaciones a la infraestructura PKI que se denomina "Advanced PKI" del sitio https://pki-tutorial.readthedocs.org/en/latest/advanced/index.html conforme a las necesidades para la implementación de la prueba de concepto.

A continuación se muestra el detalle de la infraestructura PKI Avanzada:



La estructura de archivos de la infraestructura PKI para la CA raíz debe crearse de la siguiente manera:

- Crear el directorio "pki-if"
  - #mkdir pki-if
- Ingresar al directorio "pki-if"

- #cd pki-if

- Crear el directorio “etc”
  - #/pki-if$mkdir etc
- Ingresar al directorio “pki-if”
  - #/pki-if$cd etc
- Crear el archivo root-ca.conf con los datos que aparece a continuación:

Archivo: root-ca.conf

```
# Institucion Financiera Root CA

[ default ]
ca                      = root-ca               # CA name
dir                     = .                     # Top dir
base_url                = http://www.if.hn/ca   # CA base URL
aia_url                 = $base_url/$ca.cer     # CA certificate URL
crl_url                 = $base_url/$ca.crl     # CRL distribution point
name_opt                = multiline,-esc_msb,utf8 # Display UTF-8 characters

# CA certificate request

[ req ]
default_bits            =2048                   # RSA key size
encrypt_key             = yes                   # Protect private key
default_md              = sha1                  # MD to use
utf8                    = yes                   # Input is UTF-8
string_mask             = utf8only              # Emit UTF-8 strings
prompt                  = no                    # Don't prompt for DN
distinguished_name      = ca_dn                 # DN section
req_extensions          = ca_reqext             # Desired extensions

[ ca_dn ]
countryName             = "HN"
organizationName        = "Institucion Financiera"
organizationalUnitName  = "IF Certificate Authority"
commonName              = "IF Root CA"

[ ca_reqext ]
keyUsage                = critical,keyCertSign,cRLSign
basicConstraints        = critical,CA:true
subjectKeyIdentifier    = hash

# CA operational settings
```

```
[ ca ]
default_ca                = root_ca                # The default CA section

[ root_ca ]
certificate               = $dir/ca/$ca.crt        # The CA cert
private_key               = $dir/ca/$ca/private/$ca.key # CA private key
new_certs_dir             = $dir/ca/$ca            # Certificate archive
serial                    = $dir/ca/$ca/db/$ca.crt.srl # Serial number file
crlnumber                 = $dir/ca/$ca/db/$ca.crl.srl # CRL number file
database                  = $dir/ca/$ca/db/$ca.db  # Index file
unique_subject            = no                     # Require unique subject
default_days              =3652                    # How long to certify for
default_md                = sha1                   # MD to use
policy                    = match_pol              # Default naming policy
email_in_dn               = no                     # Add email to cert DN
preserve                  = no                     # Keep passed DN ordering
name_opt                  = $name_opt              # Subject DN display options
cert_opt                  = ca_default             # Certificate display options
copy_extensions           = none                   # Copy extensions from CSR
x509_extensions           = signing_ca_ext         # Default cert extensions
default_crl_days          =365                     # How long before next CRL
crl_extensions            = crl_ext                # CRL extensions

[ match_pol ]
countryName               = match                  # Must match 'HN'
stateOrProvinceName       = optional               # Included if present
localityName              = optional               # Included if present
organizationName          = match                  # Must match 'Institucion Financiera'
organizationalUnitName    = optional               # Included if present
commonName                = supplied               # Must be present

[ any_pol ]
domainComponent           = optional
countryName               = optional
stateOrProvinceName       = optional
localityName              = optional
organizationName          = optional
organizationalUnitName    = optional
commonName                = optional
emailAddress              = optional

# Extensions

[ root_ca_ext ]
keyUsage                  = critical,keyCertSign,cRLSign
basicConstraints          = critical,CA:true
```

```
subjectKeyIdentifier          = hash
authorityKeyIdentifier        = keyid:always

[ signing_ca_ext ]
keyUsage                      = critical,keyCertSign,cRLSign
basicConstraints              = critical,CA:true,pathlen:0
subjectKeyIdentifier          = hash
authorityKeyIdentifier        = keyid:always
authorityInfoAccess           = @issuer_info
crlDistributionPoints         = @crl_info

[ crl_ext ]
authorityKeyIdentifier        = keyid:always
authorityInfoAccess           = @issuer_info

[ issuer_info ]
caIssuers;URI.0               = $aia_url

[ crl_info ]
URI.0                         = $crl_url
```

La estructura de archivos de la infraestructura PKI para la CA email debe crearse de la siguiente manera:

- Crear el archivo email-ca.conf con los datos que aparece a continuación:

Archivo: email-ca.conf

```
# Institucion Financiera
Email CA

[ default ]
ca                            = email-ca                  # CA name
dir                           = .                         # Top dir
base_url                      = http://www.if.hn/ca       # CA base URL
aia_url                       = $base_url/$ca.cer         # CA certificate URL
crl_url                       = $base_url/$ca.crl         # CRL distribution point
name_opt                      = multiline,-esc_msb,utf8   # Display UTF-8 characters

# CA certificate request

[ req ]
```

```
default_bits            =2048                   # RSA key size
encrypt_key             = yes                   # Protect private key
default_md              = sha1                  # MD to use
utf8                    = yes                   # Input is UTF-8
string_mask             = utf8only              # Emit UTF-8 strings
prompt                  = no                    # Don't prompt for DN
distinguished_name      = ca_dn                 # DN section
req_extensions          = ca_reqext             # Desired extensions

[ ca_dn ]
countryName             = "HN"
organizationName        = "Institucion Financiera"
organizationalUnitName  = "IF Certificate Authority"
commonName              = "IF Root CA"

[ ca_reqext ]
keyUsage                = critical,keyCertSign,cRLSign
basicConstraints        = critical,CA:true,pathlen:0
subjectKeyIdentifier    = hash

# CA operational
settings

[ ca ]
default_ca              = email_ca              # The default CA section

[ email_ca ]
certificate             = $dir/ca/$ca.crt       # The CA cert
private_key             = $dir/ca/$ca/private/$ca.key # CA private key
new_certs_dir           = $dir/ca/$ca           # Certificate archive
serial                  = $dir/ca/$ca/db/$ca.crt.srl # Serial number file
crlnumber               = $dir/ca/$ca/db/$ca.crl.srl # CRL number file
database                = $dir/ca/$ca/db/$ca.db # Index file
unique_subject          = no                    # Require unique subject
default_days            =730                    # How long to certify for
default_md              = sha1                  # MD to use
policy                  = match_pol             # Default naming policy
email_in_dn             = no                    # Add email to cert DN
preserve                = no                    # Keep passed DN
                                                ordering
```

```
name_opt                = $name_opt             # Subject DN display
                                                options
cert_opt                = ca_default            # Certificate display options
copy_extensions         = copy                  # Copy extensions from
                                                CSR
x509_extensions         = email_ext             # Default cert extensions
default_crl_days        =365                    # How long before next
                                                CRL
crl_extensions          = crl_ext               # CRL extensions

[ match_pol ]
countryName             = match                 # Must match 'HN'
stateOrProvinceName     = optional              # Included if present
localityName            = optional              # Included if present
organizationName        = match                 # Must match 'Institucion
                                                Financiera'
organizationalUnitName  = optional              # Included if present
commonName              = supplied              # Must be present

[ any_pol ]
domainComponent         = optional
countryName             = optional
stateOrProvinceName     = optional
localityName            = optional
organizationName        = optional
organizationalUnitName  = optional
commonName              = optional
emailAddress            = optional

# Extensions

[ email_ext ]
keyUsage                =
                        critical,digitalSignature,keyEncip
                        herment
basicConstraints        = CA:false
extendedKeyUsage        = emailProtection,clientAuth
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always
authorityInfoAccess     = @issuer_info
```

```
crlDistributionPoints        = @crl_info

[ crl_ext ]
authorityKeyIdentifier       = keyid:always
authorityInfoAccess          = @issuer_info

[ issuer_info ]
caIssuers;URI.0              = $aia_url

[ crl_info ]
URI.0                        = $crl_url
```

Creación de la CA raíz

Creación de directorios

```
Todo debe ejecutarse desde la ruta pki-if/
mkdir -p ca/root-ca/private ca/root-ca/db crl certs
chmod 700 ca/root-ca/private
```

Creación de la base de datos de certificados

```
cp /dev/null ca/root-ca/db/root-ca.db
cp /dev/null ca/root-ca/db/root-ca.db.attr
echo 01 > ca/root-ca/db/root-ca.crt.srl
echo 01 > ca/root-ca/db/root-ca.crl.srl
```

Creación de la solicitud de CA raíz

```
openssl req -new \
    -config etc/root-ca.conf \
    -out ca/root-ca.csr \
    -keyout ca/root-ca/private/root-ca.key
#Coloque una contraseña y su confirmación para proteger la llave privada
```

Creación del certificado de CA raíz (autofirmado)

```
openssl ca -selfsign \
    -config etc/root-ca.conf \
    -in ca/root-ca.csr \
    -out ca/root-ca.crt \
    -extensions root_ca_ext \
    -enddate 20301231235959Z
#Coloque la contraseña que protege la llave privada de la root-ca
```

Creación de la CRL inicial

```
openssl ca -gencrl \
    -config etc/root-ca.conf \
```

```
    -out crl/root-ca.crl
```

Creación de la CA email

Creación de directorios

```
Todo debe ejecutarse desde la ruta pki-if/
mkdir -p ca/email-ca/private ca/email-ca/db crl certs
chmod 700 ca/email-ca/private
```

Creación de la base de datos de certificados

```
cp /dev/null ca/email-ca/db/email-ca.db
cp /dev/null ca/email-ca/db/email-ca.db.attr
echo 01 > ca/email-ca/db/email-ca.crt.srl
echo 01 > ca/email-ca/db/email-ca.crl.srl
```

Creación de la solicitud de CA email

```
openssl req -new \
    -config etc/email-ca.conf \
    -out ca/email-ca.csr \
    -keyout ca/email-ca/private/email-ca.key
#Coloque una contraseña y su confirmación para proteger la llave privada
```

Creación del certificado de CA email (firmado por CA raíz)

```
openssl ca \
    -config etc/root-ca.conf \
    -in ca/email-ca.csr \
    -out ca/email-ca.crt \
    -extensions signing_ca_ext
#Coloque la contraseña que proteger la llave privada de la root-ca
```

Creación de la CRL inicial

```
openssl ca -gencrl \
```

```
    -config etc/email-ca.conf \
    -out crl/email-ca.crl
```

Creación de la cadena de certificación

```
cat ca/email-ca.crt ca/root-ca.crt > \
    ca/email-ca-chain.pem
```

Creación del certificado de usuario Operador

```
USUARIO=Operador
openssl req -new \
    -config etc/email.conf \
    -out certs/$USUARIO.csr \
    -keyout certs/$USUARIO.key
#Coloque una contraseña y su confirmación para proteger la llave privada
#Coloque los parámetros de acuerdo a lo solicitado
1. Country Name (2 letters) (eg, US)        []:HN
2. State or Province Name   (eg, region)    []:Francisco Morazan
3. Locality Name            (eg, city)      []:Tegucigalpa
4. Organization Name        (eg, company)   []:Institucion Financiera
5. Organizational Unit Name (eg, section)   []:
6. Common Name              (eg, full name) []:Operador
7. Email Address            (eg, name@fqdn) []:operdor@if.hn

#Firma del certificado por medio de la CA email (se requiere la contraseña
que protege la email-ca)

openssl ca \
    -config etc/email-ca.conf \
    -in certs/$USUARIO.csr \
    -out certs/$USUARIO.crt \
    -extensions email_ext
#Coloque la contraseña que protege la llave privada de la email-ca
```

```
#Verifique los datos, si todo está bien proceda a firmar y a hacer commit
```

Creación del certificado de usuario Autorizador

```
USUARIO=Autorizador
openssl req -new \
    -config etc/email.conf \
    -out certs/$USUARIO.csr \
    -keyout certs/$USUARIO.key

#Coloque una contraseña y su confirmación
#Coloque los parámetros de acuerdo a lo solicitado
1. Country Name (2 letters) (eg, US)        []:HN
2. State or Province Name   (eg, region)    []:Francisco Morazan
3. Locality Name            (eg, city)      []:Tegucigalpa
4. Organization Name        (eg, company)   []:Institucion Financiera
5. Organizational Unit Name (eg, section)   []:
6. Common Name              (eg, full name) []:Autorizador
7. Email Address            (eg, name@fqdn) []:autorizador@if.hn

#Firma del certificado por medio de la CA email (se requiere la contraseña
que protege la CA email)
openssl ca \
    -config etc/email-ca.conf \
    -in certs/$USUARIO.csr \
    -out certs/$USUARIO.crt \
    -extensions email_ext
#Coloque la contraseña que protege la llave privada de la email-ca
#Verifique los datos, si todo está bien proceda a firmar y a hacer commit
```

Conexión al servidor SSH utilizando la llave privada/pública del Autorizador

Para acceso al servidor SSH donde se depositan los archivos de la institución financiera, se siguen los siguientes pasos:

Creación del usuario en el servidor remoto

```
#adduser autorizador
#Colocar los datos que se le solicitan
#Crear el directorio ~/.ssh (si no existe)
# mkdir ~/.ssh
#Asignar permisos
#chmod 700 ~/.ssh
```

Obtención de la llave publica del autorizador

```
En el servidor local en el directorio /pki-if/certs
#openssl x509 -in Autorizador.crt -pubkey -noout > Autorizador.key.pub
#ssh-keygen -i -m PKCS8 -f Autorizador.key.pub
#Copiar el contenido de Autorizador.key.pub en el archivo
~/.ssh/authorized_keys del servidor remoto para el perfil de usuario
Autorizador (si el archivo no existe debe crearse).
#Cambiar los permisos del archivo Autorizador.key para restringir su uso
solo para el usuario Autorizador.
#chmod 700 Autorizador.key
# ssh -i Autorizador.key autorizador@IP_ServidorRemoto
#Debe salir algo similar a:
# The authenticity of host '192.49.6.154 (192.49.6.154)' can't be
established.
ECDSA key fingerprint is f4:90:79:9f:33:30:7e:47:3b:1d:0b:83:bd:b9:51:e1.
Are you sure you want to continue connecting (yes/no)?
#Debe confirmarse que el fingerprint corresponde al servidor remoto, de
ser así colocar “yes”.
#Seguidamente se le pide la contraseña que protege la llave privada.
Advertencia: Si en el servidor remoto se solicita la contraseña de usuario
autorizador en lugar de: Enter passphrase for key 'Autorizador.key': hay
que hacer una revisión de los pasos anteriores.
#Si la conexión fue exitosa, se puede proceder a hacer el envío de
archivos al servidor remoto mediante el comando SCP
```

```
# scp -i Analista.key analista@IP_ServidorRemoto:Mensaje-
Autorizador.sig.enc.sig MensajeAnalista.sig.enc.sig
```