



UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACION

**DISEÑO DE PROCESO Y SISTEMA DE GESTION DE SEGURIDAD
DE UNA ENTIDAD PRESTADORA DE SERVICIOS DE CERTIFICACION**

**TESIS PARA OPTAR AL GRADO DE
MAGISTER EN TECNOLOGIAS DE LA INFORMACION**

ADOLFO ANIBAL BARRA MOSCOSO

**PROFESOR GUÍA:
ALEJANDRO HEVIA ANGULO**

**MIEMBROS DE LA COMISIÓN:
JOSE A. PINO URTUBIA
ROMAIN ROBBES
JAIME NAVON COHEN**

**SANTIAGO DE CHILE
2012**

RESUMEN

El desarrollo de la presente tesis busca describir los procesos de funcionamiento de una entidad prestadora de servicios de certificación. En este sentido, el objetivo que se persigue es diseñar conceptualmente dichos procesos y subprocesos, permitiendo con ello un mejor entendimiento de la operación de una entidad prestadora de servicios de certificación (PSC).

Los alcances están definidos de acuerdo a un proyecto piloto que se ha desarrollado durante el último tiempo en la comunidad objetivo, representada en una unidad del Ejército, el cual busca implementar una autoridad certificadora que le permita administrar los certificados digitales y masificar su uso; aumentando la confidencialidad, autenticidad e integridad de la información que se administra a través de sus redes.

Para cumplir el objetivo de la presente tesis se desarrolló una descripción formal de cada uno de los procesos y subprocesos involucrados, utilizando para ello la notación “*Business Process Modeling Notation*” (BPMN) en el modelamiento de una entidad prestadora de servicios de certificación, específicamente de la autoridad certificadora, autoridades de registro y usuarios. Con ello se buscó satisfacer la necesidad de contar con procesos confiables que permitan mantener en el tiempo la implementación de una infraestructura de clave pública en la organización.

El trabajo realizado se desarrolló en seis capítulos. En una fase inicial, se describe la problemática, los objetivos, alcances y limitaciones del trabajo. En una segunda fase se desarrolla una breve perspectiva técnica respecto al estado del arte en sistemas criptográficos, describiendo su desarrollo histórico, sus ventajas y desventajas. Posteriormente, se realiza una descripción general de las normas jurídicas y legales exigibles para el funcionamiento de una entidad prestadora de servicios de certificación. Una vez estudiadas las normas, se describen las relaciones funcionales entre las distintas entidades que participan en el proceso de servicios de certificación, detallando cada una de las actividades al interior de la misma (funciones de la autoridad certificadora, autoridad de registro, usuarios y/o sistemas asociados). Una vez levantada la información requerida de su funcionamiento y las leyes que la enmarcan, se elaboraron los modelos y las relaciones adecuadas que describen su correcto funcionamiento, utilizando para ello una diagramación formal y fácil de entender como es la descripción mediante la notación BPMN. Finalmente, se realiza una evaluación y conclusiones del trabajo desarrollado.

ABSTRACT

The development of this thesis seeks to describe the process of functioning a "entity providing certification services". In this sense, the conceptual goal pursued is designing of processes and sub processes, thereby allowing a better understanding of the operation of an entity providing certification services (PSC).

The scopes was defined according to a pilot project that has been developed during the last time in the target community, represented by the Army Telecommunications Command, which seeks to implement a certificate authority that allows you to manage digital certificates and use massively increasing the confidentiality, authenticity and integrity of the information given through their networks.

To meet the objective of this thesis, was developed a formal description of each of the involved processes and subprocess, using the notation "Business Process Modeling Notation" (BPMN) in the modeling of an entity providing certification services, specifically Certificate Authority, registration authorities and users. In order to satisfy the need to have reliable processes to maintain over times the implementation of a public key infrastructure in the organization.

The work was carried in six chapters. In an initial phase, described the problem, objectives, scope and limitations of the work. In a second phase develops a brief technical perspective on the state of the art in cryptographic systems, describing their historical development, their advantages and disadvantages. Subsequently, has been developing a general description of the legal standards for the operation of an entity providing certification services. After studying the standards, describes the functional relationships between the various entities involved in the process of certification services, detailing each of the activities within the same (functions of the certifying authority, registration authority, users and / or associated systems). Having lifted the information required for its operation and the laws that around it, the models were developed in order to describe proper operation, using a layout formal and easy to understand as it is a description in BPMN notation. Finally, has been made an assessment and conclusion of this work.

ÍNDICE GENERAL

	Pág.
RESUMEN	i
ABSTRACT	ii
ÍNDICE DE TABLAS	v
ÍNDICE DE FIGURAS	vi
I. INTRODUCCIÓN	1
1.1. Problemática	1
1.2. Objetivo de la tesis	3
1.3. Objetivos específicos de la tesis	3
1.4. Alcances y limitaciones	3
II. DESCRIPCIÓN DE LOS SISTEMAS PKI	4
2.1. Criptografía de clave pública	4
2.1.1. Evolución histórica de la criptografía	4
2.1.2. Criptografía basada en sistemas simétricos	4
2.1.3. Criptografía basada en sistemas asimétricos de clave pública	5
2.2. Integridad y confiabilidad de un emisor	5
2.2.1. Certificado digital (CD)	6
2.2.2. Redes de confianza	6
2.2.3. Confianza de la autoridad certificadora (AC)	7
2.3. Arquitecturas de PKI basadas en el formato de certificados X.509	7
III. DESCRIPCIÓN GENERAL DE LAS NORMAS LEGALES PARA EL FUNCIONAMIENTO DE UNA EPSC	10
3.1. Marco legal y beneficios del empleo de la firma electrónica	10
3.1.1. Marco legal	10
3.1.2. Beneficios del empleo de certificados digitales	11
3.2. Criterios generales de acreditación	11
3.3. Requisitos de acreditación	12
3.4. Observaciones a los requisitos de acreditación	14
IV. RELACIONES ENTRE ENTIDADES Y FUNCIONAMIENTO GENERAL DE UNA ENTIDAD PSC	15
4.1. Relación funcional entre las entidades	15
4.2. Responsabilidades de las entidades	16
4.2.1. Autoridad certificadora (AC)	16
4.2.2. Autoridad de registro (AR)	16
4.2.3. Usuarios finales (UF)	16
4.2.4. Repositorio (REP)	16
4.3. Proceso general de la prestación de servicios de certificación	17

4.3.1.	Actividades del proceso general	18
4.3.2.	Detalle de actividades del proceso general	20
4.4.	Actividades de la autoridad certificadora	21
4.5.	Actividades de la autoridad de registro.....	22
4.6.	Herramienta definida para la gestión de la AC	22
V.	MODELO DE PROCESOS DEL SISTEMA	24
5.1.	Diagrama de relaciones funcionales entre las entidades.....	25
5.2.	Diagrama general del proceso de prestación de servicios de certificación.....	25
5.3.	Diagrama general del proceso de usuario	27
5.4.	Diagramas de la autoridad de registro	30
5.4.1.	Validar datos	30
5.4.2.	Enviar solicitud de certificado	32
5.4.3.	Entregar certificado.....	33
5.5.	Diagramas de la autoridad de certificadora	34
5.5.1.	Generar certificado.....	34
5.5.1.1.	Ingresar a la aplicación de AC	35
5.5.1.2.	Generar certificado de dispositivo	35
5.5.1.3.	Generar certificado personal	36
5.5.1.4.	Registro de datos en tabla de datos	36
5.5.2.	Enviar certificado.....	37
5.5.2.1.	Exportar certificado digital	38
5.5.2.2.	Grabar certificado digital	38
5.5.2.3.	Despachar certificado digital	39
5.5.3.	Cancelar certificado digital	40
5.5.3.1.	Revocar certificados.....	40
5.5.3.2.	Exportar lista de revocación de certificados	41
5.6.	Diagramas del repositorio	41
5.6.1.	Publicar certificados (Claves Públicas)	41
5.6.2.	Publicar LRC	42
VI.	EVALUACIÓN Y CONCLUSIONES	43
	GLOSARIO	48
	BIBLIOGRAFÍA	49
	A N E X O S.....	51
	ANEXO A: DESCRIPCIÓN DE NOTACIÓN BPMN UTILIZADA	52
	ANEXO B: ANTECEDENTES DE FUNCIONAMIENTO DE LA ENTIDAD PSC	58
	ANEXO C: DETALLE DE PROCEDIMIENTOS DENTRO DE LA ENTIDAD PCS	62

ÍNDICE DE TABLAS

	Pág.
Tabla N° IV-1	Actividades de prestación de servicios de certificación.....18
Tabla N° IV-2	Detalle de actividades del proceso21
Tabla N° A-1	Diagramas de objetos de flujo.....53
Tabla N° A-2	Diagramas de objetos de conexión.....55
Tabla N° A-3	Diagramas de los carriles55
Tabla N° A-4	Diagramas de los artefactos56
Tabla N° A-5	Resumen de elementos centrales de BPMN.....57
Tabla N° B-3a	Formato X.509 v359
Tabla N° B-3b	Estándar X.509 v359

ÍNDICE DE FIGURAS

	Pág.
Figura N° 4-1, Organización general de la entidad PSC.....	15
Figura N° 4-2, Ciclo de vida general de un certificado digital	17
Figura N° 4-3, Diagrama de entidades y casos de uso.....	18
Figura N° 4-4, Pantalla principal de TinyCA 0.7.3	23
Figura N° 5, Diagrama de BPMN del ciclo de vida del certificado digital	24
Figura N° 5-1, Relaciones funcionales entre las entidades	25
Figura N° 5-2, Diagrama general del proceso de la entidad PSC	26
Figura N° 5-3, Diagrama del proceso de usuario.....	28
Figura N° 5-4-1, Diagrama del proceso para validar datos	30
Figura N° 5-4-2, Diagrama proceso para enviar solicitud de certificado.....	32
Figura N° 5-4-3, Diagrama del proceso para entregar certificado	33
Figura N° 5-5-1, Diagrama del proceso para generar certificados.....	34
Figura N° 5-5-1-1, Diagrama del proceso para ingresar a la aplicación de AC	35
Figura N° 5-5-1-2, Diagrama del proceso para emitir certificado de dispositivo	35
Figura N° 5-5-1-3, Diagrama del proceso para emitir certificado personal	36
Figura N° 5-5-1-4, Diagrama del proceso para registro en tabla de datos	36
Figura N° 5-5-2, Diagrama del proceso para enviar certificado	37
Figura N° 5-5-2-1, Diagrama del proceso para exportar certificado digital.....	38
Figura N° 5-5-2-2, Diagrama del proceso para grabar certificado digital	38
Figura N° 5-5-2-3, Diagrama del proceso para despachar certificado digital	39
Figura N° 5-5-3, Diagrama del proceso para cancelar certificado	40
Figura N° 5-5-3-1, Diagrama del proceso para revocar certificado	40
Figura N° 5-5-3-2, Diagrama del proceso para exportar LRC	41
Figura N° 5-6-1, Diagrama del proceso para publicar certificados.....	41
Figura N° 5-6-2, Diagrama del proceso para publicar LRC.....	42

I. INTRODUCCIÓN

El hombre a través del tiempo se ha visto en la necesidad de transmitir mensajes con cierto nivel de seguridad, especialmente en el ámbito militar. La sociedad moderna no está ajena a este problema, es así como nuestros bancos, instituciones públicas, universidades y otros, requieren mantener un cierto nivel de privacidad en su información.

En la comunidad objetivo se ha estado liderando el desarrollo de un proyecto piloto desde el año 2009, con la finalidad de utilizar y posteriormente, masificar el empleo de la tecnología asociada al uso de certificados digitales y firma electrónica. Este sistema debiera estar actualmente en pleno funcionamiento, principalmente, en la firma de correos electrónicos en la intranet. Lamentablemente, no se ha estado utilizando en la actualidad por carecer de procedimientos claros que orienten a los usuarios y a la propia organización en su uso.

En este sentido, lo que se busca en este trabajo es entregar un diseño funcional de los procesos de una entidad prestadora de servicios de certificación a una comunidad objetivo de una institución de las FFAA. Producto de la alta rotación de su personal, se requiere contar con procesos que permitan mantener en el tiempo el funcionamiento de esta entidad y el activo del conocimiento asociado a este.

Por otra parte, para contar con un servicio de certificación de nivel de confianza y a su vez ser el inicio de la certificación de firma electrónica avanzada, es del todo necesario cumplir con los requisitos legales exigidos por el Gobierno de Chile al establecer una entidad prestadora de servicios de certificación (Ministerio de Economía, Fomento y Reconstrucción, 2002).

1.1. Problemática

Para mantener seguros los activos informáticos de la organización (principalmente en la transmisión de correos electrónicos a través de la intranet) se requiere contar con procedimientos que permitan brindar seguridad y confidencialidad a la información que se transmite a través de la red. Para dar solución a este problema, la comunidad objetivo ha estado impulsando el uso de un sistema de infraestructura de clave pública, en adelante **PKI** (del inglés "*Public Key Infrastructure*").

En criptografía, una PKI es una combinación de hardware y software, políticas y procedimientos, que permiten la ejecución de operaciones informáticas con plena garantía de seguridad; siendo las más importantes: el **cifrado**, la **firma digital**, la **autenticación** y el **no repudio** de transacciones electrónicas.

Su importancia radica en que la PKI permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados digitales de identidad (por ejemplo, las claves públicas de otros usuarios) para cifrar y descifrar mensajes, firmar digitalmente

información, garantizar que dicha información proviene efectivamente de la fuente emisora y que dicho mensaje no ha sido leído ni adulterado por ningún ente externo a quien envió y debió recibir el mensaje.

Una PKI se basa en la utilización de un **certificado digital** (CD), el cual consiste en un archivo electrónico que contiene al menos lo siguiente: los datos del propietario, los códigos que permiten la validación de firmas electrónicas y la firma electrónica de la autoridad certificadora (AC) que valida dicho certificado. Una **autoridad certificadora** es un aval que permite tener certeza que los datos del certificado digital corresponden al propietario (Carlisle Adams, 2002). Como certificado digital se entiende el documento oficial del propietario para hacer transacciones electrónicas, misma función que cumple un pasaporte o carné de identidad, tal como se define en la Ley 19.799 "Ley sobre documentos electrónicos, firma electrónica y servicios de certificación" (Ministerio de Economía, Fomento y Reconstrucción, 2002). Siendo esta autoridad certificadora equivalente al Registro Civil de Identificación.

Además, con la finalidad de extrapolar el funcionamiento de PKI en otras organizaciones externas a la comunidad objetivo, se debe contar con autoridades certificadoras que presten servicios en forma remota, esto quiere decir, que se requiere de una o varias entidades encargadas de validar la identidad de quienes no pueden asistir en forma personal a solicitar certificados digitales. Estas entidades son llamadas "autoridades de registro" (Carlisle Adams, 2002).

El funcionamiento conjunto de la autoridad certificadora, **autoridades de registro** y sistemas asociados, en la normativa chilena es denominada "Prestadora de servicios de certificación" (Ministerio de Economía, Fomento y Reconstrucción, 2002).

Es así que, con la finalidad de lograr la implementación de una entidad prestadora de servicios de certificación, durante el transcurso del año 2010 se puso en ejecución un plan piloto realizando las siguientes actividades: implementación técnica de la autoridad certificadora con empleo de una aplicación de fuente abierta; dotación de una organización que permita el funcionamiento de la entidad prestadora de servicios de certificación; levantamiento de requerimientos de usuarios de la comunidad objetivo; levantamiento de los procedimientos e instrucciones técnicas asociadas a dicha entidad. Todo lo anterior, con la finalidad de que la comunidad objetivo mantenga el activo del conocimiento en la organización o, si es necesario, traspasar dichos conocimientos a otra organización.

Para que esta autoridad certificadora garantice el empleo de la firma electrónica, debe cumplir con los mínimos requisitos legales exigidos para establecer una Prestadora de Servicios de Certificación (Ministerio de Economía, Fomento y Reconstrucción, 2002), quedando posteriormente en condiciones de ser acreditada si es necesario.

1.2. Objetivo de la tesis

El desarrollo de la presente tesis tiene por objetivo diseñar, conceptualmente, un proceso para el funcionamiento de una entidad prestadora de servicios de certificación tendiente a ser acreditada legalmente para la comunidad objetivo.

1.3. Objetivos específicos de la tesis

- 1.3.1.** Describir en forma general el ambiente operacional (hardware, software y comunicaciones) en la cual operará el sistema.
- 1.3.2.** Describir los aspectos a considerar para su funcionamiento y las características de una entidad prestadora de servicios de certificación.
- 1.3.3.** Detallar las normas legales y jurídicas exigibles por parte del gobierno a las instituciones públicas.
- 1.3.4.** Diseñar a nivel conceptual y mediante el empleo de “Business Process Modeling Notation” (BPMN), un modelo de proceso para el funcionamiento de una entidad prestadora de servicios de certificación, que se ajuste a la realidad nacional.

1.4. Alcances y limitaciones

La presente tesis está desarrollada a partir de un proyecto piloto, por lo que se parte de los estudios desarrollados previamente en la organización que cobija a la comunidad objetivo.

En este sentido, se parte de premisas ya trabajadas, de forma de permitir el modelamiento de los procesos elaborados. Esto permitió que este trabajo no se extendiera excesivamente y desvirtuara el tiempo y cumplimiento de los objetivos trazados.

El trabajo consta de una introducción en la cual se describe el objetivo de la presente tesis, la problemática, alcances y limitaciones. En el segundo capítulo se desarrolla una breve perspectiva técnica respecto al estado del arte en sistemas criptográficos, describiendo su desarrollo histórico, sus ventajas y desventajas. En el tercer capítulo se presenta una descripción general de las normas jurídicas y legales exigibles para el funcionamiento de la EPSC. En el cuarto capítulo se describen las relaciones funcionales entre las distintas entidades que participan en el proceso de servicios de certificación. En el quinto capítulo se presenta la descripción de detalle respecto a las actividades que se desarrollan al interior de una entidad prestadora de servicios de certificación (funciones de autoridad certificadora, autoridad de registro y sistemas asociados). En el sexto capítulo se presentan los diagramas BPMN elaborados para el modelo de funcionamiento de la entidad prestadora de servicios de certificación. Finalmente, en la última etapa se realiza un análisis y conclusiones al desarrollo del presente trabajo.

II. DESCRIPCIÓN DE LOS SISTEMAS PKI

La finalidad del presente capítulo es describir brevemente los sistemas criptológicos existentes, su evolución histórica, utilización de certificados digitales X.509 basados en PKI (*Public Key Infrastructure*), base teórica de los algoritmos de clave pública y entidades principales que conforman una PKI.

2.1. Criptografía de clave pública

2.1.1. Evolución histórica de la criptografía

El ser humano, a través del tiempo, se ha visto en la necesidad de transmitir mensajes con cierto nivel de seguridad, principalmente, en el ámbito militar. En la antigüedad se utilizaban patrones de transposición para transmitir mensajes secretos, los cuales dejaban reemplazar una letra por otra, permitiendo con esto ocultar el mensaje original, el problema se generaba porque el patrón de encriptación debía ser conocido tanto por el emisor del mensaje como por el receptor.

Para evitar que un mensaje se pudiera descifrar mediante técnicas de criptoanálisis, se ha ido evolucionando velozmente en los métodos criptográficos. En métodos más complejos se utiliza una contraseña asociada a un algoritmo, la cual debe ser utilizada en cada mensaje para su cifrado y descifrado, este método también exigía distribuir previamente el algoritmo y su contraseña.

El criptoanálisis ha ido avanzando en paralelo al desarrollo de los métodos criptográficos, ya que muchos de los métodos de cifrado que se han ido empleando en el tiempo presentan debilidades que los hacen vulnerables.

2.1.2. Criptografía basada en sistemas simétricos

Los sistemas criptográficos simétricos utilizan la misma clave para realizar el cifrado y descifrado del mensaje. Estos sistemas requieren de canales de comunicación seguros y de criptosistemas suficientemente robusto contra ataques criptoanalíticos o fuerza bruta.

Lamentablemente, los sistemas simétricos presentan el grave inconveniente que la clave de cifrado y descifrado del mensaje debe ser conocida por quien envía y recibe el mensaje, haciéndolo altamente vulnerable a la interceptación de un tercero; considerando más grave aún que se utilizan los mismos canales de transmisión del mensaje encriptado para el envío previo de la clave.

En la actualidad para minimizar el éxito de ataques por fuerza bruta o de ataques mediante métodos avanzados de criptoanálisis, se utilizan algoritmos de cifrado que emplean un espacio de claves muy grande (256 bits), lo que hace que el número de claves posible sea de 256^2 .

Con espacios de claves tan grandes, los ataques por fuerza bruta tendrían que emplear más tiempo en descifrar la clave, de lo que el universo ha tomado desde su creación a la fecha.

2.1.3. Criptografía basada en sistemas asimétricos de clave pública

Pese a que los sistemas simétricos ya habían sido perfeccionados y la longitud de sus claves hacía casi imposible un ataque por fuerza bruta, seguía siendo un grave problema el envío de la clave para descifrar el mensaje.

En este sentido, se considera revolucionaria la creación de criptosistemas en los que no fuera necesario el envío previo de claves para su cifrado y descifrado. Al contrario de los sistemas simétricos donde se utilizaba la misma clave para cifrar y descifrar el mensaje, tanto por el emisor como por el receptor respectivamente.

Los sistemas de clave pública emplean pares de claves, en la que una de ellas se emplea para cifrar información y la otra se emplea para descifrarla. Una de las claves se considera pública, pudiendo ser transmitida por canales que no presenten un gran nivel de seguridad, pudiendo ser empleada por cualquier persona que tenga acceso a la base de datos que contenga esta clave. La otra clave tiene carácter secreto, siendo sólo conocida y empleada por su propietario.

Este sistema de clave pública y privada, permite:

Cifrar la información: Esta función es similar a la empleada en los criptosistemas simétricos, pero en los criptosistemas asimétricos esta función tiene la particularidad de que el emisor debe emplear la clave pública del receptor del mensaje para que sólo él pueda descifrarla mediante el uso de su clave privada.

Firmar digitalmente el documento: Es una cadena de caracteres asociada a un mensaje digital. Una firma digital entrega al destinatario la seguridad de que el mensaje fue creado por el remitente (autenticidad de origen), y que no fue alterado durante la transmisión (integridad). La firma digital consiste en un método criptográfico que asocia la identidad de una persona o de un equipo informático, al mensaje o documento

2.2. Integridad y confiabilidad de un emisor

Los algoritmos de clave pública permiten firmar mensajes de tal forma de asegurar la relación entre una clave privada empleada para la firma y la clave pública correspondiente a quien firmó el mensaje.

De esta forma, un usuario al tener un par de claves (pública y privada), permite inferir que si se tiene absoluta certeza que la clave pública de un usuario es, realmente, de quien dice ser, se asegura que cualquier mensaje que haya sido firmado con la clave privada de este, procede efectivamente de él. Pero aún existen algunos inconvenientes:

- ¿Cómo tener certeza absoluta que cierta clave pública pertenece realmente a una persona o institución?
- ¿Cómo saber que cierto par de claves ya no es confiable para determinar la identidad de una persona o institución producto del acceso a las claves privadas por parte de un tercero?

Para dar solución a estas incógnitas, se utiliza el certificado digital (CD), bajo dos soluciones distintas: Las redes de confianza y las autoridades de certificación (AC).

2.2.1. Certificado digital (CD)

Un certificado digital se define como un documento electrónico que asocia una clave pública con una serie de datos (nombre, dirección, correo electrónico, organización, etc.) similar al carné de identidad del propietario de la clave. Para hacer confiable este certificado, se incorpora una firma electrónica a dicho documento:

- En las redes de confianza, es el propio titular del certificado quien lo firma con su clave privada. Esta firma puede ser validada, posteriormente, por usuarios quienes certifican la veracidad del mismo.
- En el caso de las autoridades certificadoras, es esta autoridad quien firma con su clave privada el certificado digital de un determinado usuario, certificando que es, realmente, quien dice ser.

2.2.2. Redes de confianza

Se basa en un modelo de confianza descentralizado bajo un concepto de una comunidad virtual, existiendo un sinnúmero de redes de confianza independientes. Una red de confianza es un concepto utilizado para establecer la correlación entre una clave pública y un usuario determinado.

El concepto de red de confianza se emplea, principalmente, en los sistemas PGP, GnuPG¹ y otros compatibles con la norma OpenPGP². Los certificados de identidad de OpenPGP incluyen datos personales del propietario como su clave pública, el que puede ser firmado por otros usuarios respaldando la asociación de esa clave pública con la persona o entidad

¹ *GNU Privacy Guard*, una herramienta de cifrado de archivos.

² *Pretty Good Privacy* es un programa desarrollado por Phil Zimmermann.

indicada en el certificado digital. Para esto existen servidores donde se almacenan los certificados digitales que son de libre acceso desde internet.

Un problema que se genera en las redes de confianza, radica principalmente, en que nuevos usuarios con certificados no se considerarán confiables por el resto de usuarios, especialmente, porque no se conocen físicamente, lo que se traduce en un problema mayúsculo si los usuarios se encuentran a grandes distancias uno del otro.

2.2.3. Confianza de la autoridad certificadora (AC)

Este es un modelo de confianza centralizado y depositado en una autoridad de certificación. En estos modelos las autoridades de certificación son los encargados de emitir los certificados tras verificar la identidad del titular, validando, mediante su firma electrónica la identidad del usuario.

En estos sistemas existe y se emplea el concepto de jerarquías y rutas de certificación: una autoridad de certificación, puede delegar en otras entidades de nivel jerárquico inferior la capacidad de desempeñar funciones de autoridad de certificación, lo que genera un árbol jerárquico de certificación. La ruta dentro del árbol que une el certificado raíz con un certificado dado, es lo que se denomina ruta del certificado.

Uno de los principales problemas que se presenta en los sistemas basados en autoridades de certificación es la dificultad de comprobar la fidelidad de los datos suministrados por el usuario solicitante del certificado digital, debiendo emplear engorrosos métodos para corroborar la identidad.

El mayor riesgo existente en este sistema, es la vulnerabilidad de la clave secreta de la autoridad certificadora, de caer en manos de un tercero no autorizado, vulneraría la confianza de todos los certificados validados por dicha autoridad. Otro peligro que afecta a estos sistemas es la existencia de un eventual engaño a la autoridad certificadora, falseando la identidad de quien supuestamente solicita validar un certificado digital.

2.3. Arquitecturas de PKI basadas en el formato de certificados X.509

El X.509, fue publicado oficialmente en 1988 y asume un sistema jerárquico estricto de autoridades de certificación (AC) para emisión de certificados. Esto contrasta con modelos de redes de confianza (PGP), donde cualquier usuario puede validar un certificado de otro usuario.

Tras su publicación, el RFC 1422 (*request for comments*) escrito en 1993, describe una primera aproximación para el empleo de la infraestructura de autenticación X.509 en entornos TCP/IP y OSI, tanto para correo electrónico seguro (*Privacy-Enhanced Mail*,

PEM) como para otros protocolos. Dentro de este enfoque se puede destacar las siguientes características:

- La infraestructura de gestión de certificados para uso en internet, se debería acomodar a unas políticas de certificación diseñadas con buen criterio y claramente definidas, tanto para usuarios como para organizaciones.
- Los procedimientos para autenticar emisores y receptores dentro de la transmisión y entrega de un mensaje deberían ser sencillos, automatizados y uniformes, a pesar de la existencia de distintas políticas de gestión de certificados. Los usuarios no deberían realizar ningún proceso de revisión para evaluar la credibilidad otorgada a la identidad indicada por un certificado.
- El RFC 1422 anticipaba que el sistema RSA3 sería el algoritmo principal de firma al establecer una jerarquía de certificación en internet. De hecho, se afirma que se había llegado a acuerdos para facilitar el uso de este algoritmo en la parte de internet incluida dentro de las fronteras estadounidenses, considerando que RSA estaba patentado.

La IPRA⁴ establecería políticas globales descritas en el RFC que se aplicarían a todo certificado creado bajo su jerarquía. Bajo el certificado raíz de IPRA se encontrarían las autoridades de certificación (ACs), cada una de las cuales establecería y publicaría (mediante un RFC informativo) sus políticas para registro de usuarios y organizaciones.

En noviembre de 1993, se actualizó la versión X.509 que pasó a X.509 v2, incorporándose dos nuevos campos que permitían identificar inequívocamente las claves del emisor del certificado y del titular del mismo.

En respuesta a los requisitos de contar con nuevos campos dentro de los certificados que permitieran portar información necesaria, se desarrolló el formato de certificado X.509 v3. Este formato añade al formato X.509 v2 la posibilidad de incorporar campos adicionales en forma de extensión. Los distintos tipos de campos de extensión pueden ser definidos y registrados por cualquier organización o grupo. Los trabajos de estandarización del formato básico v3 se finalizaron en junio de 1996.

Junto al formato X.509 v3 se definía el formato de listas de certificados revocados. En estos trabajos de estandarización, también se desarrollaron ciertas extensiones estándar, que podían incluir información adicional sobre el titular, propiedades de la clave, información sobre la política y restricciones de la ruta de certificación. La capacidad de los certificados X.509 v3 permitió darle la flexibilidad necesaria para su uso general en internet.

³ **RSA** de sus autores Rivest, Shamir y Adleman, es un sistema criptográfico de clave pública desarrollado en 1977.

⁴ **IPRA** (*Internet Policy Registration Authority*) actúa como la raíz de la jerarquía de certificación para la comunidad de internet.

En enero de 1999 se publicó el RFC 2459 con el objetivo de crear restricciones de flexibilidad para el estándar X.509 v3, desarrollando un protocolo para el uso de las extensiones de este estándar en internet. Este RFC define en la arquitectura de un sistema PKI:

- a) Autoridades certificadoras (AC)
- b) Autoridades de Registro (AR)
- c) Usuarios
- d) Repositorio o Directorio de servicios.

En abril de 2002 se publicó el RFC 3280 que actualizaba y completaba al RFC 2459. Los cambios se centraban en incluir un algoritmo para determinar el estado (revocado o no) de un certificado y se añadían nuevas extensiones al estándar.

Finalmente en mayo del 2008 y después de varias mejoras en la implementación del estándar X.509 v3, se publicaba el RFC 5280 que se podría considerar una nueva edición corregida del RFC 3280. Las diferencias más importantes son:

- Soporte mejorado para nombres con caracteres internacionales, con reglas para la codificación y comparación de nombres de dominio internacionalizados y nombres distintivos (*Distinguished names*, DN).
- Se clarifican las reglas para el manejo de extensiones de LRC.

III. DESCRIPCIÓN GENERAL DE LAS NORMAS LEGALES PARA EL FUNCIONAMIENTO DE UNA EPSC.

La finalidad del presente capítulo es describir, brevemente, el marco legal exigido para desarrollar una infraestructura de clave pública, los beneficios de su empleo, su organización general y las responsabilidades de sus integrantes; todo lo anterior con la finalidad de fomentar e implementar el uso de certificados digitales en la organización.

3.1. Marco legal y beneficios del empleo de la firma electrónica

3.1.1. Marco legal

Durante el año 2002 se promulgó en Chile la “Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma” N° 19.799 y su reglamentación correspondiente (Ministerio de Economía, Fomento y Reconstrucción, 2002), en la cual se determina la forma legal del documento electrónico y se define la firma electrónica como cualquier sonido, símbolo o proceso electrónico que permite identificar, formalmente, a su autor, definiendo además:

- a) **Firma electrónica avanzada**, como aquella certificada por una entidad prestadora acreditada que cumpla con ciertas características de verificación, estableciendo quién puede proveer certificados y bajo qué condiciones poder hacerlo.
- b) **Prestadora de servicios de certificación**, como aquella entidad que cumple con lo necesario para dar fe del vínculo entre el firmante de un documento electrónico o titular del certificado digital y los datos del usuario de dicho certificado y su firma electrónica asociada.

Producto de lo anterior, la Contraloría General de la República emite el dictamen N° 4941 “Firma electrónica de los servicios públicos”, la cual autoriza el empleo de la firma electrónica por parte de los organismo públicos.

Por otra parte, el 12 ENE 2005 el Ministerio Secretaría General de la Presidencia promulga el Decreto N° 83 “Aprueba la norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos”, en donde se establece el uso de firma electrónica como una medida de seguridad para dotar de confidencialidad, integridad y autenticidad a los documentos electrónicos.

Por su parte, el Ministerio de Economía, Fomento y Reconstrucción, elaboró una guía de evaluación “Procedimiento de acreditación prestadores de servicios de certificación”. Documento que puede ser empleado por una organización para reconocer los requisitos y estándares que deben cumplir, con la finalidad de asegurar el nivel mínimo de confiabilidad que requiere el sistema y así obtener la certificación que lo acredite para emitir certificados digitales de acuerdo a lo dispuesto en la Ley 19.799.

3.1.2. Beneficios del empleo de certificados digitales

El empleo de certificados digitales otorga la capacidad de emplear la firma electrónica al interior de la organización, lo que permite beneficiarse de las siguientes capacidades:

- a) Firmar documentos electrónicos, permitiendo **autenticar** la autoría de estos y verificar la **integridad** de los mismos, es decir, que no han sido alterados después de efectuada la firma.
- b) Cifrar documentos electrónicos, otorgando **confidencialidad** al proteger el acceso a la información contenida en estos y **disponibilidad**, ya que sólo serán accesibles para el autor y las entidades que él decida.
- c) Establecer un **sello de tiempo** en la documentación electrónica, garantizando de esta forma la fecha y hora de firma de éstos, atributo relevante en el ámbito comercial y legal.
- d) Establecer enlaces de comunicaciones seguros, permitiendo **proteger** los servicios de correo electrónico y servicios Web, además de autenticar e identificar a los usuarios en el acceso a servicios informáticos.

Estos beneficios permiten reducir la impresión de documentación que no catalogue como secreta, lo que otorgará la capacidad de emplear sistemas electrónicos en la generación, transporte, gestión y almacenamiento de la documentación electrónica, derivando en un empleo más eficiente de los recursos a largo plazo, beneficiando a la organización entre otros aspectos, de:

- a) Disminuir la necesidad de emplear servicios de valijas, correos y todo lo referido a costos de entrega.
- b) Reducir, drásticamente, la impresión de documentación.
- c) Emplear sistemas de gestión documental electrónicos para el control de salida, entrada y seguimiento de los documentos con codificación única para cada documento.
- d) Disminuir el empleo de espacio físico para el almacenamiento de la documentación impresa.
- e) Disminución del riesgo de seguridad en cuanto a pérdida de documentación por traslado humano.

Todos estos beneficios en reducción de costos, ya han sido probados por variadas organizaciones con resultados positivos. Por ejemplo, el Registro Civil e Identificación, fomenta el uso de certificados electrónicos como una forma de reducir costos y agilizar sus transacciones.

3.2. Criterios generales de acreditación

En un futuro cercano y con la finalidad de obtener una acreditación, se determina el cumplimiento de los requisitos y los criterios generales que orientan la ejecución de la

acreditación para cada uno de los requisitos. En términos resumidos, se debe cumplir con lo siguiente:

a) **Transparencia**

Disposición pública de requerimientos de información que tienden a dar a conocer el estado del sistema de certificación, proporcionando confianza a los usuarios, conforme a las normas y acuerdos internacionales.

b) **Interoperabilidad internacional**

Fomentar la compatibilidad con estándares internacionales.

c) **Gradualidad**

La acreditación tiende a ser gradual, se debe ir adaptando desde exigencias que apuntan a cumplir con lo suficiente para dar confianza y su compatibilidad con la realidad nacional, hasta el cumplimiento estricto de los estándares internacionales a medida que el desarrollo de la actividad lo requiera.

d) **Independencia**

Asegurar la independencia de los entes reguladores. La entidad acreditadora y los evaluadores no podrán ser participantes directos del proceso de servicios de certificación ni tener vínculos contractuales con estas organizaciones.

e) **Neutralidad tecnológica**

Promover el desarrollo tecnológico y mejoramiento de calidad de servicios, sin preferencia tecnológica en particular.

f) **Privacidad**

Compromiso de la autoridad acreditadora de no usar ni divulgar la información clasificada como confidencial y que fue entregada por la entidad prestadora de servicios de certificación. Esto es extensible además, a todo organismo y persona que intervenga en el proceso de acreditación.

3.3. Requisitos de acreditación

Son los aspectos que deben ser cumplidos para que una organización obtenga la acreditación en conformidad a lo descrito en la Ley 19.799 y especificado en la publicación “Procedimiento de acreditación de prestadores de servicios de certificación” (Ministerio de Economía, Fomento y Reconstrucción, 2002):

a) **Requisitos de admisibilidad (AS01)**

Requisitos necesarios para iniciar la evaluación, incluye la presentación de la documentación exigida, la entrega del comprobante de pago de costos de acreditación y el cumplimiento de los plazos determinados para la entrega de la documentación que quedará pendiente.

b) **Requisitos generales de la Ley 19799 y su reglamento (RG01)**

Todos aquellos aspectos relacionados con el cumplimiento de plazos y procedimientos de acreditación.

c) **Aspectos legales y de privacidad (LE01)**

Aquellos relacionados con la comprobación de la documentación legal solicitada.

- d) Aspectos tecnológicos básicos
Requisitos específicos de la ley y su reglamentación, Estos requisitos se dividen en:
 - i) Estructura e información del certificado de firma electrónica (TB01).
 - ii) Estructura e información de la lista de certificados revocados (TB02).
 - iii) Servicios, información y accesibilidad del registro público (TB03).
 - iv) Modelo de confianza (TB04).
- e) Seguridad
Requisitos que permiten determinar el nivel de seguridad que se dispone para dar estos servicios. Están relacionados con la valoración de riesgos y amenazas, la implementación de salvaguardas de seguridad y planes asociados. Estos requisitos se dividen en:
 - i) Documentación y mantención de la política de seguridad (PS01).
 - ii) Revisión del análisis de riesgos y amenazas (PS02).
 - iii) Plan de continuidad del negocio y recuperación de desastres (PS03).
 - iv) Plan de seguridad de sistemas y administración de claves (PS04).
 - v) Evaluación de la implementación del plan de seguridad de sistemas (PS05).
 - vi) Evaluación del plan de administración de Claves (PS06).
- f) Evaluación tecnológica (ET01)
Requisitos relacionados con el cumplimiento de estándares de la plataforma tecnológica de emisión de certificados de firma electrónica y datos de creación de firmas.
- g) Seguridad física (SF01)
Requisitos de salvaguardas físicos tomados para proteger las áreas sensibles, equipos e información.
- h) Política
Implementación de políticas de certificación de firma electrónica. Estos se dividen en:
 - i) Política de los certificados de firma avanzada (PO01).
 - ii) Declaración de prácticas de certificación (PO02).
 - iii) Modelo operacional de la AC (PO03).
 - iv) Modelo operacional de la AR (PO04).
- i) Administración
Especificación de operaciones y gestión de certificación y registro, la asignación de funciones y responsabilidad del personal, planes de entrenamiento, etc. Estos se dividen en:
 - i) Manual de operaciones de la AC (AD01).
 - ii) Manual de operaciones de la AR (AD02).
- j) Examen del Personal
Requerimientos del personal que maneja información sensible y del oficial de seguridad. Estos se dividen en:
 - i) Evaluación de detalle de los perfiles del personal al nivel altamente confiable

- (PE01).
- ii) Evaluación del oficial de seguridad de la instalación (PE02).

3.4. Observaciones a los requisitos de acreditación

Respecto al cumplimiento de los requisitos de acreditación, necesarios para potenciar a la organización y posibilitar una tendencia a su futura certificación por un organismo externo, se puede detallar lo siguiente:

- a) De los requisitos anteriores, en este documento se tocan en forma tangencial los requisitos estipulados en el punto h) “políticas”, específicamente los del “Modelo operacional” de la AC (PO03) y AR (PO04). Por cuanto, este documento, sugiere la adopción de una serie de políticas para el funcionamiento de las entidades involucradas.
- b) Los requisitos “tecnológicos básicos”, “Seguridad”, “Evaluación tecnológica”, “Seguridad física” y “Administración”, de los puntos d), e), f), g) e i) en el orden respectivo, están bien desarrollados.
- c) Los requisitos, “requisitos de admisibilidad”, “Requisitos generales de la Ley 19799 y su reglamento” “Aspectos legales y de privacidad” y “Examen al personal”, de los puntos a), b), c) y j) en el orden respectivo, se deben cumplir en el momento mismo de la acreditación y además presentan la posibilidad de posponerlos.
- d) Considerando que la finalidad de establecer los modelos operacionales es asegurar la implementación de un sistema acorde a las políticas de certificación definidas, asegurando su normal funcionamiento y permanencia en el tiempo, se estima que es de suma importancia que estos sean, correctamente, definidos y documentados.
- e) Para cumplir con las exigencias es obligatorio elaborar la documentación del modelo de funcionamiento, el cual debe cumplir con los requisitos y obligaciones que dispone la Ley y su reglamentación.

IV. RELACIONES ENTRE ENTIDADES Y FUNCIONAMIENTO GENERAL DE UNA ENTIDAD PSC

Para modelar los procesos de funcionamiento requeridos se debió determinar las tareas y actividades de cada una de las entidades involucradas en este proceso. Esta EPSC está formada por tres entidades o roles principales: **autoridad certificadora**, **autoridad de registro** y **usuarios finales** que son los integrantes de la organización que emplean los certificados. A estos tres roles principales se suma como otra entidad, el **repositorio**. Teniendo, finalmente, cuatro entidades constitutivas en el proceso general de una EPSC.

4.1. Relación funcional entre las entidades

De acuerdo a lo que establece el estándar X.509 (IETF, 2002) y lo determinado en la Norma Chilena y otros textos para la gestión de los certificados digitales e implementación de una EPSC, se identificaron y establecieron las entidades involucradas en el proceso general, que se representan en la siguiente figura:

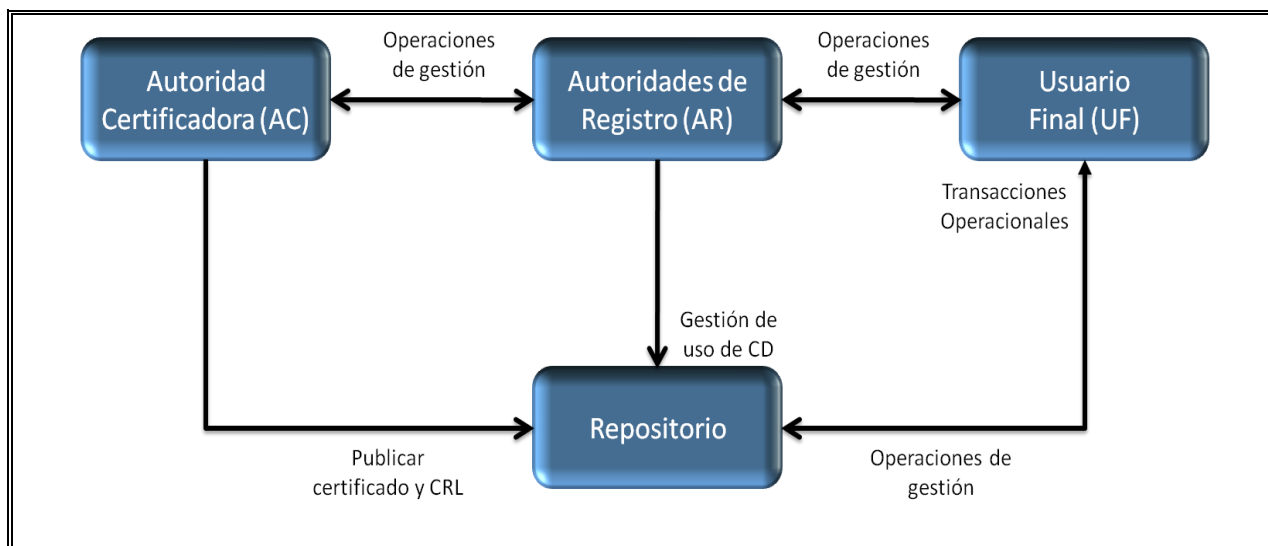


Figura N° 4-1, Organización general de la entidad PSC⁵

En la figura N° 4-1, se representan los principales roles e interacciones involucradas en el proceso general de una EPSC, conforme a al RFC 2459:

- Autoridad certificadora (AC).
- Autoridad de registro (AR).
- Directorio de los servicios o repositorio (REP).
- Usuarios finales (UF), que no forman parte de la entidad prestadora de servicios de certificación pero que hacen uso de los certificados digitales.

⁵ Arquitectura de PKI conforme al RFC 2459

4.2. Responsabilidades de las entidades

Para el funcionamiento del proyecto piloto de acuerdo al estándar X.509, se determinaron las siguientes responsabilidades generales:

4.2.1. Autoridad certificadora (AC)

Con la responsabilidad de:

- a) Generar los certificados digitales.
- b) Gestionar los certificados digitales y servicios relacionados.
- c) Cancelar certificados digitales, generando las listas de revocaciones.
- d) Mantener el repositorio mediante servicio de acceso público con las claves públicas y listas de revocaciones.

Para la operación de la AC se estableció el desempeño de los siguientes roles:

- a) Jefe de la AC, responsable por el funcionamiento y correcta ejecución de todas sus actividades de certificación acorde a las normas estipuladas.
- b) Administrador de la AC, responsable de desarrollar las actividades de:
 - i) Instalación de sistemas.
 - ii) Procedimiento de respaldos al servidor de la AC.
 - iii) Administración del sitio WEB de la AC.
- c) Operador de sistemas, responsable de desarrollar las siguientes funciones:
 - i) Procedimientos de gestión de certificados digitales.
 - ii) Procedimientos de actualización de datos en el servicio del repositorio.

4.2.2. Autoridad de registro (AR)

Tiene la responsabilidad de:

- a) Verificar la identidad de los usuarios finales.
- b) Solicitar la emisión de certificados digitales a la autoridad certificadora.
- c) Distribuir los certificados digitales, siendo el intermediario entre la autoridad certificadora y los usuarios finales.
- d) Verificar el buen empleo de los certificados digitales por parte de los usuarios.

4.2.3. Usuarios finales (UF)

Son quienes utilizan los certificados digitales y tienen la responsabilidad de:

- a) Solicitar a través de la AR la generación de certificados digitales por parte de la AC y el envío del mismo al usuario.
- b) Solicitar a la AC, a través de la AR, la validación del certificado digital generado por el propio usuario y la respectiva publicación de su clave pública para conocimiento de todos los integrantes de la organización.

4.2.4. Repositorio (REP)

Cumple con el objetivo de:

- a) Mantener las claves públicas de los usuarios para el acceso público de todos los usuarios del sistema.
- b) Mantener la lista de certificados revocados que han sido previamente caducados o invalidados.

4.3. Proceso general de la prestación de servicios de certificación

En la Figura N° 4-2 se muestra un diagrama que representa el ciclo de vida (CV) del certificado digital. Está compuesto por diez actividades, pero dos (Solicitud / renovación de certificado y Empleo del certificado) son propias del usuario final, es decir, son parte del ciclo de vida, pero no del proceso directo de prestación de servicios de certificación.

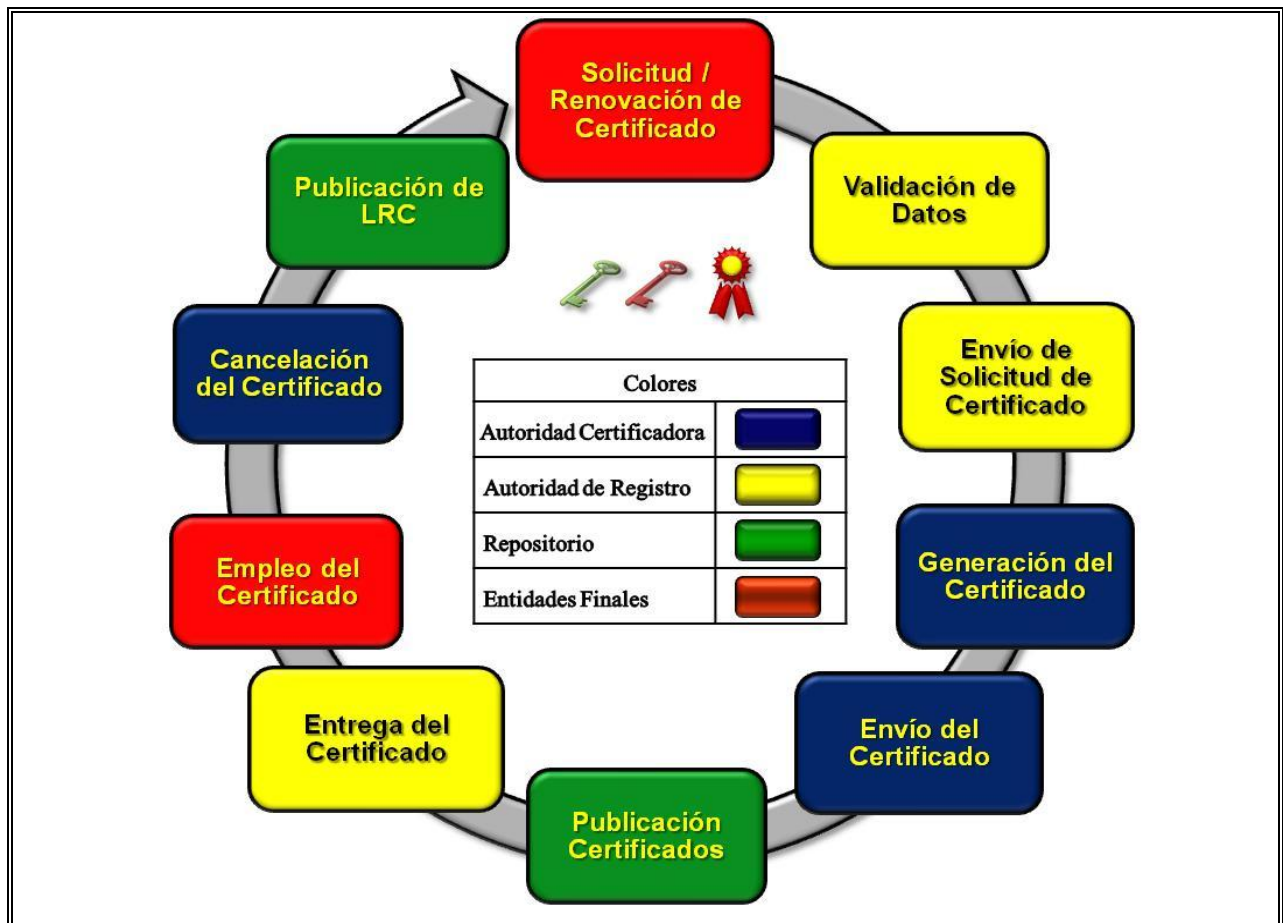


Figura N° 4-2, Ciclo de vida general de un certificado digital

Por otra parte en la siguiente Figura N° 4-3, se muestra el diagrama de las entidades y casos de uso involucrados del ciclo de vida anterior, con sus 10 actividades asociadas y e interacciones entre sus integrantes.

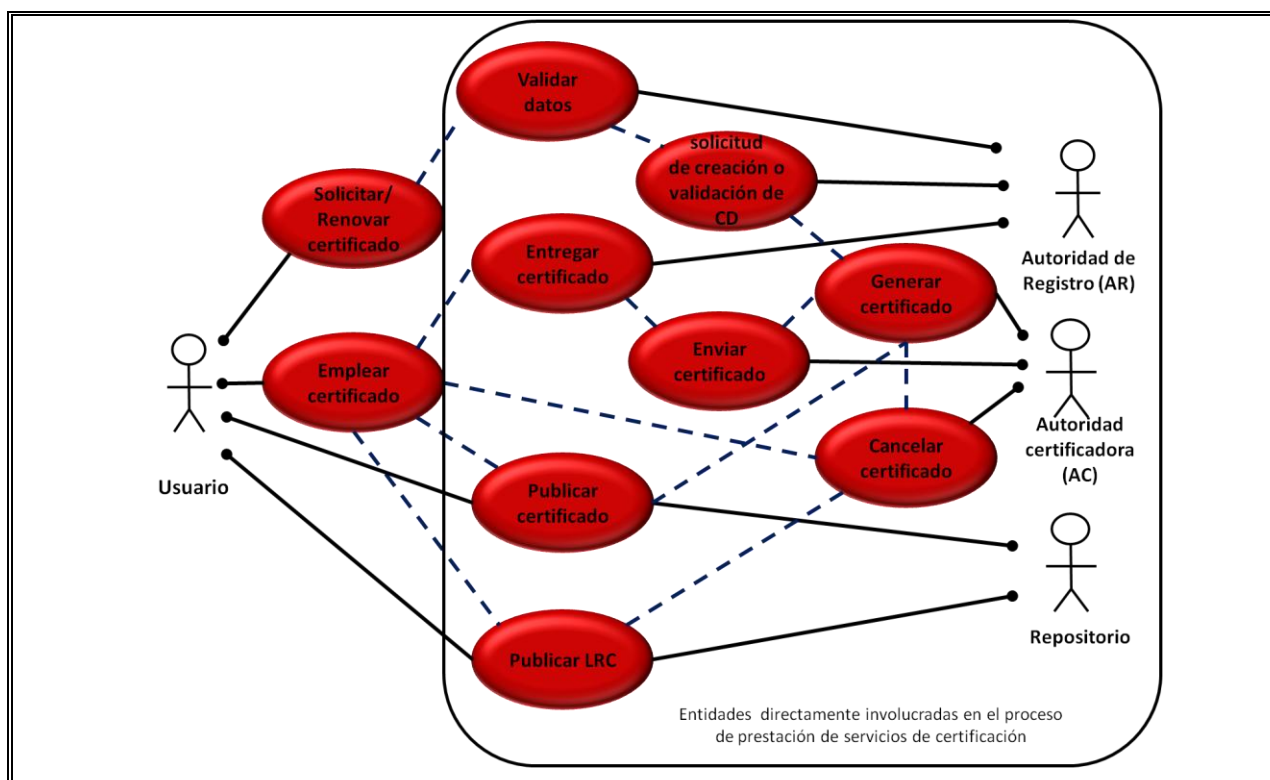


Figura N° 4-3, Diagrama de entidades y casos de uso

En el diagrama anterior, con línea continua, se pueden apreciar las actividades que son responsabilidades directas de cada una de las entidades involucradas en el proceso y con línea segmentada, la asociación entre las mismas, que a su vez, se relacionan indirectamente a tareas directas de otras entidades. Por otra parte, para un mejor entendimiento, se enmarcan en el recuadro aquellas entidades que tienen una responsabilidad directa en el proceso de una EPSC, siendo el usuario final, quien se comporta como cliente y quien hace uso del servicio que entrega dicha EPSC.

4.3.1. Actividades del proceso general

La siguiente Tabla N° IV-1, muestra un resumen de las actividades del proceso general implementado.

Tabla N° IV-1 Actividades de prestación de servicios de certificación.

N°	Nombre Actividad	Descripción
1	Solicitud de Certificado	Petición a la AC de un certificado digital por necesidad de la organización, del usuario final, por caducación, revocación o bien, la validación del certificado creado por el propio usuario.

N°	Nombre Actividad	Descripción
2	Validación de Datos	Validación en presencia del usuario final y verificación de los datos personales del usuario. La solicitud debe ser validada en el sistema de la AC. Si no existe AR, se debe validar los datos por el procedimiento alternativo, mediante documento certificado a la AR del nivel organizacional superior.
3	Envío de solicitud de certificado	Si el sistema de la AC está disponible, sólo se debe confirmar el envío de las solicitudes de certificado, si la validación de datos está correcta. En caso contrario y como procedimiento alternativo, se debe enviar a la AC la solicitud en sobre sellado y firmado por el operador de la AR.
4	Generación de Certificado	<p>Al recibir una solicitud:</p> <ol style="list-style-type: none"> 1 Verificar integridad de la solicitud, extracción de datos y verificación de datos. 2 Si se presentan problemas de integridad y/o en los datos, se desecha y elimina, enviando un aviso por correo electrónico a la AR correspondiente. 3 Si todo está en orden se procede a la “Generación del par de claves” y a la “Creación del certificado” correspondiente. 4 Se procede al “Respaldo del certificado”, almacenar en un lugar seguro los certificados emitidos.
5	Envío de Certificado	<p>Al emitir un certificado de un usuario o validarlo:</p> <ol style="list-style-type: none"> 1 Se procede a exportar el certificado. 2 Se procede a la grabación del certificado en un medio seguro. 3 El certificado es despachado a la AR correspondiente para su entrega. Si es por renovación se envía por medio protegido directamente al usuario final.
6	Publicación de Certificados	Al recibir el archivo con la actualización de las claves públicas, se publican estas claves en un sitio Web de la Intranet, permitiendo de esta forma que todos quienes quieran cifrar y firmar documentos electrónicos, tengan acceso a las claves públicas del resto de los usuarios.

N°	Nombre Actividad	Descripción
7	Entrega de Certificado	<p>Al recibir un certificado de la AC, la AR debe contactarse con el usuario final o encargado del dispositivo que hará uso del certificado digital para hacerle entrega de éste en forma personal.</p> <p>Al recibir el aviso que un certificado está listo para la entrega y el sistema reporta que ha pasado una semana sin ser descargado, se debe informar al usuario final que debe realizar la descarga respectiva.</p>
8	Empleo del Certificado	<p>Al recibir un certificado, la entidad final puede emplear su certificado digital para mantener la correspondencia cifrada, firmar correos y documentos.</p>
9	Cancelación	<p>Revocar o proceder a la cancelación de un certificado digital:</p> <ol style="list-style-type: none"> 1. Al “Caducar un certificado” por termino de vida útil, si es del caso. 2. Al recibir una solicitud de “Revocación de certificado” por parte de un usuario final. 3. Al recibir una solicitud de “Revocación de certificado” por parte de una AR, reportando un mal uso. <p>Se debe incluir el certificado correspondiente en la LRC, enviando esta al repositorio para mantener el “Historial de claves” y “Archivo de certificados revocados”.</p>
10	Publicación de LRC	<p>Al recibir una actualización de la LRC por parte de la AC, publicar la LRC actualizada, permitiendo de esta forma informar a los usuarios finales, a través de la WEB intranet, de los certificados que están caducados.</p>

4.3.2. Detalle de actividades del proceso general

En la siguiente Tabla N° IV-2 se delimitaron las responsabilidades, nombres, iniciadores de las actividades y entidades involucradas en proceso general.

Tabla N° IV-2 Detalle de actividades del proceso

N°	Nombre Actividad (Qué)	Responsable (Quién)	Iniciador (Cuándo)	Entidades Involucradas
1	Solicitud de Certificado o validación	• UF	Por necesidad de la organización, del usuario final, por caducación o revocación.	• AR
2	Validación de Datos	• AR	Al recibir en presencia del UF el documento de la solicitud.	• UF
3	Envío de solicitud de certificado	• AR	Al confirmar el envío de las solicitudes de certificado a la AC, si la validación de datos está correcta.	• AC
4	Generación de Certificado	• AC	Al recibir una solicitud de certificado, por parte de la AR.	• AR • UF • REP
5	Envío de Certificado a AR	• AC	Al exportar, grabar y despachar certificados a las respectivas AR de los UF.	• AR • UF
6	Publicación de Certificados	• AC	Al poseer el archivo con las claves públicas.	• UF • REP
7	Entrega de Certificado	• AR	Al recibir un certificado digital de la AC para un UF.	• UF • AC
8	Empleo del Certificado	• UF	Al recibir un certificado por parte de la AR, si es la primera solicitud, o por parte de la AC si es una renovación.	• AR • AC • REP
9	Cancelación de certificado (Caducación y Revocación)	• AC	Al caducar un certificado por termino de vida útil, si es del caso. Al recibir solicitud de revocación por parte de un UF. Al recibir solicitud de revocación por parte de una AR, reportando un mal uso.	• AR • UF • REP
10	Publicación de LRC	• AC	Al recibir una actualización de la LRC por parte de la AC.	• UF • REP

De este proceso general, se derivan las tareas y las actividades de detalles de los procesos de la autoridad certificadora y autoridad de registro, como entidades fundamentales dentro del proceso de prestación de servicios de certificación.

4.4. Actividades de la autoridad certificadora

De acuerdo al proceso general de la Tabla N° IV-2, las actividades de ámbito de la autoridad certificadora son las detalladas en puntos N° 4, 5, 6, 9 y 10 de la respectiva tabla. Siendo estas, las que permiten establecer los procedimientos de detalle para la emisión,

revocación y listas de revocación de certificados digitales, para su adecuado funcionamiento y repositorio.

Las actividades administrativas y de seguridad, tales como: las de almacenamiento y respaldo de dichos certificados, lista de revocación e información de los usuarios finales, además de las acciones necesarias para recuperar a la autoridad certificadora en caso de eventos significativos, no serán considerados en el diagrama de este modelo, ya que son parte de los procedimientos de seguridad y de administración.

Por lo tanto, a la autoridad certificadora le corresponden las siguientes actividades:

- a) Generación de certificado.
- b) Emisión de certificado.
- c) Actualización datos en el repositorio.
- d) Envío de certificado.
- e) Cancelación de certificado.
- f) Publicación de certificados públicos (usuario final).
- g) Publicación de listas de revocación a través del repositorio (usuario final).

Se observa que los puntos f) y g) son actividades del usuario final, pero serán modeladas como parte de las responsabilidades que en la práctica asume la AC como fragmento de sus funciones.

4.5. Actividades de la autoridad de registro

Las actividades de ámbito de la autoridad de registro, de acuerdo al proceso general, son las detalladas en puntos N° 2, 3 y 7, Tabla N° IV-2. Siendo estas, las que permiten establecer los procedimientos de detalle para validar y cursar solicitudes y uso de los certificados digitales, entregando instrucciones a la autoridad de registro e integrantes de la organización solicitantes.

Por otra parte, las actividades de esta autoridad deberían ser desempeñadas como una entidad con capacidad para validar los datos personales de los solicitantes, debiendo contar con un servicio que permita administrar los datos de estos, así como interactuar con la autoridad de certificadora y el repositorio.

Por lo tanto, a la autoridad de registro le corresponden las siguientes actividades:

- a) Validación de datos personales.
- b) Enviar solicitud de creación o validación de certificado a la AC.
- c) Entrega de certificado digital al UF.

4.6. Herramienta definida para la gestión de la AC

La herramienta definida por la organización para la gestión de una autoridad certificadora, en su proyecto piloto, es la aplicación gráfica TinyCA. Esta aplicación fue creada por Stephan Martin en 2002, liberada en abril de 2005.

El programa TinyCA está realizado en el lenguaje interpretado Perl (*Practical extraction and report language*)⁶, empleando como “*toolkit*” gráfico GTK+⁷.

Para la gestión criptográfica, TinyCA emplea llamadas al ejecutable del programa binario openSSL, lo que lo obliga a utilizar el mismo formato de almacenamiento, ficheros y directorios generados por openSSL⁸.

En la Figura N° 4-4, se muestra la pantalla principal de la aplicación TinyCA 0.7.3, que fue definida, previamente, por la organización.

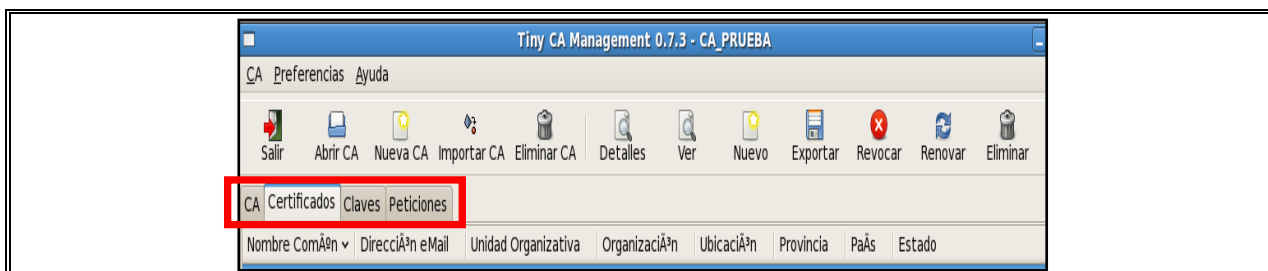


Figura N° 4-4, Pantalla principal de TinyCA 0.7.3

La interfaz gráfica de TinyCA está dividida en cuatro pestañas:

CA (*Certification authority - Autoridad certificadora*): Aquí se muestra toda la información respecto al titular de la autoridad, como los datos propios del certificado raíz. Desde esta pestaña se puede exportar el certificado raíz a formato DER, PEM o TXT, así como emitir LRCs.

Certificados: Aquí se muestra el listado de todos los certificados emitidos por la AC a la fecha y su información si se requiere. Desde aquí se puede crear nuevos certificados, exportar el certificado en los formatos PEM, DER, TXT o PKCS#12 (Con la clave privada); revocar el certificado o renovarlo.

Claves: Aquí se muestra el listado de todas las claves privadas correspondientes a certificados o solicitudes de certificación que se hayan generado desde TinyCA, estas además se pueden exportar o borrar. Cada clave privada en TinyCA está protegida por su propia contraseña, lo que provee un cierto nivel de seguridad al acceso subrepticio a las claves.

Peticiones: Aquí se puede ver el listado de todas las solicitudes en el directorio raíz de la AC, desplegando la siguiente información si se requiere: Información del titular de la solicitud y datos técnicos de la solicitud (cifrado, longitud de clave, etc.). Desde esta ubicación se puede crear, importar o firmar la solicitud seleccionada para crear un nuevo certificado.

⁶ Lenguaje de programación diseñado por Larry Wall en 1987, el que toma características de distintos lenguajes de programación.

⁷ Conjunto de bibliotecas multiplataforma para desarrollar interfaces gráficas de usuario (GUI).

⁸ Software libre desarrollado por Eric Young y Tim Hudson. Robusto paquete de herramientas de administración y bibliotecas relacionadas con la criptografía.

V. MODELO DE PROCESOS DEL SISTEMA

Como se mencionó anteriormente y con la finalidad de realizar un modelamiento a través de una notación formal, se utilizará una diagramación del ciclo de vida del certificado digital planteado en el capítulo anterior. En la Figura N° 5 se representa dicho ciclo mediante un diagrama BPMN (*Business Process Modeling Notation*), donde se utilizan “pools”, que representan las actividades propias de la entidad prestadora de servicios de certificación (EPSC) y los usuarios finales, además de señalar que muchas de las actividades de la EPSC están compuestas a su vez de subtareas, representadas mediante el empleo del símbolo de subprocesos anidados.

A partir de esta diagramación se diseñó el proceso general para determinar las interrelaciones entre las distintas entidades, permitiendo mejorar los procedimientos de implementación y explotación de una entidad prestadora de servicios de certificación.

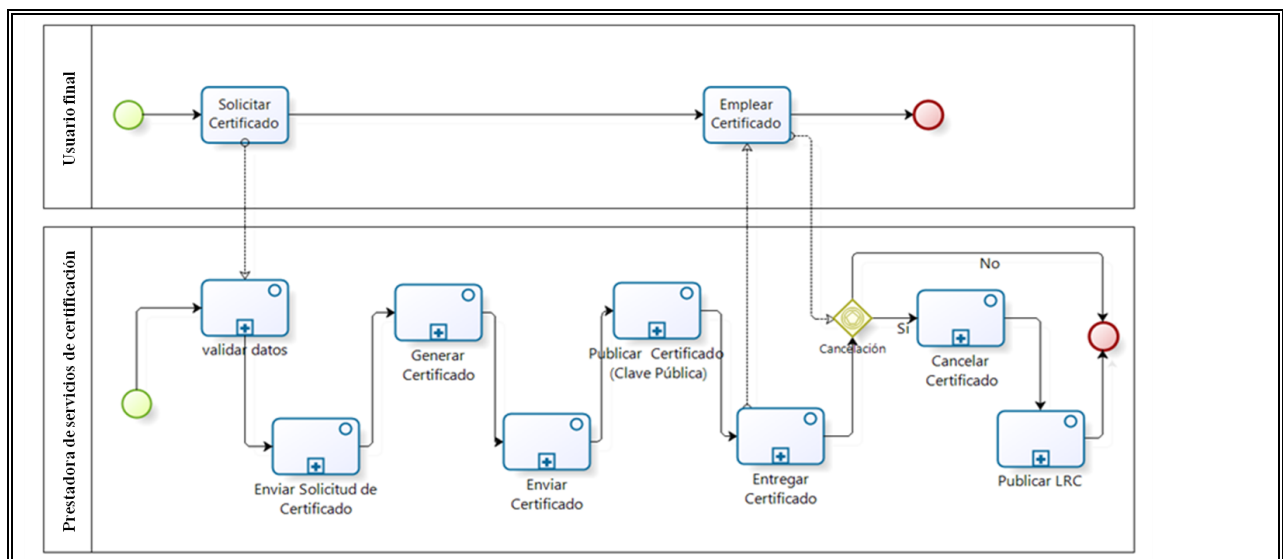


Figura N° 5, Diagrama de BPMN del ciclo de vida del certificado digital

Para el desarrollo de los diagramas de detalle, se consideraron los siguientes aspectos:

- Las actividades del modelo de la autoridad certificadora se desarrollaron de acuerdo a las características de la aplicación de gestión de certificados digitales “Tiny CA”. Esta es una aplicación de fuente abierta que fue seleccionada para la generación y gestión de los certificados.
- Las actividades del modelo de la autoridad de registro se modelaron con el supuesto de que en el futuro se desempeñe efectivamente un servicio remoto, el cual facilite las actividades de la entidad en cuestión, existiendo alternativas de contingencia en caso de no tener disponible el servicio WEB por períodos prolongados.
- Las actividades del modelo usuario para la generación de su propio certificado digital se desarrollaron de acuerdo a las características de la aplicación de generación de certificados digitales con formato X.509 v3 Gpg4win 2.1.0 “Kleopatra”. Esta decisión

permite que sea el usuario quien genere su propio certificado, lo que conlleva a que nadie más que él conozca su clave privada, lo que reduce ostensiblemente, la posibilidad que dicha clave se filtre en algún eslabón del proceso que no sea el propio usuario del certificado digital.

5.1. Diagrama de relaciones funcionales entre las entidades

En la Figura N° 5-1 que se presenta a continuación y conforme a lo planteado en el Capítulo IV, se representan las relaciones funcionales entre las distintas entidades involucradas en el proceso, utilizando para describirlas la notación formal de BPMN. Estas relaciones corresponden a relaciones funcionales de carácter general, por cuanto aquellas que requieran un mayor nivel de desagregación, se personalizan como subprocesos anidados, los que serán desarrollados con mayor detalle.

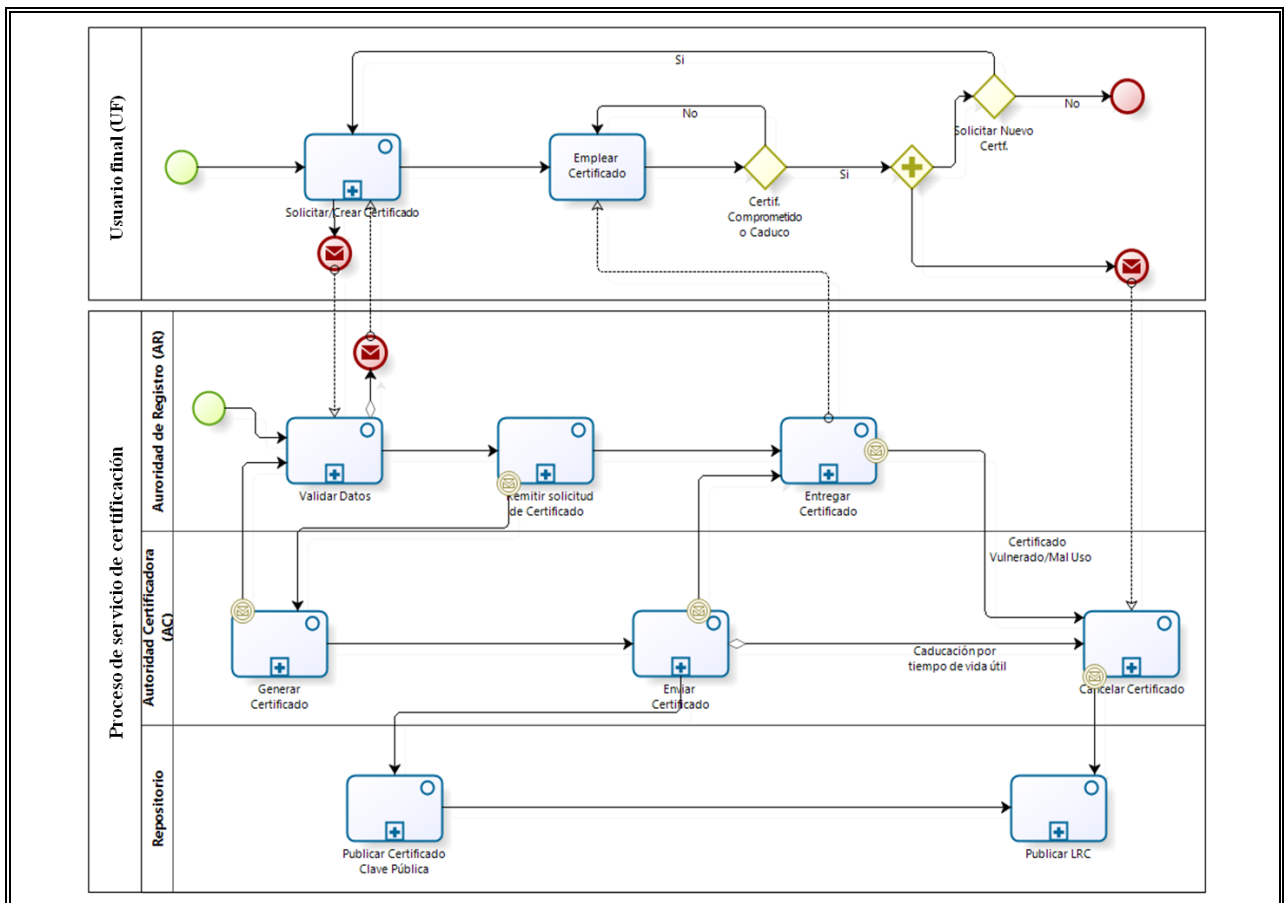


Figura N° 5-1, Relaciones funcionales entre las entidades

5.2. Diagrama general del proceso de prestación de servicios de certificación

En la Figura N° 5-2 que se presenta a continuación, se presenta el diagrama general del proceso de una entidad prestadora de servicios de certificación y sus entidades involucradas, en el se aprecian las diez actividades identificadas en el Capítulo IV.

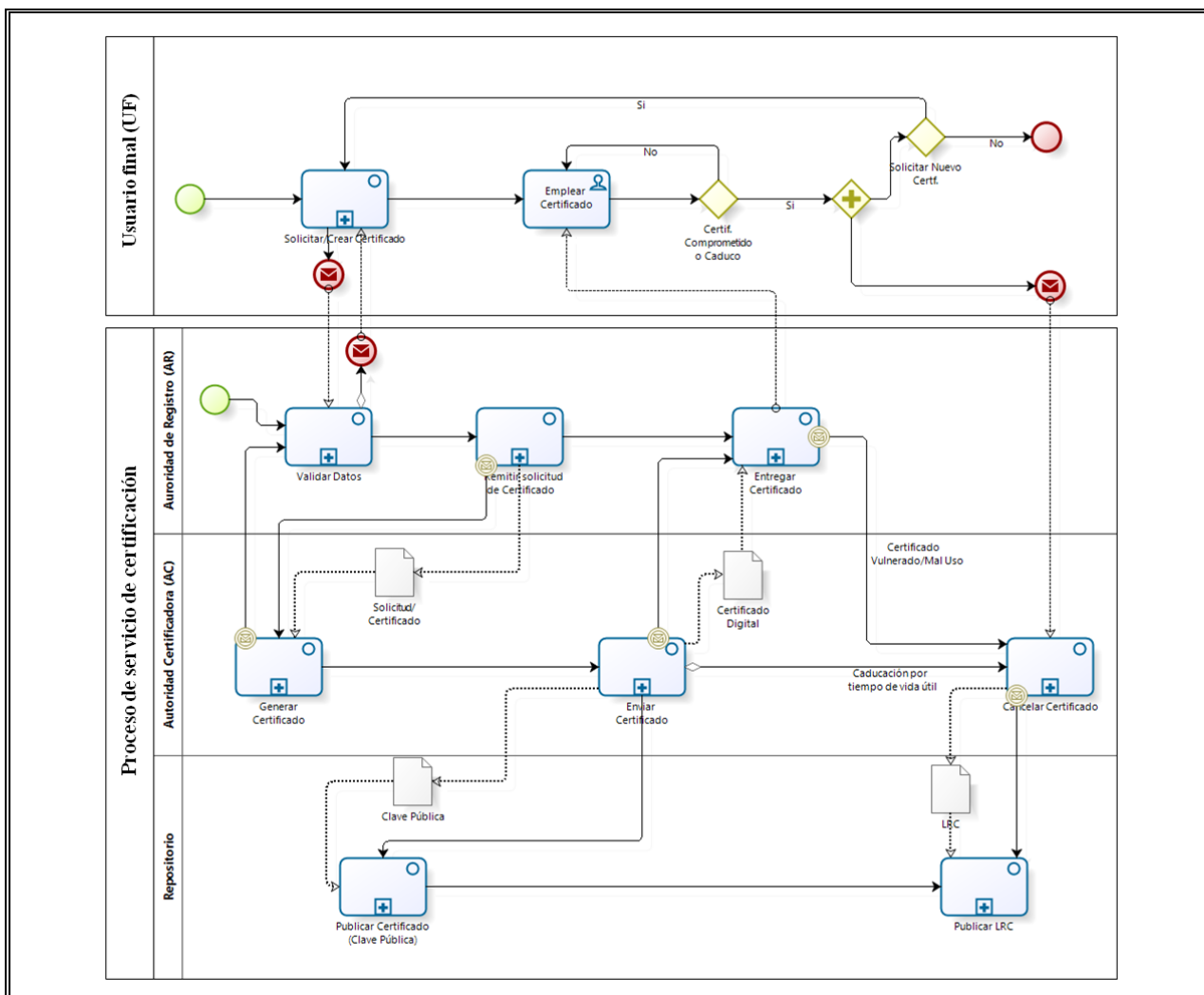


Figura N° 5-2, Diagrama general del proceso de la entidad PSC

El diagrama de la Figura anterior 5-2, representa el nivel más alto y general de agregación, es por esto que las nueve actividades del “pool” de la entidad PSC se representan como subprocesos anidados, lo que otorga simpleza para comprender el proceso y permite describir cada uno de estos subprocesos con mayor detalle.

La descripción de detalle del proceso general, sigue la siguiente secuencia:

1. El proceso se inicia cuando el UF solicita crear o validar un certificado digital a la AR, quien es la autoridad responsable de la verificación de los antecedentes personales de los usuarios que soliciten un certificado digital, asegurando que el usuario solicitante es quien dice ser.
2. Una vez validados los datos del usuario solicitante, estos son registrados en línea en el sistema, si el sistema no se encuentra disponible, en forma temporal, el registro se hará en un libro y se registrará una vez que el sistema vuelva a estar en línea.

3. Una vez recibido los datos del solicitante en el sistema de la AC, esta debe generar el certificado digital o validarlo, para posteriormente, enviarlo a la AR y publicar la clave pública del usuario en el repositorio.
4. Una vez que AR reciba el certificado digital por parte de la AC, esta AR debe hacer entrega de dicho certificado al usuario solicitante para su empleo.
5. El usuario final, queda en condiciones de utilizar su certificado digital para encriptar y firmar documentos. Si el UF ve comprometido el uso de su CD, este puede solicitar la cancelación del mismo o bien, caducará una vez cumplido el plazo definido para su uso.
6. La AC, al recibir la solicitud de cancelación del certificado digital por parte del usuario, o por parte de la AR (si existe vulneración o mal uso del CD), procede a cancelarlo y publicarlo en la LRC para el conocimiento del resto de los usuarios.
7. Finalmente, el UF que presente un certificado caducado o cancelado, podrá nuevamente, solicitar un CD para su uso o bien, salir del sistema.

Posteriormente, a este diagrama, se desarrollan cada uno de los subprocesos anidados que corresponden a un segundo y tercer nivel de agregación para aquellos procesos que lo requieren.

5.3. Diagrama general del proceso de usuario

En la Figura N° 5-3, se muestra el diagrama del proceso de usuario cuando este decide generar su propio certificado digital. De esta forma, el usuario tendrá certeza absoluta que su clave privada no será conocida por ninguna otra persona. Para lo anterior, debe generar su certificado digital con la clave pública y posteriormente, enviarlo a la AC para que esta lo valide, firme y publique en el repositorio.

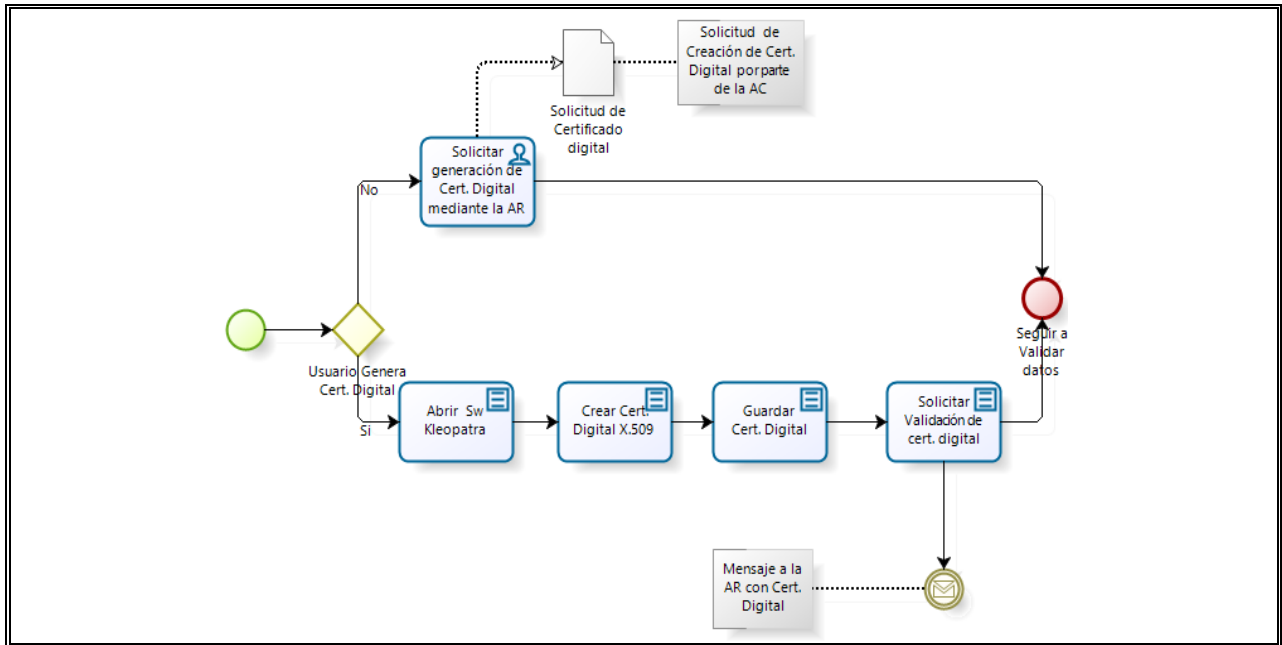


Figura N° 5-3, Diagrama del proceso de usuario

El usuario final tiene asociado las siguientes actividades:

- a. Solicitar certificado o crearlo
- b. Emplear certificado
- c. Solicitar nuevo certificado, solicitando la caducación del anterior
- d.

Descripción de las actividades del usuario dentro del proceso:

- a. Solicitar certificado o crearlo
 - 1) Para solicitar la creación de un certificado digital por parte de la AC, este deberá hacerlo, a través de la AR de la instalación a la cual pertenece y una vez que esta autoridad valide los datos, deberá ingresar la solicitud en el sistema de la AC.
 - 2) Para crear su propio certificado digital, el usuario debe instalar el software Gpg4win 2.1.0 que tiene asociado el gestor de certificados digitales “Kleopatra”, el cual soporta los estándares de criptografía pertinentes OpenPGP y S/MIME (X.509), éste es utilizado para cifrar y crear certificados por parte del usuario en su computador, posteriormente, a la instalación se debe:
 - i. Abrir “crear certificado” y elegir la opción señalada, la cual permite crear certificados mediante OpenPGP o bien utilizando el formato X.509, el que será el utilizado para este trabajo.
 - ii. Posteriormente, se deben llenar los datos del usuario de tal forma que permita crear su propio certificado digital.
 - iii. Una vez llenados los datos del usuario, se debe elegir una clave privada para crear su certificado digital y su clave pública.

iv. Finalmente, una vez creado el certificado digital, éste deberá ser enviado a la AR, mediante correo electrónico o bien, debe ser entregado en forma presencial a la AR en medio magnético, una vez que se concurra a validar sus datos personales.

b. Emplear certificado digital

Durante el período de empleo del certificado digital, el usuario no debe comprometer la seguridad de su clave privada, quedando en condiciones de utilizar su certificado por un período no superior a 2 (dos) años o hasta el momento en que el usuario cambie de desempeño dentro de la organización.

c. Solicitar nuevo certificado, solicitando la caducación del anterior

Para solicitar la creación de un nuevo certificado digital, este debe solicitar la caducación de su certificado actual a la AR y solicitar la creación de otro certificado digital para su uso.

5.4. Diagramas de la autoridad de registro

5.4.1. Validar datos

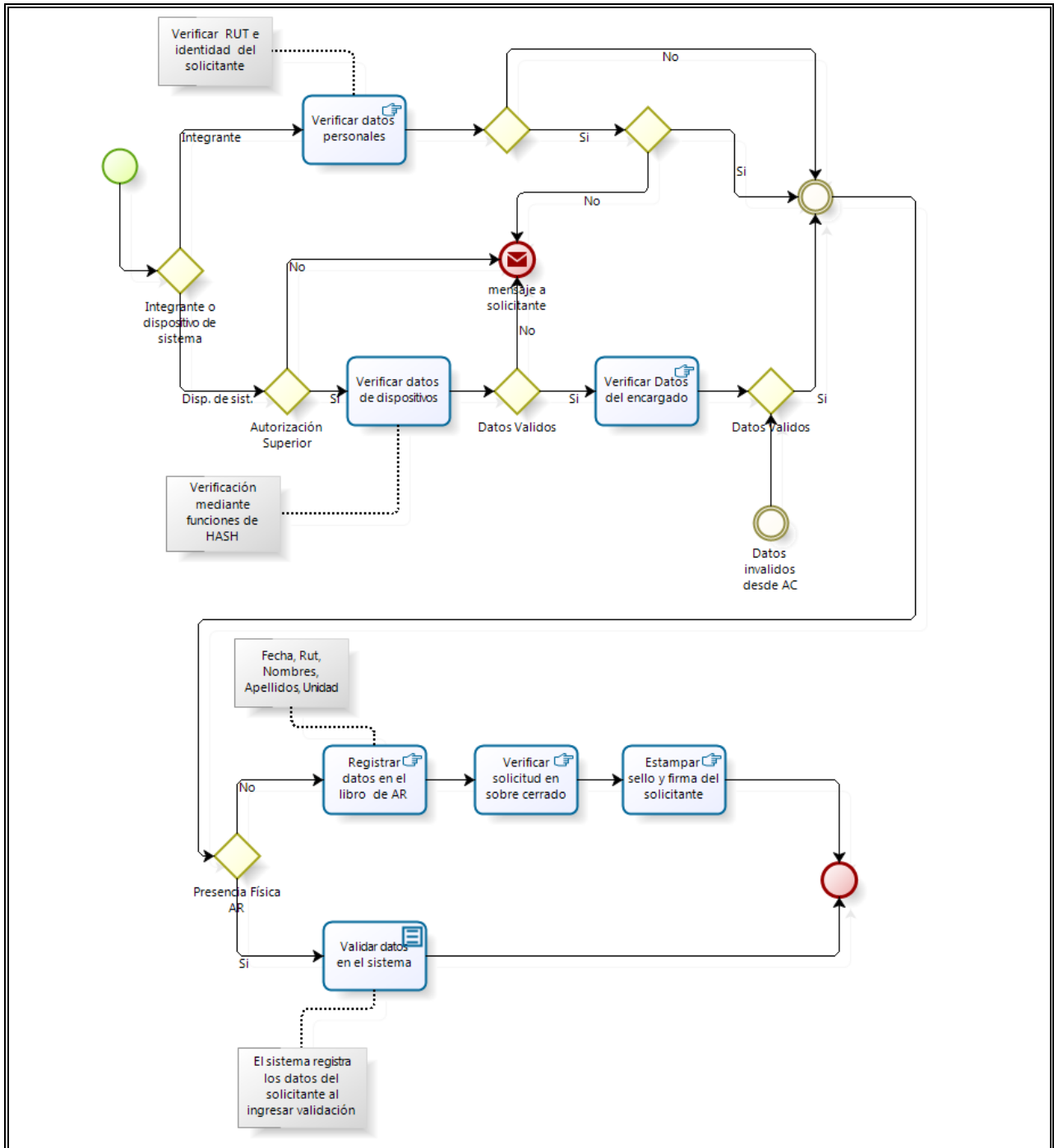


Figura N° 5-4-1, Diagrama del proceso para validar datos

La AR es la responsable de la verificación de los antecedentes personales de los usuarios que soliciten un certificado digital, asegurando que el usuario es quien dice ser, para lo cual debe realizar en forma presencial lo siguiente:

1. Si el solicitante es persona natural integrante de la organización, se debe:
 - a. Confirmar la identidad del solicitante requiriendo su cédula de identidad y datos presentados mediante la consulta a los sistemas de personal. Si la verificación no es satisfactoria, no se debe autorizar la solicitud.
 - b. Luego, si el certificado anterior fue revocado por pérdida o mal uso, la AR debe requerir la autorización por escrito del jefe directo del usuario. La falta de alguno de estos documentos significará que no se debe autorizar la solicitud.

2. Si el solicitante es el administrador o encargado autorizado de un dispositivo de sistema (servidores, dispositivos de comunicaciones o servicios), se deberá efectuar lo siguiente:
 - a. Solicitar la autorización del jefe respectivo. La falta de este documento significará que no se debe cursar la solicitud.
 - b. Verificar la integridad de los datos del archivo de petición generado por el propio dispositivo o servicio, esto normalmente, a través de funciones de hash. Si la verificación no es satisfactoria no se debe autorizar la solicitud.
 - c. Confirmar la identidad del solicitante requiriendo su cédula de identidad y datos del solicitante mediante consulta a sistemas de personal. Si la verificación no es satisfactoria, no se debe autorizar la solicitud.

3. Si el sistema en línea de la AC está disponible se selecciona autorizar, cursando de esta forma la solicitud.

4. La AR deberá considerar que si el sistema de la AC no está disponible para realizar el registro en línea, deberá registrar la información obtenida de la cédula de identidad y autorización en su respectivo libro para ser llenadas una vez reiniciado el sistema. Las instrucciones para emplear el libro de la AR se muestra más adelante en este documento, pero en forma general considera lo siguiente:
 - a. Datos del solicitante que deben ser registrados en el libro en el momento de la solicitud:
 - i) Fecha y hora de realización del trámite.
 - ii) Grado.
 - iii) Nombres.
 - iv) Apellidos.
 - v) Departamento o unidad a la cual pertenece el solicitante.
 - b. La AR debe verificar que la solicitud de certificado digital sea guardada en el respectivo sobre y que el solicitante firme la tapa del sobre una vez sellado.
 - c. La AR estampará en la tapa del sobre sellado, en el mismo lugar donde firmó el solicitante, su timbre oficial.

5.4.2. Enviar solicitud de certificado

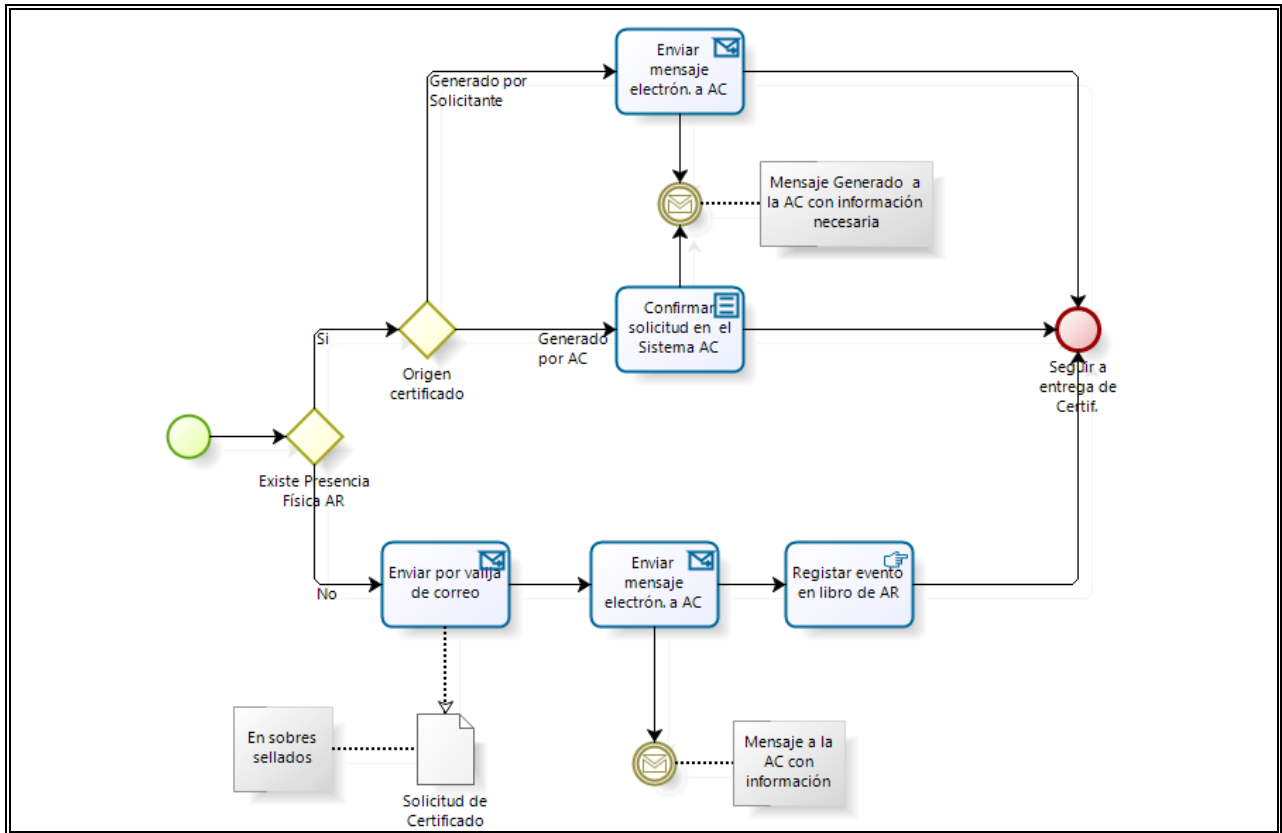


Figura N° 5-4-2, Diagrama proceso para enviar solicitud de certificado

1. Si el sistema en línea de la AC está disponible, con sólo confirmar las solicitudes es generado un mensaje hacia la AC, firmado y encriptado.
2. Si no está disponible el sistema en línea de la AC, se deben enviar las solicitudes por valija de correo en sobre sellados y firmados, debiendo:
 - a. Enviar un correo electrónico firmado y encriptado que informe a la AC el envío una valija con solicitudes, indicando la fecha y el número de solicitudes incluidas y a más tardar tres días después de recibidas la solicitudes.
 - b. Registrar en el libro de la AR la fecha y número de la valija. Detalles para esta actividad están en el Anexo B.4 de este documento.

5.4.3. Entregar certificado

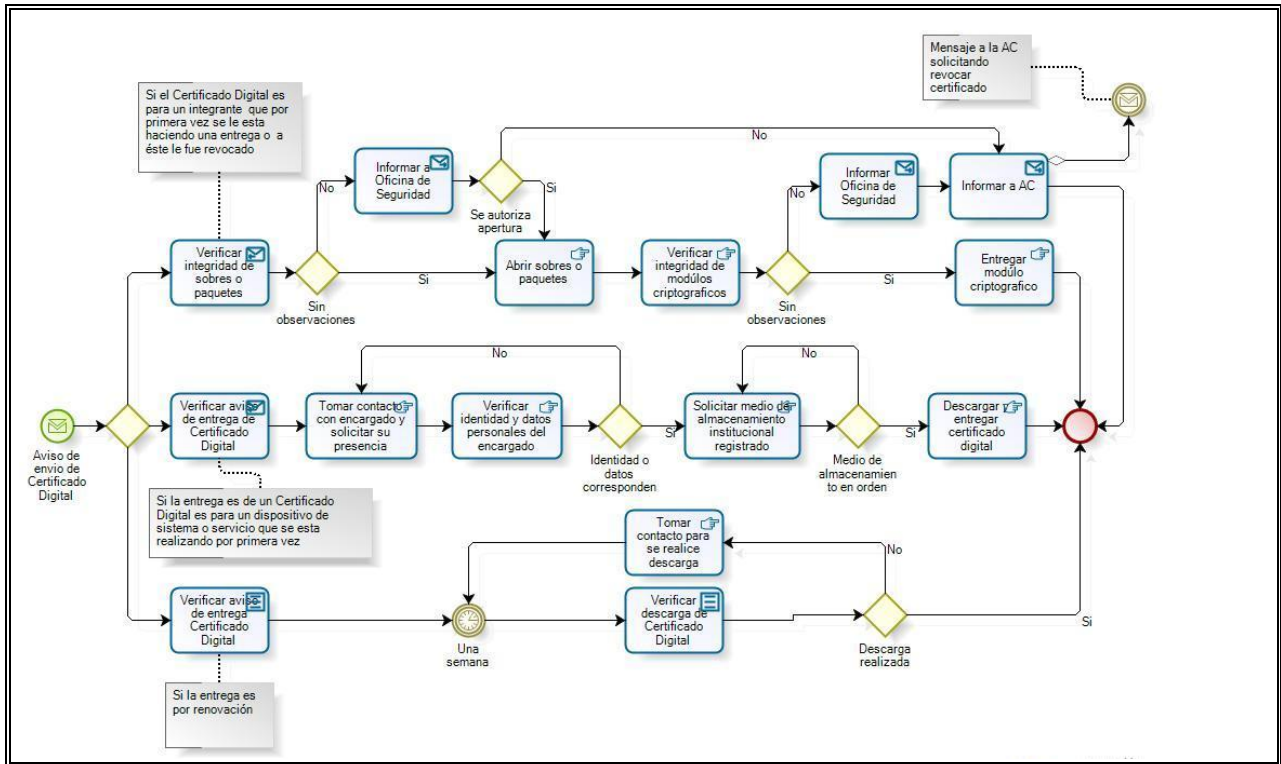


Figura N° 5-4-3, Diagrama del proceso para entregar certificado

1. Si el certificado digital es para un usuario que por primera vez se le está haciendo una entrega, o bien le fue revocado (por pérdida o mal uso), le será enviado un módulo criptográfico a la AR respectiva, el cual contiene el certificado digital, debiendo realizar los siguientes pasos:
 - a. Verificar la integridad física de los sobres o paquetes que contienen los certificados digitales. Si estos presentan evidencia de que su integridad se ha vulnerado, se debe dar aviso a la AC y oficina de seguridad local.
 - b. Abrir los sobres o paquetes y verificar la integridad física de los módulos criptográficos. Si los módulos criptográficos presentan evidencia física de haber sido vulnerados se debe dar aviso a la AC y a la oficina de seguridad local, no entregándose los certificados a los usuarios finales, quedando en espera de una resolución por parte de la oficina de seguridad.
 - c. Si no ha habido observaciones, la AR debe personalmente hacer entrega al usuario final del módulo criptográfico que contiene su certificado digital. El usuario debe firmar y registrar el número de serie del certificado digital en el libro de AR.
2. Si la entrega de un certificado digital es para un dispositivo de sistema o servicio que, se está realizando por primera vez, o bien, le fue revocado, el certificado digital será enviado en un archivo electrónico por el sistema de la AC a la AR, para lo cual se debe:
 - a. Tomar contacto con el encargado del dispositivo de sistema, de acuerdo a los datos que registra el sistema de la AC.

- b. Solicitar que el encargado, en persona, se presente a retirar el certificado digital. Al presentarse, se debe verificar la identidad y datos personales del encargado.
 - c. Descargar y entregar el certificado digital en un dispositivo de almacenamiento registrado, el cual debe ser traído por el encargado del dispositivo de sistema.
 - d. El usuario responsable del dispositivo debe firmar y registrar el número de serie del certificado digital en el libro de AR.
3. Si es un usuario o encargado de dispositivo de sistema que está renovando un certificado digital para su empleo personal o instalación en un dispositivo de sistema respectivamente, este le será enviado directamente al encargado, a través del sistema de la AC a su respectiva cuenta registrada, para lo cual se debe:
- a. Verificar los avisos de entrega de certificados generados por el sistema de la AC.
 - b. Verificar que el usuario final o encargado del dispositivo de sistema haga descarga del certificado digital. Si este no ha sido descargado, debe tomar contacto con el usuario final o encargado para que realice esta acción, esto cada semana hasta que sea realizada la descarga.

5.5. Diagramas de la autoridad de certificadora

5.5.1. Generar certificado

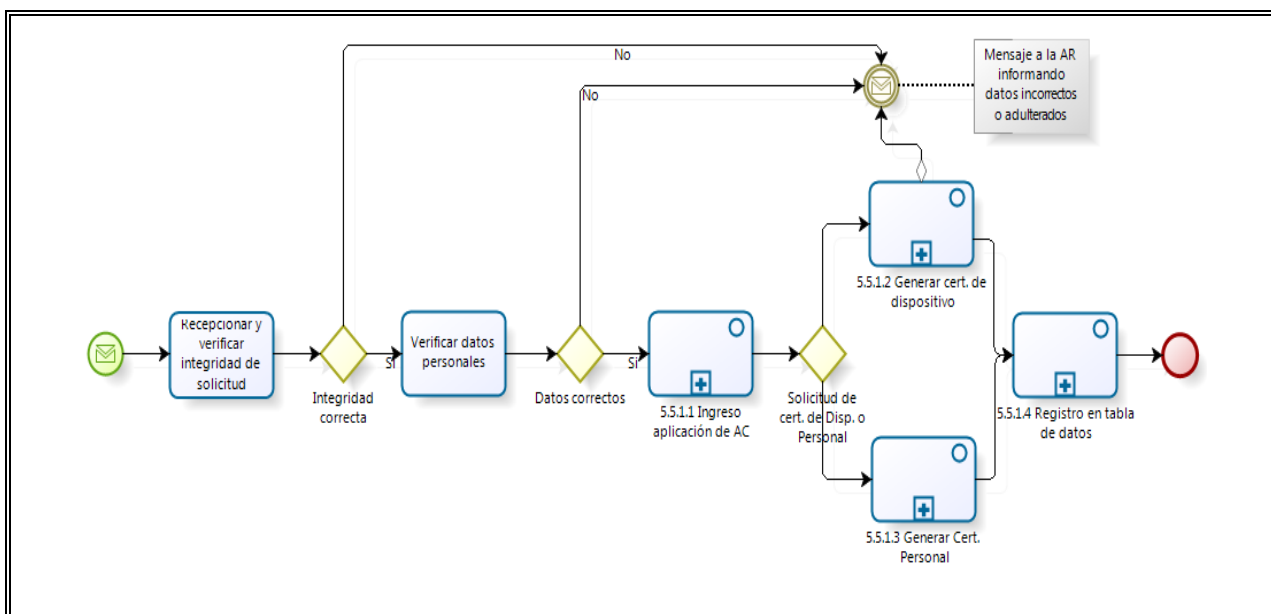


Figura N° 5-5-1, Diagrama del proceso para generar certificados

1. La AC, una vez recibida la solicitud para generar un certificado digital, debe verificar su integridad, si esta posee datos adulterados, la AC debe enviar un mensaje en respuesta a la AR que realizó dicho trámite.
2. Si los datos son íntegros, la AC debe verificar si los datos del usuario solicitante son correctos, de ser incorrectos la AC procede de igual forma al caso anterior.

3. Una vez confirmada la integridad y validez de la solicitud, la AC procede a ingresar a la aplicación “Tiny ca” para generar el certificado digital requerido.
4. Finalmente, la AC debe hacer el registro respectivo en la tabla de datos.

5.5.1.1. Ingresar a la aplicación de AC

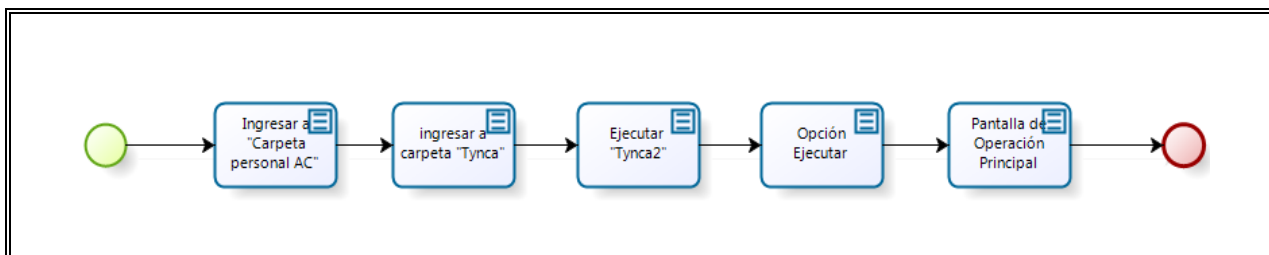


Figura N° 5-5-1-1, Diagrama del proceso para ingresar a la aplicación de AC

1. Se debe ingresar a la carpeta con el nombre: “Carpeta personal de CA” con la finalidad de acceder a la Subcarpeta con el nombre “TinyCA2-0.7.3”
2. Al abrir la subcarpeta anterior, se mostrará un menú en el cual se debe ejecutar “TinyCA2” y seleccionar la opción “Ejecutar”.
3. Este proceso se demora unos minutos, al completarse se desplegará la “pantalla de operación principal”, donde aparecen las 4 opciones indicadas en Figura N° 4-4.

5.5.1.2. Generar certificado de dispositivo

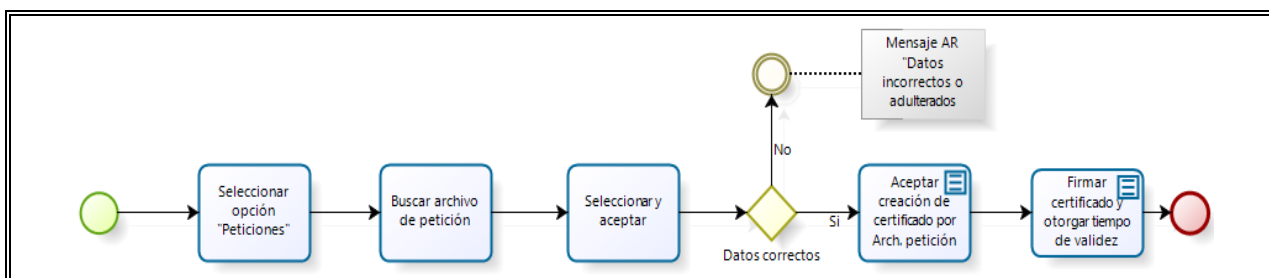


Figura N° 5-5-1-2, Diagrama del proceso para emitir certificado de dispositivo

1. En la Pantalla de operación principal, se debe seleccionar la opción “Peticiones” y desde ahí seleccionar el archivo que ha sido enviado como una petición de certificado de servidor.
2. Luego, se proyectará una ventana para buscar el archivo que permite crear el certificado de servidor. Se debe buscar el archivo con la opción “Browse”, el cual tendrá una extensión “.csr”, una vez encontrado se debe “Aceptar”.
3. Luego de encontrar el archivo y aceptar, se proyecta una pantalla donde se verifica y se pregunta si quiere importar la solicitud de certificado, se debe “Aceptar”, siempre y cuando, los datos y los archivos sean correctos.
4. Una vez realizado los pasos anteriores correctamente, en la opción “Peticiones” se muestra la petición que se ha creado para la unidad que la solicitó.

5. Luego, se debe ir a la opción “Firmar” de la Figura N° 4-4, e ingresar el “*password*” del operador y el tiempo de validez del certificado de servidor, mínimo 2 años y máximo la fecha de expiración de la autoridad certificadora, luego se acepta.
6. Una vez firmada la petición, se proyecta la pantalla que la petición ha sido firmada correctamente, con este paso la petición queda lista para ser exportada.
7. Luego de firmada la petición, se debe exportar el certificado con sus respectivas extensiones: “.cert.crt “o “.p12 “.

5.5.1.3. Generar certificado personal

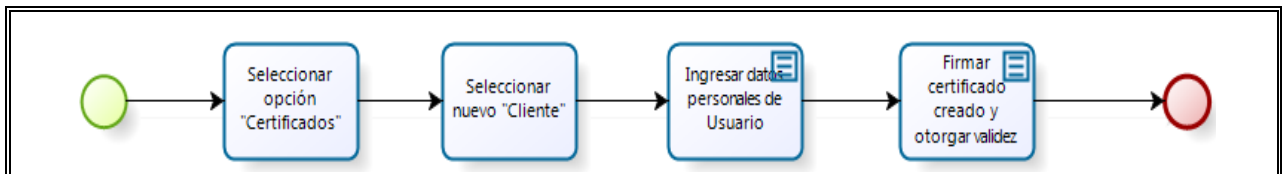


Figura N° 5-5-1-3, Diagrama del proceso para emitir certificado personal

1. En la “pantalla de operación principal” se debe seleccionar la opción “Certificados”.
2. Después de lo anterior, se selecciona la opción “Nuevo” donde aparecerán dos opciones:
 - a. Crear clave y certificado (Servidor)
 - b. Crear clave y certificado (Cliente), posteriormente, seleccionar la opción b.
3. Después de haber seleccionado la opción anterior, se deben ingresar los datos de la persona que solicitó el certificado.

Estos datos deben ser ingresados con estricto cuidado. El “*password*” ingresado en la etiqueta debe ser la misma que ingresó el usuario en la solicitud del certificado. Se debe tener especial cuidado entre las minúsculas y mayúsculas. Después de haber ingresado todos los datos, correctamente, se procede a aceptar.

4. Finalmente, para generar el certificado en el servidor y que este quede firmado correctamente, se debe ingresar el “*password*” del operador de la AC y el tiempo de validez del certificado, luego se acepta quedando listo para ser exportado
5. Para exportar el certificado digital se procede como se explica en el punto 5-5-2-1

5.5.1.4. Registro de datos en tabla de datos



Figura N° 5-5-1-4, Diagrama del proceso para registro en tabla de datos

1. Para ingresar los datos en la tabla de datos, se debe ingresar a la carpeta de nombre “Carpeta personal ca”. Esta carpeta contiene un archivo con el nombre: “Información certificados. Ods”, el que debe ser abierto.
2. Para acceder al archivo, se debe introducir el “password” del operador del servidor.
3. Luego se ingresan los datos de la persona que solicita el certificado digital y elegir la opción guardar.

5.5.2. Enviar certificado

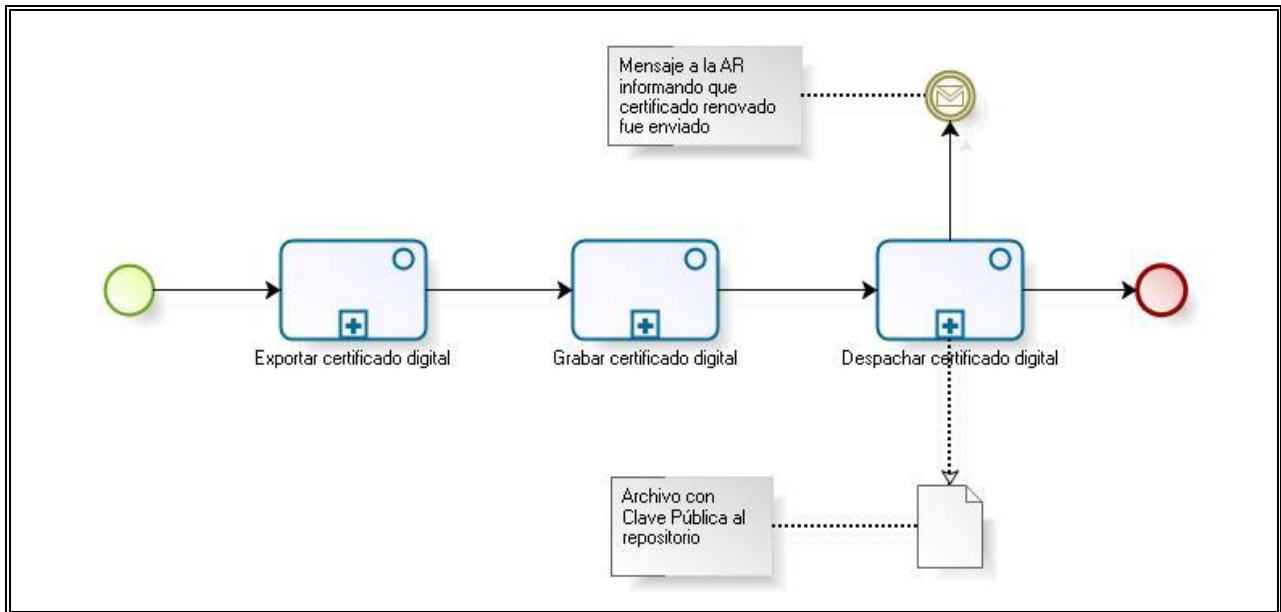


Figura N° 5-5-2, Diagrama del proceso para enviar certificado

1. Una vez generado el certificado digital, la AC procede a enviarlo a quien lo solicitó, realizando los siguientes subprocessos:
 - a. Exportar certificado digital
 - b. Grabar certificado digital
 - c. Despachar el certificado digital
2. Esta etapa termina cuando se despacha el certificado digital, al mismo tiempo se envía un mensaje a la AR, informando que el certificado fue enviado y se publica la clave pública respectiva en el repositorio para el acceso de terceros.

5.5.2.1. Exportar certificado digital

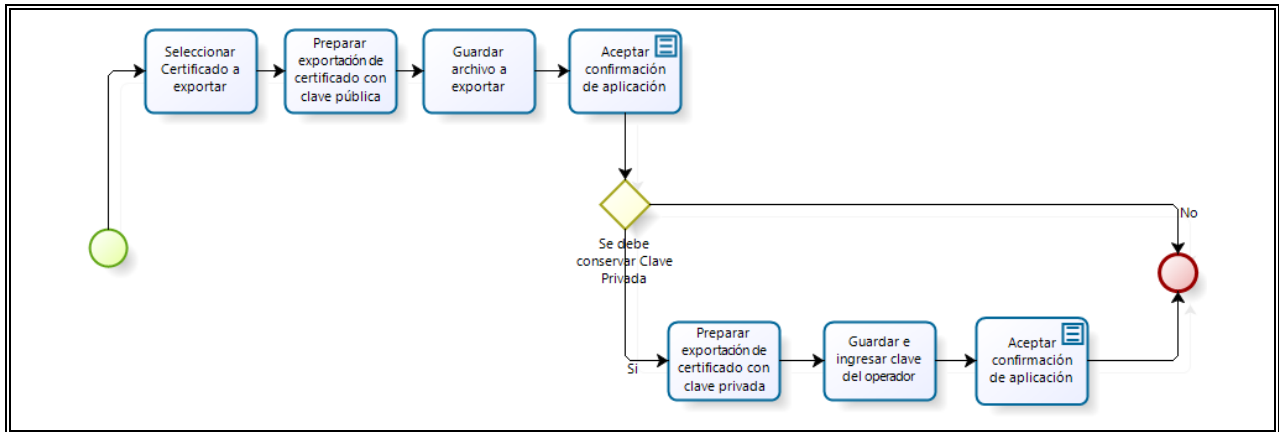


Figura N° 5-5-2-1, Diagrama del proceso para exportar certificado digital

1. En la “pantalla de operación principal”, se debe seleccionar el nombre del usuario o unidad que solicitó el certificado, en “Certificados” o “Peticiónes” respectivamente, y elegir la opción “Exportar”.
2. Luego se prepara la exportación del certificado con la clave pública, para lo cual, se debe seleccionar la opción “DER”, y en el casillero “Fichero” se debe colocar la extensión del certificado: mil-cert.crt.
3. Luego de se selecciona la opción “Guardar”, durante este paso se está exportando la clave pública. Para terminar de exportar el certificado se debe “Aceptar”.
4. Para preparar la exportación del certificado con clave privada y pública en archivo de extensión PKCS#12, se debe seleccionar el archivo indicado “PKCS#12 (Certificado & Clave)”, este archivo se “Guarda” con la misma extensión que tiene.
5. Al seleccionar la opción “Guardar” aparece una pantalla donde se debe ingresar un “password”. Este es necesario para poder exportar el certificado con la clave privada.
El “password” ingresado en el casillero correspondiente, debe ser la misma que ingresó el usuario en la solicitud del certificado. Se debe tener especial cuidado entre las minúsculas y mayúsculas, como se explico anteriormente.
6. Finalmente, se informa que el certificado y la clave han sido exportados correctamente. Se procede a “Aceptar” y se da término al proceso de exportar el certificado digital.

5.5.2.2. Grabar certificado digital

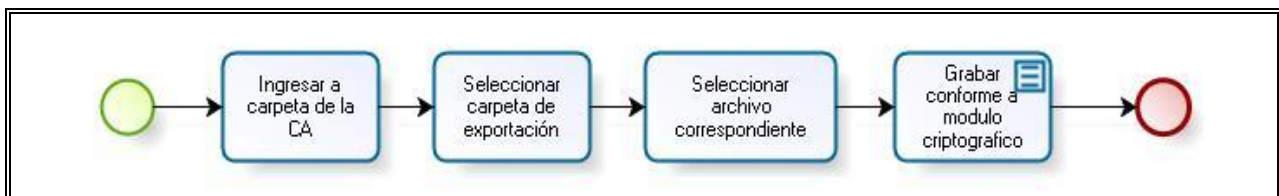


Figura N° 5-5-2-2, Diagrama del proceso para grabar certificado digital

1. Para realizar este procedimiento, se debe ingresar a la carpeta con el nombre “Carpeta personal de ca”, donde hay varias carpetas diferentes.
2. Se debe seleccionar la carpeta donde fueron enviados los archivos al momento de guardarlos.
3. Al abrir esta carpeta, se debe seleccionar el archivo de certificado con clave privada, conforme al nombre de la persona a la que se le está confeccionando el certificado digital.
4. Grabar conforme al método correspondiente al módulo criptográfico que almacenará el certificado.

5.5.2.3. Despachar certificado digital

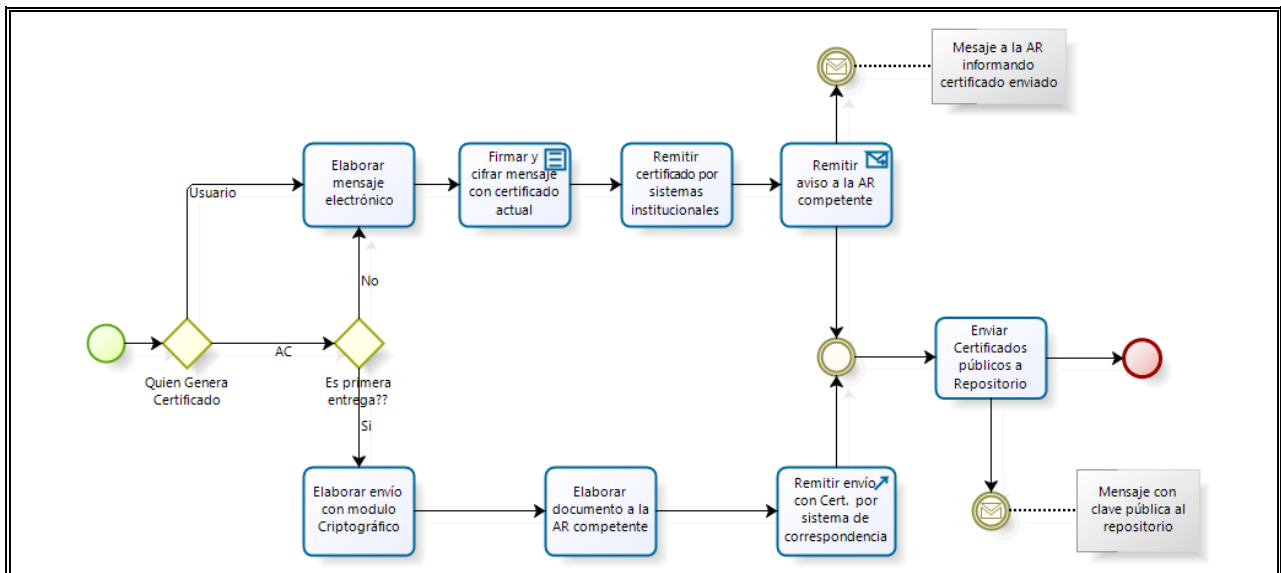


Figura N° 5-5-2-3, Diagrama del proceso para despachar certificado digital

1. Si es la primera entrega de un certificado digital o el certificado anterior no ha sido revocado, se debe:
 - a. Elaborar envío con modulo criptográfico.
 - b. Este será remitido mediante documento a la AR correspondiente, de acuerdo a los procedimientos de entrega de documentación por correspondencia establecidos.
2. Si es una renovación de certificado digital, se debe:
 - a. Elaborar mensaje con certificado digital adjunto.
 - b. El mensaje electrónico debe ser firmado y cifrado.
 - c. Será remitido, directamente, a quien solicitó la renovación.
 - d. Remitir un aviso de que fue enviada una renovación a la AR correspondiente.

5.5.3. Cancelar certificado digital

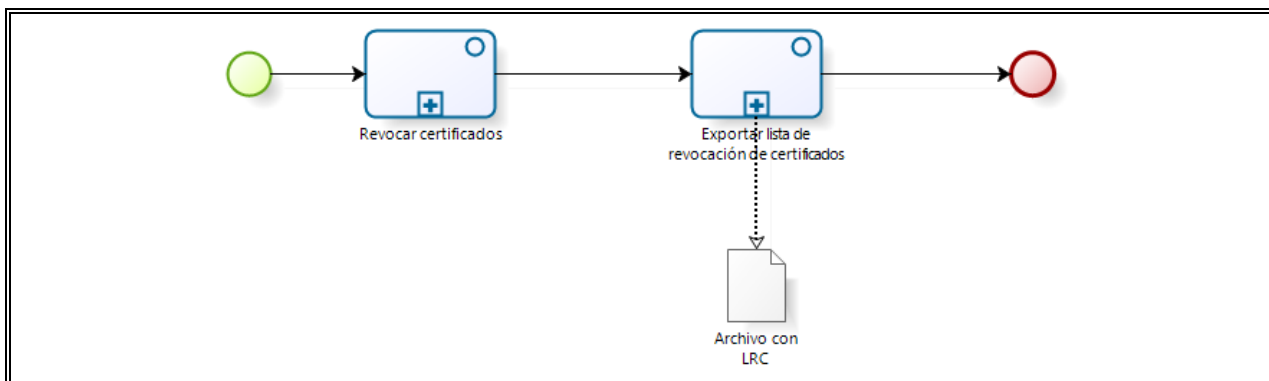


Figura N° 5-5-3, Diagrama del proceso para cancelar certificado

1. Los Certificados sólo se revocarán por solicitud del titular. Para solicitar la revocación de un certificado, el titular deberá enviar un mensaje electrónico firmado a la casilla de la AC.
2. Los Certificados caducarán por el fin del período de autorización del mismo, el cual es indicado en certificado. Esto se realizará automáticamente al finalizar este período.
3. La AR correspondiente, es la responsable de solicitar la revocación a la AC mediante documento o mensaje electrónico firmado en los siguientes casos:
 - a. Por cualquier tipo de desvinculación del usuario de la organización.
 - b. Por mal uso del sistema por parte del usuario.
4. El UF será el responsable de la renovación del certificado digital (revocación de su certificado anterior), en los siguientes casos:
 - a. Por cambio del cargo del usuario.
 - b. Por cambio de denominación de una organización o desempeño.
5. Los Certificados podrán ser revocados por resolución escrita del jefe directo del usuario y la caducidad provocará la invalidez del certificado existente y la inclusión en la LRC.

5.5.3.1. Revocar certificados

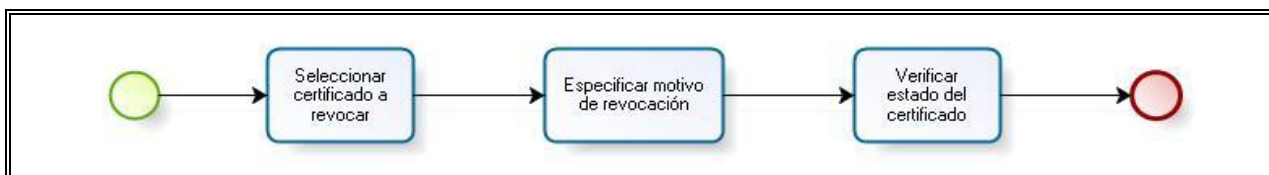


Figura N° 5-5-3-1, Diagrama del proceso para revocar certificado

1. En la “pantalla de operación principal”, se debe ingresar a la opción “Certificados” y se selecciona el certificado a revocar.
2. Luego se debe seleccionar la opción revocar, donde se debe especificar una de las razones por cual será revocado el certificado, debiendo ingresar el “password” del operador y seleccionar aceptar.

3. El procedimiento anterior, termina cuando se verifica el estado del certificado, el cual cambia de VÁLIDO a REVOCADO.

5.5.3.2. Exportar lista de revocación de certificados

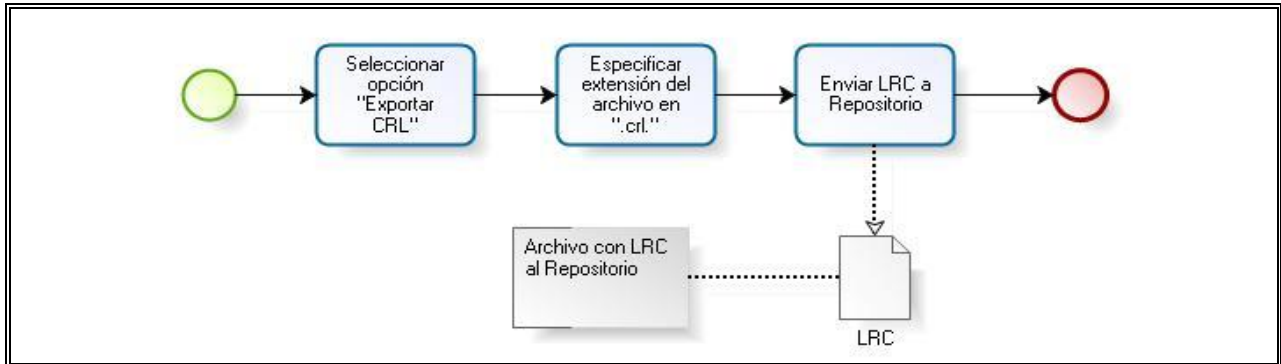


Figura N° 5-5-3-2, Diagrama del proceso para exportar LRC

1. Luego de revocar el certificado, se debe exportar la lista certificados revocados, con la finalidad de actualizar el repositorio donde están publicados todos los certificados que están vigentes.

Para realizar este paso, en la “pantalla de operación principal”, se debe seleccionar la opción “CA” y luego “Exportar CRL”.

2. Aquí se debe especificar la extensión del archivo en la opción “Fichero”, que debe quedar con la extensión “.crl” y con la opción “Formato a Exportar”, seleccionada en la opción “DER”. Luego se debe ingresar el “password” del operador y finalmente se “Guarda”. Con este paso se da término al procedimiento de exportar la lista de certificados revocados.

5.6. Diagramas del repositorio

5.6.1. Publicar certificados (Claves Públicas)

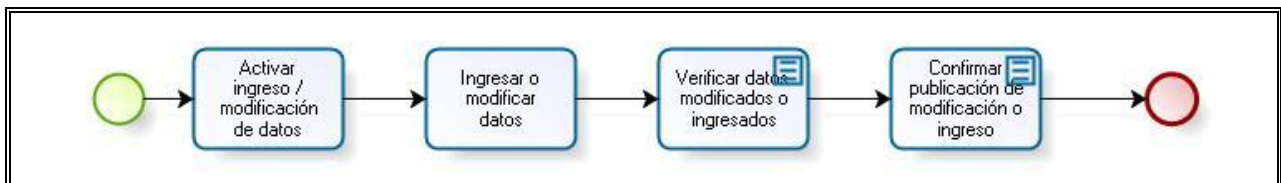


Figura N° 5-6-1, Diagrama del proceso para publicar certificados

1. Una vez realizados los pasos anteriores, se debe ingresar a la web de intranet de la comunidad objetivo, aquí se debe activar el ingreso o modificación de datos.
2. Luego se proyecta la pantalla donde se deben ingresar los datos a publicar: Estos datos deben ser ingresados como se indica.
 - Nombres
 - Apellidos
 - Dirección de correo electrónico

- Puesto
- Unidad

3. Finalmente, se procede a verificar los datos y confirmar la publicación.

5.6.2. Publicar LRC



Figura N° 5-6-2, Diagrama del proceso para publicar LRC

1. Después de haber exportado la LRC, se debe realizar el paso siguiente para poder actualizar el servidor con los datos de los certificados que han sido caducados o revocados.
2. Seleccionar y abrir la carpeta con LRCs en el servidor de la AC de nombre: “Carpeta de personal de ca”.
3. Dentro de esta carpeta se debe abrir la subcarpeta de nombre “Certificados”, y buscar el archivo.
4. El archivo tiene el nombre de “Intranet.crl” con la fecha del día de modificación, eso demostrará que ha sido actualizado y que contiene nuevos datos. Se debe copiar en un medio extraíble para ser llevado al servidor del repositorio.
5. Se debe transferir el archivo “Intranet.crl” a la carpeta del servidor del repositorio que contiene las LRC.
6. Con este paso, se da término a la actualización de la lista de revocación de certificados, lo cual se debe verificar en la página web del repositorio.

VI. EVALUACIÓN Y CONCLUSIONES

6.1. Respecto a los sistema de PKI

El modelo desarrollado permite el establecimiento de un sistema lo suficientemente robusto que garantiza la disponibilidad, confidencialidad, integridad y autenticidad en la generación, almacenamiento, transporte, acceso y distribución de información a través de los sistemas de comunicaciones propios de la organización, utilizando un modelo de confianza centralizado y depositado en una autoridad de certificación.

El estándar escogido, basado en el formato X.509 v3 para certificados digitales, tiene la fortaleza de vincular un conjunto de información que identifica a la entidad propietaria del certificado digital con un valor de clave pública, el cual, es asociado a una clave privada que debiera conocer sólo el propietario de dicho certificado.

El usuario final, como dueño único de su propio certificado digital, tiene la capacidad de firmar electrónicamente y cifrar documentos emitidos por él, así como, establecer sellos de tiempo a la documentación

La organización, a través de la implementación de una infraestructura PKI, permite establecer las políticas de seguridad, como también, proveer el canal de comunicación que soporte la transmisión de datos entre sus integrantes.

Aunque, uno de los principales problemas que se presenta en los sistemas basados en autoridades de certificación, es la dificultad de comprobar la fidelidad de los datos suministrados por los usuarios solicitantes de certificados digitales, la conformación de ARs competentes que realicen esta labor, permite disminuir, significativamente este problema, considerando además, que utilizan una base de datos única con la información de sus integrantes para toda la organización.

6.2. Respecto a las normas legales exigibles para el funcionamiento de la EPSC

Respecto al cumplimiento de las normas legales que enmarcan el funcionamiento de una entidad prestadora de servicios de certificación, se puede inferir que en Chile existen normas claras respecto a los requisitos que se deben cumplir para poner en práctica un sistema PKI de estas características.

Para establecer el funcionamiento de la entidad prestadora de servicios de certificación en la organización, se requiere de estándares acordes a los de una entidad acreditada que posibilite en el futuro, su acreditación por parte de un organismo externo, bajo el concepto de firma electrónica avanzada.

Al establecer los modelos operacionales que rigen a la entidad prestadora de servicios de certificación, se cumple lo establecido en el capítulo III de este documento, asegurando su implementación acorde a las políticas y las leyes que rigen su funcionamiento, de tal forma, que se asegure su correcta ejecución y permanencia en el tiempo, validando la necesidad que dichos procesos sean correctamente definidos y documentados.

Uno de los mayores inconvenientes que presenta la organización, es la alta rotación de

personal, lo que hace evidente la necesidad de contar con procesos bien documentados, de no hacerlo de esta forma, se llevaría a la organización a la pérdida de la experiencia y conocimientos adquiridos en el área de la certificación digital y uso de los certificados digitales.

Desde la implementación del correo electrónico a través de la intranet institucional, la reducción significativa de documentos públicos impresos, es uno de los mayores beneficios que se ha podido obtener en la organización. Al agregar al proceso documentos reservados, el beneficio será mucho mayor, por cuanto un usuario que reciba un documento, puede tener certeza absoluta, que dicho documento no fue alterado, que no ha sido leído y que es, efectivamente, de quien dice ser.

Uno de los mayores problemas en la documentación impresa de carácter reservado, es su almacenamiento físico, grandes volúmenes de espacio y alta probabilidad de violación de su seguridad. Al implementar un sistema de estas características, su almacenamiento debiera ser digital (Bajo volumen de almacenamiento), cifrado (Impidiendo el acceso no autorizado) y mantendría un registro eficaz respecto a las responsabilidades de quien emitió un determinado documento.

6.3. Respetto a las relaciones entre las entidades y su funcionamiento

De acuerdo a lo que se establece en el estándar X.509 v3, lo determinado en la norma Chilena y otros textos para la gestión de los certificados digitales e implementación de una EPSC definidos previamente, fueron identificadas y modeladas las interrelaciones de 4 (Cuatro) entidades en el proceso general, lo que obedece además a la arquitectura de PKI propuesta:

- a) Autoridad de Certificación (AC)
- b) Autoridad de registro (AR)
- c) Usuarios Finales (UF)
- d) Repositorio (REP)

Como base del proyecto, existían factores de partida tendientes a materializar la PKI y que debían ser considerados como un *input* al proceso de modelamiento, estos son los siguientes:

- 1) **Escalabilidad.** Una vez implementada la PKI, esta pudiera ampliarse y extenderse de forma eficiente a todos los sistemas de información de la organización, logrando un empleo masivo de los certificados digitales y la firma electrónica.
- 2) **Seguridad.** Operar los certificados digitales totalmente al interior de la comunidad objetivo, sin depender de servicios informáticos externos y con control total en lo que se refiere a generación, copias y respaldos de estos.
- 3) **Tecnológica.** Emplear firma electrónica con características técnicas equivalentes a la firma electrónica avanzada, sin tener la necesidad de llegar a estar acreditada como tal.

Dado lo anterior, se decidió para la organización contar con una PKI administrada, con una entidad prestadora de servicios de certificación propia y con capacidad técnica

equivalente a firma electrónica avanzada, de tal forma que se facilite en una primera instancia cumplir con parte de los requisitos que permitan ser acreditados legalmente en el futuro.

- 1) Ventajas
 - a) A futuro permitirá acreditar la autoridad certificadora, con los costos asociados a la acreditación, pudiéndose extender el uso de firma electrónica avanzada en los sistemas electrónicos de información de la organización.
 - b) Control total de los certificados al interior de la organización, lo que otorgará seguridad integral al tratamiento de la documentación electrónica.
 - c) Capacidad para renovar certificados de acuerdo a necesidades, sin costos adicionales.
 - d) Capacidad de revocar certificados digitales y tener control absoluto de aquellos certificados caducados y/o obsoletos.
- 2) Desventajas

Legalmente, mientras no se acredite la entidad prestadora de servicios de certificación, se permite el empleo de firma electrónica similar a la avanzada, pero sin contar con dicho reconocimiento.

6.4. Respecto a la herramienta de gestión de una autoridad certificadora (AC)

TinyCA emplea la licencia GPL (*General public licence*), el uso conjunto de esta licencia y de OpenSSL no supone un problema, puesto que TinyCA no está enlazado con la biblioteca OpenSSL, sino que sólo realiza llamadas al ejecutable openssl.

- 1) Ventajas
 - a) Se pueden importar y firmar peticiones PKCS#10.
 - b) Permite escoger los distintos algoritmos de cifrado simétrico y de resumen (hash) empleados.
- 2) Desventajas
 - a) TinyCA almacena su información en el directorio \$HOME/.TinyCA, acopiando la información de cada autoridad de certificación en un subdirectorio que sigue la estructura de directorios y ficheros necesaria para la ejecución del programa openssl.

Esto exige a crear una infraestructura externa a TinyCA para que toda la información (pública y privada) no esté reunida en una misma unidad.
 - b) TinyCA no permite la gestión conjunta de una jerarquía de varias autoridades de certificación, permitiendo tener sólo una autoridad de certificación abierta.

6.5. Respecto al modelo de procesos

Con el desarrollo de este trabajo, queda en evidencia, una de las grandes desventajas que presenta el modelo inicial, es decir, que una AC genere para un determinado usuario, tanto el certificado digital con su clave pública, como su clave privada. Este modelo vulnera la seguridad en el resguardo de las claves privadas de los usuarios, por cuanto, no sólo son conocidas por el usuario final, sino también por la autoridad certificadora quien es, finalmente, la entidad que ingresa la clave privada del usuario para la creación de dicho certificado. Esto se agrava, aún más, considerando que el UF envía su clave privada

mediante formato impreso (sellado) a la AC competente, lo cual también podría vulnerar su seguridad, considerando una posible violación de esta por parte de terceros a través del sistema de correos de la organización.

Para corregir lo anterior, la AC debe fiscalizar la integridad e inviolabilidad de dicha solicitud antes de generar el respectivo certificado digital. Por otra parte, para minimizar la filtración de las claves privadas de los integrantes del sistema, la organización mantiene dichas claves en un servidor externo al de funcionamiento de la PKI, evitando el ingreso a través de la red de terceros indeseables, con la intención de obtener la clave privada de algún usuario.

Uno de los mayores problemas que se presentan cuando la AC tiene todas las claves privadas almacenadas, es cuando una de ellas es duplicada y, peor aún, se hace mal uso de ellas. Uno de los cambios más trascendentes propuestos en este documento, es el hecho de introducir al proceso, la posibilidad de que cualquier miembro de la comunidad genere su propio certificado digital y su par de claves (pública y privada), entregando únicamente su certificado digital con la clave pública a la AC, para que este la valide y publique en el repositorio para conocimiento del resto de los integrantes. Con esto, se desligaría a la AC de la responsabilidad en la filtración de la clave privada de un usuario, ya que de producirse esta situación, sólo sería responsable quien posee su clave privada y en este caso la responsabilidad recae sólo en el usuario final.

La existencia de autoridades de registro en gran parte de la organización, permite disminuir la carga de actividades de la AC (principalmente, en la generación de solicitudes y en la validación de los datos del usuario), existiendo siempre el problema que la organización posee sólo una AC centralizada en la ciudad de Santiago, esto impacta profundamente, cuando la AR se encuentra sin sistema para realizar las solicitudes a la AC, ya que el canal de comunicaciones microondas (propietario de la organización) puede presentar cortes en el troncal a la ciudad de Santiago, provocando que las AR deban utilizar procesos alternativos como el llenado del libro de registro, en la espera del restablecimiento del sistema. Para solucionar esto, se propone, en el futuro, modificar dicho proceso por una jerarquía de AC, permitiendo la generación de certificados digitales en niveles inferiores de la organización.

Una ventaja en la implementación de este sistema, es la existencia de una base de datos centralizada que contiene la información personal de cada solicitante de un certificado digital, permitiendo validar su información y no duplicar dichos CD para un mismo integrante de la organización.

6.6. Respecto a la utilización de la herramienta BPMN

La notación BPMN, otorga la capacidad para diagramar de forma sencilla y formal todas las actividades involucradas en los procesos requeridos, de comienzo a fin. Dar un orden a los procesos que se encontraban escritos o como una simple idea, llevándolos a una graficación de fácil entendimiento.

La modelación, mediante la utilización de un modelo formal, permite contribuir a la implementación de una infraestructura de clave pública en la organización, ayudando a su

divulgación y elaboración de manuales de uso de certificados digitales que sea comprensible para toda la organización.

El presente trabajo, permite dar un orden lógico a la secuencia que existe desde que se genera una solicitud de creación de certificado digital, hasta su desecho. Determinando, claramente, las responsabilidades e interacciones existentes entre las distintas entidades involucradas a través del proceso, simplificando la comprensión de los procesos y subprocesos, mediante la utilización de anidamiento de sus subprocesos.

El contar con procesos bien definidos, permite dar una trascendencia en el tiempo de la información plasmada en ellos, minimizando el efecto que provoca la alta rotación del personal dentro de la organización.

GLOSARIO

SIGLA	DESCRIPCIÓN
AC	Autoridad Certificadora
AR	Autoridad de Registro
CV	Ciclo de Vida
CD	Certificado Digital
DN	Distinguished Names
EPSC	Entidad Prestadora de Servicios de Certificación
IETF	<i>Internet Engineering Task Force</i>
LRC	Lista de Revocación de Certificados
PSC	Prestadora de Servicios de Certificación
PKI	<i>Public Key Infrastructure</i>
PSC	Prestadora de Servicios de Certificación
REP	Repositorio
RFC	<i>Request For Comments</i>
UF	Usuario Final
X.509	Estándar de Certificado

BIBLIOGRAFÍA

BizAgi. (2008). *BizAGi*. (BizAgi) Recuperado el 06 de mayo de 2011, de <http://www.bizagi.com/esp/>

Carlisle Adams, S. L. (2002). *Understanding PKI: Concepts, Standards, and Deployment Considerations, Second Edition*. Boston: Pearson Education, Inc.

Chile Emprende. (07 de Mayo de 2007). *Chile Emprende*. Recuperado el 19 de Mayo de 2010, de Contabilidad Electrónica, Un Ahorro Para Las Pyme: http://chileemprende.cl/home/index.php?option=com_content&task=view&id=142&Itemid=190#Top

Contraloría General de la República. (2004). Dictamen N° 4941 "Firma Electrónica de los Servicios Públicos". (4941) . Santiago.

Gero Decker, A. G.-B. (2008). *BPMN - Business Process Modeling Notation. BPMN - Business Process Modeling Notation 1.1 Poster* . Potsdam, Alemania: IT Systems Engineering, Universität Potsdam.

IETF, R. H. (Abril de 2002). internet X.509 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile. *Request for Comments: 3280* . IETF.

Instituto Nacional de Normalización. (2003). *NCh 2803.Of2003 "Tecnología de la Información" - Requisitos de las políticas de la autoridades certificadoras que emiten certificados de claves públicas*. Santiago: INN.

Instituto Nacional de Normalización. (2003). *NCh 2777.Of2003 "Tecnología de la Información - Código de prácticas para la gestión de seguridad de la información"*. Santiago: INN.

Ministerio de Economía, Fomento y Reconstrucción. (2002). *Guía de Evaluación Procedimiento de Acreditación Prestadores de Servicios de Certificación, Versión 1.0*. Santiago.

Ministerio de Economía, Fomento y Reconstrucción. (2002). *Ley 19.799; "LEY SOBRE DOCUMENTOS ELECTRÓNICOS, FIRMA ELECTRÓNICA Y SERVICIOS DE CERTIFICACIÓN DE DICHA FIRMA*. Santiago.

Ministerio Secretaría General de la Presidencia . (2004). Decreto N° 83. *Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos* . Santiago.

OMG. (Febrero de 2008). Business Process Specification. *BPMN 1.1* . Object Management Group.

Polacic, G., Rozman, T., & Vajde, R. (2007). *Business Porcess Modelling Notation (BPMN) Poster*. University of Maribor, Faculty of Electrical Engineering and Computer Science.

Servicio de Impuestos Internos. (2004). Resolución Exenta SII N°63 del 15 de Julio del 2004. *Establece Normas y Procedimientos de Operación para los Organismos Públicos que Sean Autorizados como Receptores Electrónicos de Documentos Tributarios Electrónicos*. Santiago.

Servicios de Impuestos Internos. (2003). Resolución Exenta SII N° 45 del 01 Septiembre del 2003. *Establece normas y procedimientos de operación respecto de los documentos Tributarios Electrónicos* . Santiago.

TinyCA. (s.f.). *TinyCA*. Recuperado el 14 de Diciembre de 2008, de <http://TinyCA.sm-zone.net/White>, S. A. *Introduction to BPMN*.

ANEXOS

ANEXO A: DESCRIPCIÓN DE NOTACIÓN BPMN UTILIZADA

El “*Business Process Modeling Notation*” (BPMN) es una notación formal, realizada para estandarizar y proveer el fácil entendimiento para cualquier persona que sea parte de una organización de negocio, considerando desde los diseñadores de los primeros borradores de los procesos, los especialistas encargados de implementar los procesos y hasta las personas que, finalmente, controlan y ejecutaran los procesos. El BPMN en su versión 1.0 fue publicada en mayo de 2004 por la “*Business Process Management Initiative (BPMI) Notation Working Group*”. Actualmente, la iniciativa es mantenida por el “*Object Management Group*”(OMG) y está disponible la versión 2.3.0.5 de fecha Mayo del 2012.

El propósito de la notación, es facilitar la descripción de los procesos de negocios, para lo cual su producto final son los diagramas de proceso de negocio, o BPD (*Business Process Diagram*), una representación que se basa, esencialmente, en las técnicas de diagramado de flujos para crear modelos. Estos gráficos representan la secuencia u operación de los procesos de negocio mediante una red de objetos que simbolizan actividades y flujos que definen el orden en que se ejecutan. BPMN intenta cerrar la brecha existente entre el diseño de procesos de negocio y la implementación de estos.

El BPMN fue una notación aprendida y practicada durante el desarrollo del magister, por lo tanto, dada su formalidad, se estimó como la más adecuada para desarrollar el modelado de los procesos de negocio de la entidad prestadora de servicios de certificación.

Para el desarrollo de los diagramas BPMN, se empleó la herramienta de software para el modelado de procesos “*BizAgi Process Modeler*” (BizAgi, 2012), en su versión 2.3.0.5, aplicación que es distribuida en forma gratuita por la empresa del mismo nombre. Esta empresa se dedica al modelado, automatización, ejecución y mejoramiento de procesos, pudiendo encontrarse más información en www.bizagi.com. Por esta razón, a continuación se mostrarán los elementos gráficos con los diagramas que son empleados por este software.

A.1. Elementos gráficos utilizados

La notación se estructura, esencialmente, de un grupo de cuatro elementos básicos.

A continuación, dentro de cada grupo se describirán sólo los diagramas de BPMN que fueron empleados para elaborar los diagramas el modelo. Además, la diagramación fue desarrollada de acuerdo a las recomendaciones dadas en documentos como “*BPMN and Business Process Management*” (Owen & Raj, 2003), “*Business Porcess Modelling Notation (BPMN)*” (Polacic, Rozman, & Vajde, 2007), “*BPMN - Business Process Modeling Notation 1.1*” (Gero Decker, 2008) e “*Introduction to BPMN*” (White). Éstos son:

A.2. Objetos de flujo (*Flow objects*)

Evento (*Event*)

Un evento se representa por un círculo y ocurre durante el curso de un proceso de negocio. Los eventos afectan el flujo del proceso y usualmente, tienen un causa (*trigger* - gatillo) o un impacto (*Result* – resultado). Los eventos se representan con círculos con el centro abierto para permitir anotar diferentes gatillos o resultados. Hay tres tipos de eventos: Comienzo (*Start*), Intermedio (*Intermediate*), Fin (*End*).

Actividad (*Activity*)










Una actividad se representa por un rectángulo con sus bordes redondeados y es un término genérico para el trabajo que una organización realiza. Un actividad puede ser atómica o no atómica (compuesta).








Decisión (*Gateway*)

Una decisión es representada por la figura de un diamante y se usa para controlar la divergencia de la secuencia de un flujo. Determina las tradicionales decisiones, tanto bifurcaciones, como uniones y acoplamientos de flujos. Las anotaciones al interior indican el tipo de comportamiento de control

En la Tabla N° A-1 se muestra la forma de los diagramas los objetos de flujo.

Tabla N° A-1 Diagramas de objetos de flujo

Objetos de Flujo	Diagrama
Eventos	
- Comienzo	
<ul style="list-style-type: none"> Evento de inicio que indica el comienzo de un proceso Evento de inicio de mensaje, en donde un mensaje llega desde un participante y gatilla el inicio del proceso 	
- Intermedio	
<ul style="list-style-type: none"> Evento de mensaje, un mensaje se recibió o es enviado por un participante, causando que el proceso continúe. Evento de temporización, es usado como un mecanismo de espera. 	
- Fin	
<ul style="list-style-type: none"> Evento de fin, indica donde un proceso termina. Evento de fin de mensaje, indica que un mensaje es enviado al término del proceso 	
Actividades	
<ul style="list-style-type: none"> Tareas, es aquella desarrollada durante el proceso 	
<ul style="list-style-type: none"> Tarea de usuario, aquella que es desarrollada por un humano, con o sin asistencia de una aplicación. 	
<ul style="list-style-type: none"> Tarea de Recepción, aquella que espera la llegada de un mensaje. 	

<ul style="list-style-type: none"> • Tarea de envío, aquella que es diseñada para enviar un mensaje. 	
<ul style="list-style-type: none"> • Tarea manual, aquella que se espera que sea ejecutada sin la ayuda de ninguna aplicación o mecanismo. 	
<ul style="list-style-type: none"> • Tarea de script, aquella que es ejecutada con la ayuda de alguna aplicación del proceso. 	
<ul style="list-style-type: none"> • Sub proceso anidado, es una actividad que está conformada por otras actividades. 	
Objetos de Flujo	Diagrama
Decisiones	
<ul style="list-style-type: none"> • Compuerta exclusiva basada en datos, aquella que permite que el flujo continúe exclusivamente por una de sus alternativas. • Compuerta paralela, indica un flujo paralelo de actividades. • Compuerta exclusiva basada en una decisión, permite que el flujo continúe después de haber tomado una decisión. 	  

A.3. Objetos de conexión (*Connecting Objects*)

Los objetos de conexión u objetos de flujo se conectan entre ellos en un diagrama para crear el esqueleto básico de la estructura de un proceso de negocio

Existen tres tipos de objetos de conexión que proveen esta función de flujo:

Flujo de secuencia (*Sequence flow*)

Una secuencia de flujo se representa por una línea sólida con el extremo sólido. Es usada para mostrar el orden (secuencia) de la actividad dentro del proceso.

Flujo de mensaje (*Message flow*)





Un flujo de mensaje se representa por una línea segmentada con el extremo sin relleno. Es usada para mostrar el flujo de mensajes entre dos participantes de procesos separados, como entidades empresariales o roles empresariales distintos (*business entities o business roles*), es decir, en “*Pool*” distintos como se verá más adelante

Asociación (*Association*)

Una asociación se representa por una línea segmentada, finamente, con el extremo en punta. Se usa para asociar datos, textos u otros artefactos con flujos de objetos. Las asociaciones son usadas para mostrar las entradas y salidas de las actividades.

En la Tabla N° A-2 se muestra la forma de diagramas los objetos de conexión.

Tabla N° A-2 Diagramas de objetos de conexión

Objetos de Conexión	Diagrama
i. Secuencia de Flujo	
Flujo condicional, indica que el flujo sucede dependiendo de una decisión	
ii. Flujo de mensaje	
iii. Asociación	

A.4. Carriles (*Swimlanes*)

Otras técnicas de modelados también utilizan el concepto de “carril”, como mecanismo de organización de actividades en categorías visuales separadas para ilustrar las diferentes capacidades funcionales o responsabilidades. BPMN utiliza dos tipos carriles:

Fondo Común (*Pool*)

Un “*Pool*” representa un participante o una entidad en un proceso determinado, pero también, se utiliza como contenedor gráfico que separa un grupo de actividades realizadas por un participante de otros “*Pool*” cuando los diagramas involucran a dos entidades de negocios o participantes separados, por lo que se deben graficar, físicamente, separados en el diagrama.

Las actividades dentro de “*Pools*” separados son consideradas autocontenidas en el proceso. De esta forma, la secuencia del flujo podría no atravesar el límite del *Pool*.

Los flujos de mensajes son los mecanismos que muestran la comunicación entre dos participantes, conectando de esta manera a dos “*Pools*” (ó objetos dentro de los *Pools*).


Línea (*Lane*)

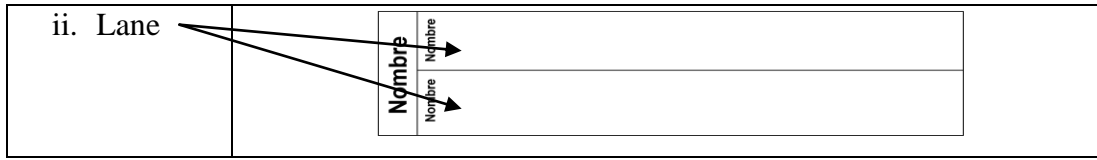
Los “*Lanes*” son más cercanos a los “*swimlanes*” que, tradicionalmente, se utilizan para modelar procesos de negocio.

Los “*Lanes*” son usados para separar actividades asociadas con una función específica de la organización, es decir, dentro del mismo “*Pool*”. Por lo que la secuencia de flujos puede atravesar los límites del “*Lane*” dentro de un “*Pool*”, sin necesidad de usar flujos de mensajes entre objetos de flujo en “*Lanes*” del mismo “*Pool*”.

En la Tabla N° A-3 se muestra la forma de diagramar a los carriles

Tabla N° A-3 Diagramas de los carriles

Carriles	Diagrama
i. Pool	



A.5. Artefactos (*Artefacts*)

BPMN fue diseñado para permitir flexibilidad y no está limitado el número de artefactos que se pueden agregar a un diagrama para que este represente, apropiadamente, al contexto del negocio.

Los diseñadores y modeladores pueden crear sus propios tipos de artefactos que agreguen más detalle al proceso. Sin embargo, la estructura básica de los procesos, es especificada sólo con objetos de flujo y objetos de conexión.

BPMN predefine tres tipos de artefactos.

Objetos de datos (*Data object*)

Los objetos de datos son un mecanismo para mostrar cómo las actividades requieren o producen objetos. Ellos se conectan a las actividades a través de asociaciones.



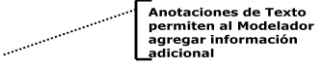
Grupo (*Group*)

Un grupo es representado por un rectángulo redondeado dibujado con línea segmentada. El agrupamiento puede ser usado para propósitos de documentación o análisis, y no afecta la secuencia del flujo.

Anotaciones (*Annotation*)













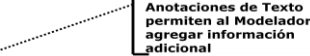

Las anotaciones son artefactos para que un modelador pueda agregar información textual adicional para el lector del diagrama BPMN, tal como se muestra en la Tabla N° A-4.

Tabla N° A-4 Diagramas de los artefactos

Artefactos	Diagrama
i. Objeto de datos	
ii. Grupos	
iii. Anotaciones	

A.6. Resumen de elementos centrales de BPMN

Tabla N° A-5 Resumen de elementos centrales de BPMN

a) Objetos de Flujo	
i. Evento	
- Comienzo	
- Intermedio	
- Fin	
ii. Actividad	
- Tareas	
- Sub proceso	
iii. Decisión	
b) Objetos de Conexión	
iv. Secuencia de Flujo	
v. Flujo de mensaje	
vi. Asociación	
c) Carriles	
iii. Pool	
iv. Lane	
d) Artefactos	
iv. Objeto de datos	
v. Anotaciones	
vi. Grupos	

ANEXO B: ANTECEDENTES DE FUNCIONAMIENTO DE LA ENTIDAD PSC

B.1. Servicios prestados por la AC

- a. Acreditar y verificar los antecedentes personales de los operadores que se desempeñarán en las autoridades de registro.
- b. Emitir los certificados con mecanismos tecnológicos y criptográficos que garanticen que el proceso de certificación es realizado adecuadamente, siguiendo el estándar X.509 y de acuerdo a lo siguiente:
 - 1) Certificados para uso personal:
Longitud de Claves: de 1024 a 4096 bits
Validez: hasta 2 años o por cambio de grado jerárquico / destinación
 - 2) Certificados para Dispositivos
Longitud de Claves: de 1024 a 4096 bits
Validez: hasta 2 años o por cambio de configuración
- c. Revocar, unilateralmente, los certificados, por solicitud y en los cuales se vea comprometida la confianza respecto a la veracidad de su contenido.
- d. Enviar al directorio de los servicios (repositorio) las claves públicas de los usuarios para que se encuentren disponibles al público en general y las listas de revocación de certificados, cada vez que se produzca una revocación de certificado para que sea pública.
- e. Publicar en su sitio web en la intranet institucional, las prácticas de certificación utilizadas.

B.2. Lugares donde operará

La autoridad certificadora se encuentra implementada, en forma centralizada, con sus instalaciones, en la comuna de Peñalolén, las autoridades de registro en el futuro operarán, en forma remota, en instalaciones de cada una de las unidades a las cuales pertenezcan, respectivamente, y el usuario final operará en forma centralizada.

B.3. Tipos de certificados que se entregarán

Se entregarán certificados digitales personales como para dispositivos informáticos o de comunicaciones. Los que serán utilizados de acuerdo a lo siguiente:

- a. Certificados de uso personal.
 - 1) Firma, cifrado y/o sellado de tiempo de documentos electrónicos.
 - 2) Firma, cifrado y/o sellado de tiempo de mensajería electrónica.
 - 3) Autenticación a sistemas electrónica de tratamiento de Información.
- b. Certificados de dispositivos.
 - 1) Establecer VPNs.
 - 2) Autenticación a sistemas electrónicos de tratamiento de información u otros dispositivos informáticos o de comunicaciones.
 - 3) Firma, cifrado y/o sellado de tiempo de documentos electrónicos.
 - 4) Firma, cifrado y/o sellado de tiempo de mensajería electrónica.

Las LRCs de certificados son emitidas de acuerdo con el formato CRLv2 definido por X.509, conforme a la siguiente estructura:

Tabla N° B-3a Formato X.509 v3

Nombre	Descripción
Versión	Versión empleada en la lista de revocaciones
Emisor	Información de la AC emisora de la CRL E: Casilla de e-mail de la AC CN: Nombre de la AC OU: Organización superior a la AC. O: Organización de la AC. L: Ciudad. S: Comuna. C: País.
Fecha efectiva	Fecha de efectividad de publicación de la LRC.
Próxima Actualización	Fecha de próxima publicación de la LRC.
Algoritmo de firma	Algoritmo de firma empleado en la LRC.

Los certificados digitales son emitidos de acuerdo al estándar X.509, conforme a la siguiente estructura:

Tabla N° B-3b Estándar X.509 v3

Campo	Descripción
Versión	Certificado en versión 3
Numero de serie	Número que identifica unívocamente al certificado
Algoritmo de firma	Algoritmo empleado por la AC para firma el certificado
Emisor	Nombre distintivo (DN) del Emisor, formato X.509 Debe incluirse: E: e-mail de la AC emisora. CN: Nombre de la AC. OU: Organización superior de la cual depende la AC. O: Organización de la cual depende la AC. L: Cuidad de ubicación de la AC S: Comuna de ubicación de la AC C: País
Válido desde	Fecha de Inicio de validez del certificado.
Válido hasta	Fecha de Término de validez del certificado.
Asunto	Nombre distintivo (DN) del titular, formato X.509 Debe incluirse: E: e-mail del Titular.

	CN: Nombre del Titular. OU: Organización superior del Titular O: Organización del Titular L: Ciudad de ubicación del Titular S: Comuna de ubicación del Titular C: País
Clave pública	Clave pública del titular del certificado (mínimo 1024).
Restricciones básicas	Restricciones del certificado emitido

B.4. Instrucciones para el emplear el libro de la AR

- a. Todo integrante que se presente a la AR solicitando un certificado digital debe ser registrado en el Libro de la AR.
- b. Debe tener sus hojas numeradas y ser elaborado de acuerdo a las políticas vigentes.
- c. Debe ser llenado, personalmente, por un integrante de la AR, comprobando los datos con la Cédula de Identidad y consulta al sistema de personal.

B.5. Procedimientos para la autoridad certificadora

Los procedimientos para la autoridad certificadora se desarrollaron de acuerdo a las características de la aplicación de gestión de certificados digitales “Tiny CA”, en su versión 0.7.3, basada en OpenSSL. Aplicación de fuente abierta que fue seleccionada durante la investigación inicial para la generación, emisión y gestión de los certificados.

B.6. Procedimientos del repositorio

La actualización de datos debe ser realizada cada vez que se emitan, caduquen o se revoquen certificados digitales o al menos al último día hábil de la semana. Considerando un tiempo de ejecución no mayor a seis horas.

B.7. Medidas de protección de los activos

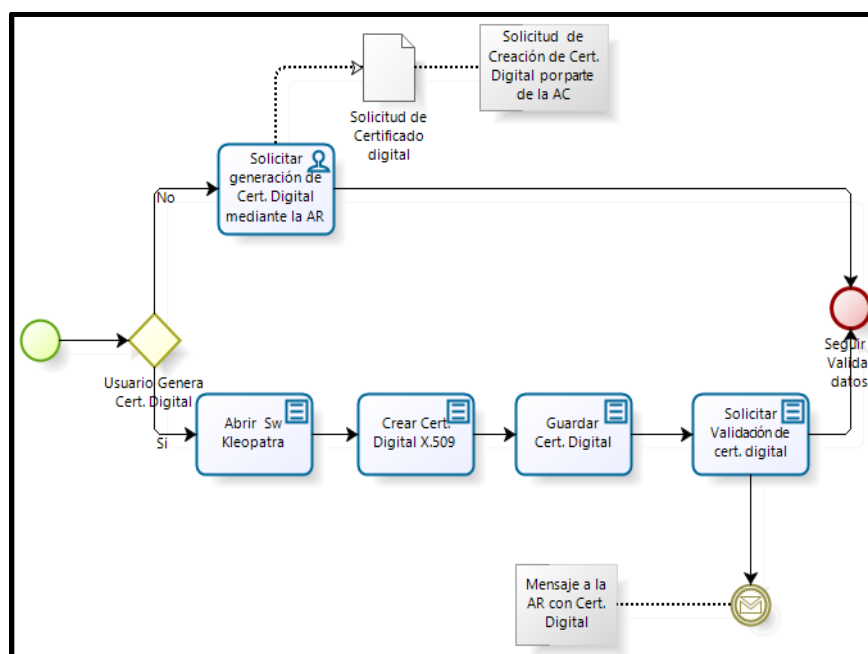
- a. Ejecutar todas sus actividades de certificación acorde a lo normas estipulados en presente documento.
- b. Proceder de acuerdo a lo estipulado en los planes de contingencia, en caso de contingencia y/o desastres.
- c. Revisar cada seis meses el estudio de análisis de riesgo, si es del caso actualizándolo. Así como a la respectiva política de seguridad
- d. Mantener el sistema maestro de administración de certificados aislado y sin interconexión con alguna red interna o externa, el traspaso de información se realizará por un medio de almacenamiento adecuado entre el sistema y la intranet.
- e. Crear sus propios certificados raíz, los que se deben guardar en un lugar seguro, con respaldos antidesastres y con procedimientos de contingencia adecuados.

- f. Emitir los certificados con mecanismos tecnológicos y criptográficos que garanticen que el proceso de certificación es realizado adecuadamente.
- g. Almacenar en una base de datos de la AC por un tiempo mínimo de seis años, los certificados generados para cada entidad.
- h. Contar con una base de datos que almacene los Certificados Digitales emitidos, Listas de Revocaciones emitidas y Solicitudes recibidas, protegido con las medidas de seguridad físicas y lógicas adecuadas.
- i. Mantener los resguardos tecnológicos para evitar cualquier falsificación y adulteración de las claves privadas mantenidas por la AC.
- j. Entregar los Certificados emitidos en medios adecuados a los usuarios, conforme lo establece las disposiciones de seguridad.
- k. Mantención de un registro electrónico actualizado con la lista de los certificados revocados y/o suspendidos.
- l. Revocar, unilateralmente, los certificados, en los cuales se vea comprometida la confianza respecto a la veracidad de su contenido, y notificar a las partes correspondientes.
- m. Ingresar a la base de datos la información aplicaciones que deben ser operadas por personal informático que validen la información antes de ser ingresada.
- n. Revocar o suspender un certificado desde que se solicita hasta que se actualiza la base datos en un tiempo no mayor a 6 horas laborales, en horario de laboral de lunes a domingo.

ANEXO C: DETALLE DE PROCEDIMIENTOS DENTRO DE LA ENTIDAD PCS

C.5.3 Diagrama general del proceso de usuario

En la siguiente Figura, se muestra el diagrama del proceso de usuario cuando este decide generar su propio certificado digital. De esta forma, el usuario tendrá certeza absoluta que su clave privada no será conocida por ninguna otra persona. Para lo anterior, debe generar su certificado digital con la clave pública y enviarlo, posteriormente a la AC, para que esta la valide, firme y publique en el repositorio.



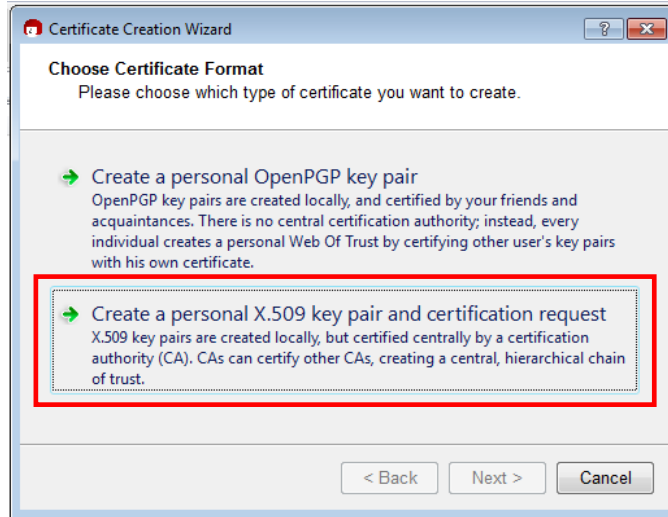
El usuario final tiene asociado las siguientes actividades:

- Solicitar certificado o crearlo
- Emplear certificado
- Solicitar nuevo certificado, solicitando la caducación del anterior

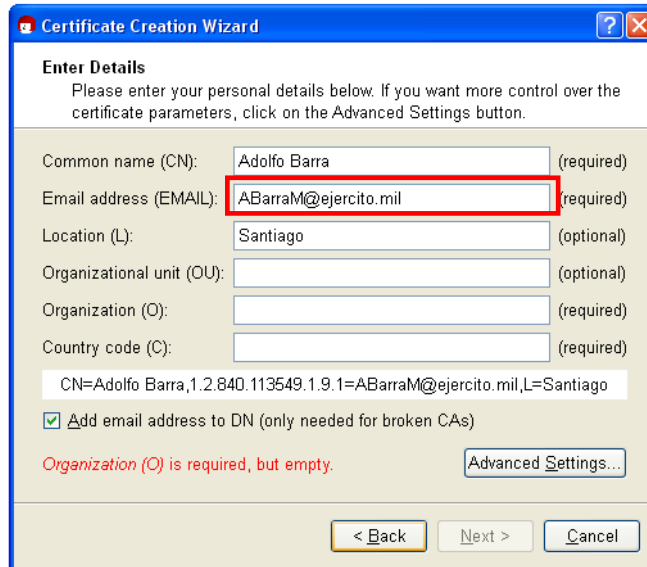
Descripción de las actividades del usuario dentro del proceso:

- Solicitar certificado o crearlo
 - Para solicitar la creación de un certificado digital por parte de la AC, este deberá hacerlo, a través de la AR de la instalación a la cual pertenece y una vez que esta autoridad valide los datos, deberá ingresar la solicitud en el sistema de la AC.
 - Para crear su propio certificado digital, el usuario debe tener instalado el software Gpg4win 2.1.0 que tiene asociado el gestor de certificados digitales "Kleopatra", el cual soporta los estándares de criptografía pertinentes OpenPGP y S/MIME (X.509), este es utilizado para cifrar y crear certificados por parte del usuario en su computador, posteriormente a la instalación se debe:

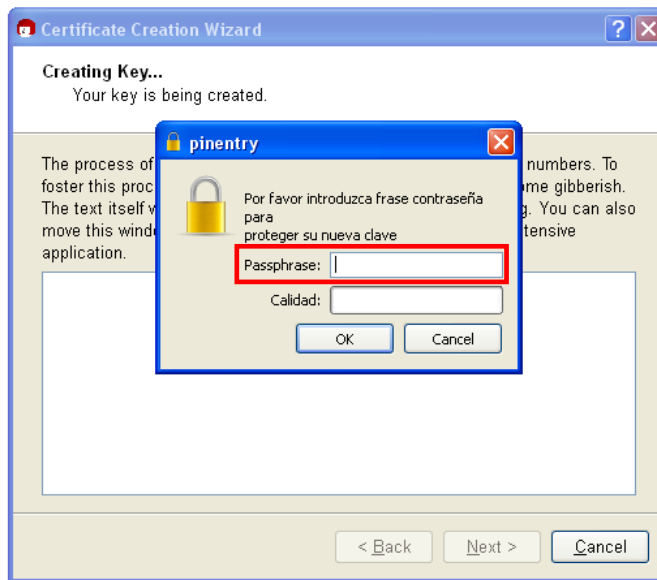
- i. Abrir “crear certificado” y elegir la opción señalada, la cual permite crear certificados mediante OpenPGP o bien utilizando el formato X.509, el que será el utilizado para este trabajo.



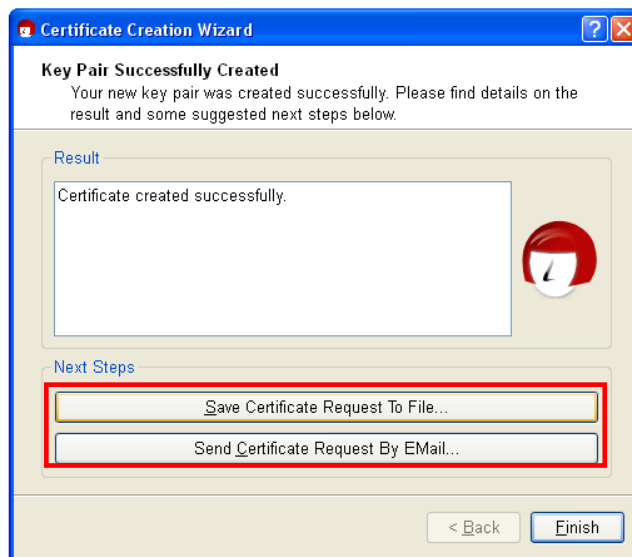
- ii. Posteriormente, se deben llenar los datos del usuario de tal forma que permita crear su propio certificado digital.



- iii. Una vez llenados los datos del usuario, se debe elegir una clave privada para crear su certificado digital y su clave pública.



- iv. Finalmente, una vez creado el certificado digital, este deberá ser enviado a la AR, mediante correo electrónico o bien, debe ser entregado en forma presencial, mediante un medio magnético, a esta AR, una vez que se concurra a validar sus datos personales.



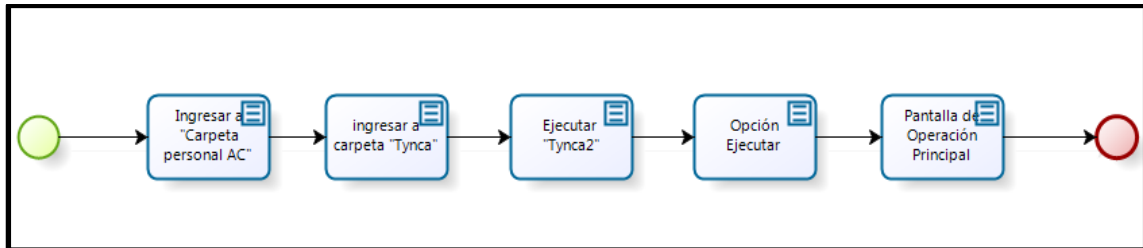
b. Emplear certificado digital

Durante el período de empleo del certificado digital, el usuario no debe comprometer la seguridad de su clave privada, quedando en condiciones de utilizar su certificado por un período no superior a 2 (dos) años o hasta el momento en que el usuario cambie de desempeño dentro de la organización.

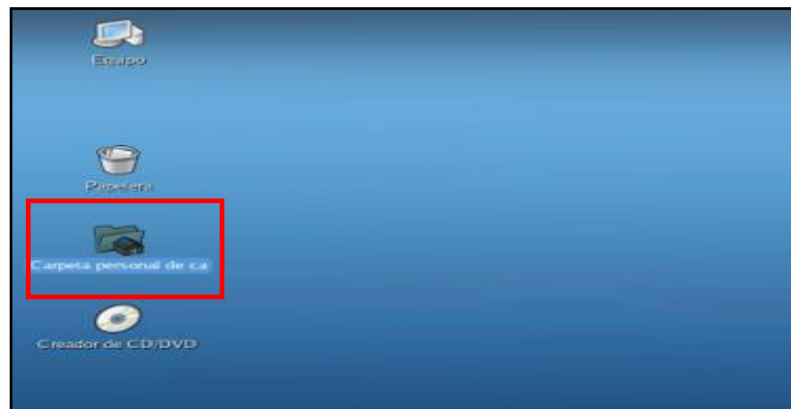
- c. Solicitar nuevo certificado, solicitando la caducación del anterior

Para solicitar la creación de un nuevo certificado digital, este debe solicitar la caducación de su certificado actual a la AR y solicitar la creación de otro certificado digital para su uso.

C.5.5.1.1 Ingresar a la aplicación de AC



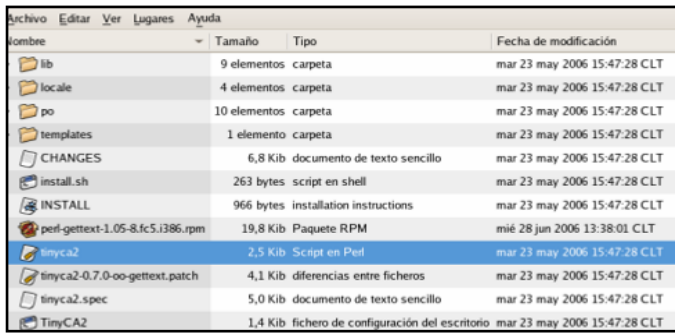
1. Se debe ingresar a la carpeta con el nombre: "Carpeta personal de ca", que se indica a continuación.



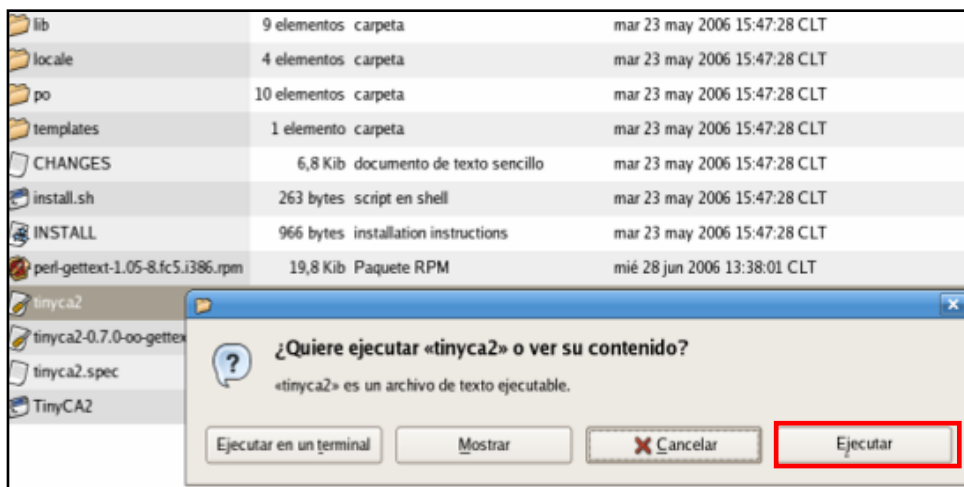
2. Luego se procede a ingresar la carpeta con el nombre "TinyCA2-0.7.3", que se indica a continuación.



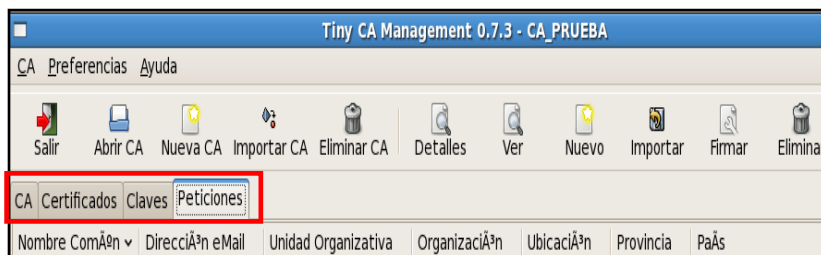
3. Al abrir la carpeta anterior, se mostrará la siguiente pantalla, donde se debe ejecutar "Tynca2".



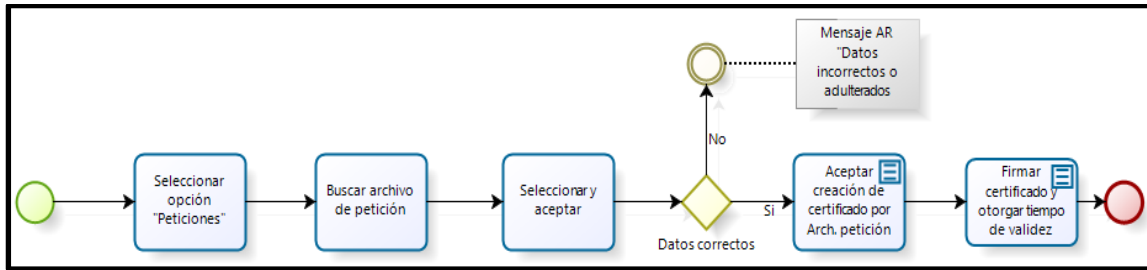
4. Luego se despliega la siguiente ventana en la cual, se debe seleccionar la opción “Ejecutar”.



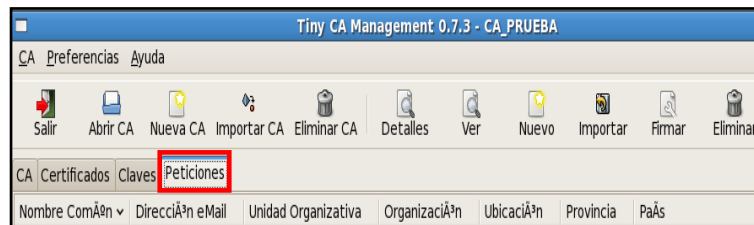
5. Este proceso se demora unos minutos, al completarse se desplegará la “pantalla de operación principal”, en donde aparecen las 4 opciones que se indican.



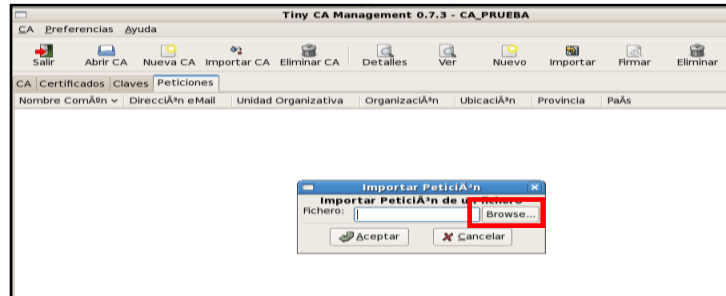
C.5.5.1.2 Generar certificado de dispositivo AC



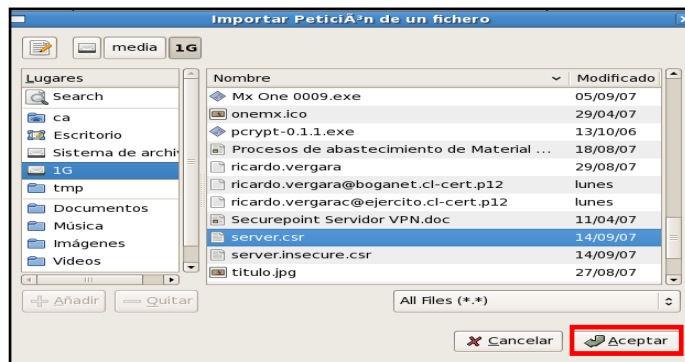
1. En la “pantalla de operación principal”, se debe seleccionar la opción “Peticiones” y desde ahí, seleccionar el archivo que ha sido enviado como una petición de certificado de servidor.



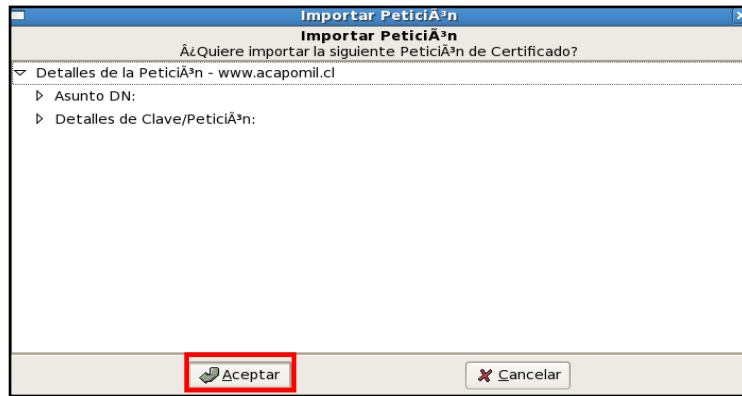
2. Luego se proyecta una ventana para buscar el archivo que permite crear el certificado de servidor. Se debe buscar el archivo con la opción “Browse”.



3. El archivo correspondiente con la extensión “.csr”, una vez encontrado, se debe “Aceptar”.



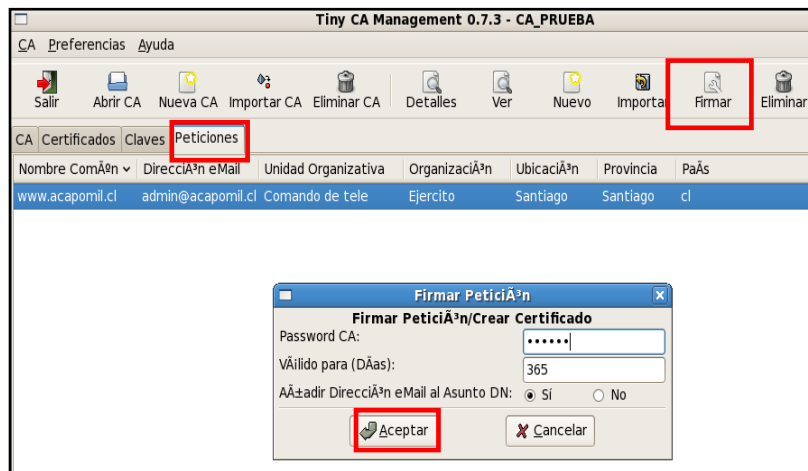
4. Luego de encontrar el archivo y aceptar, se proyecta una pantalla donde se verifica y pregunta si quiere importar la solicitud de certificado, se debe “Aceptar” siempre y cuando los datos y el archivos sean correctos.



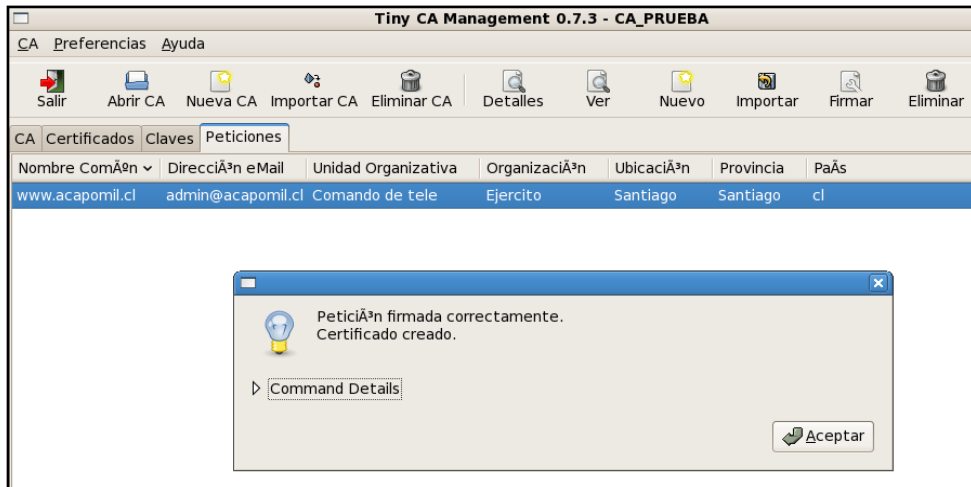
- Una vez realizado los pasos anteriores correctamente, en la opción “Peticiones”, se muestra la petición que se ha creado para la unidad que la solicitó.



- Luego se debe ir a la opción “Firmar” que se indica, e ingresar el “password” del operador y el tiempo de validez del certificado de servidor, mínimo 2 años y máximo la fecha de expiración de la autoridad certificadora, luego se acepta.



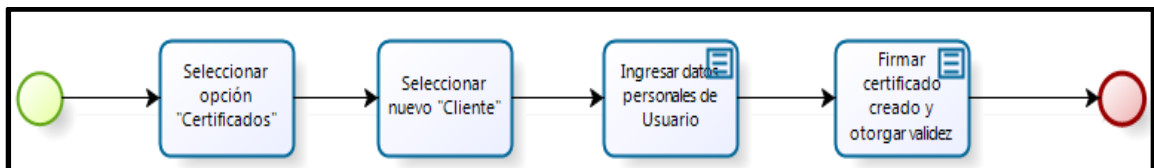
- Una vez firmada la petición, se proyecta la pantalla con la información que ha sido firmada correctamente, con este paso la petición queda lista para ser exportada.



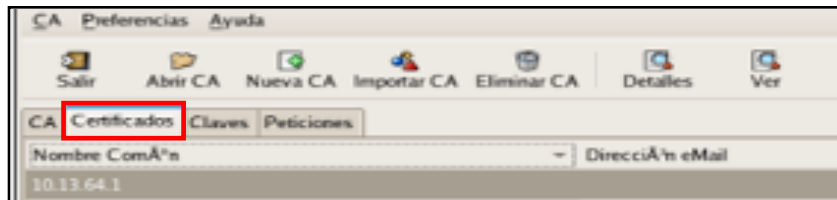
8. Luego de firmada la petición se debe exportar el certificado con sus respectivas extensiones: “.cert.crt “o “.p12 “



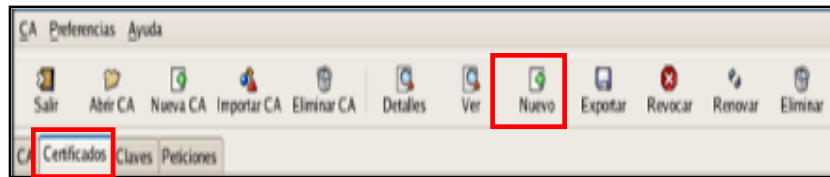
C.5.5.1.3 Generar certificado personal



1. En la “pantalla de operación principal”, se debe seleccionar la opción “Certificados”.



2. Después de lo anterior, se selecciona la opción “Nuevo” donde aparecerán dos opciones:
 - a. Crear clave y certificado (Servidor)
 - b. Crear clave y certificado (Cliente), posteriormente seleccionar la opción b.



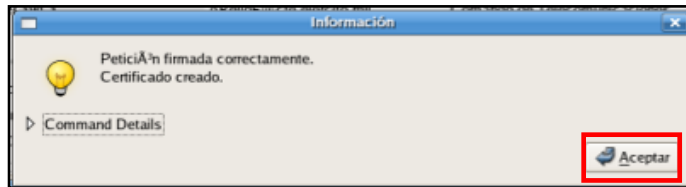
- Después de haber seleccionado la opción anterior, se muestra la siguiente pantalla, donde se deben ingresar los datos de la persona que solicitó el certificado.

Estos datos deben ser ingresados con estricto cuidado. El “password” ingresado en la etiqueta, debe ser la misma que ingresó el usuario en la solicitud del certificado. Se debe tener especial cuidado entre las minúsculas y mayúsculas.

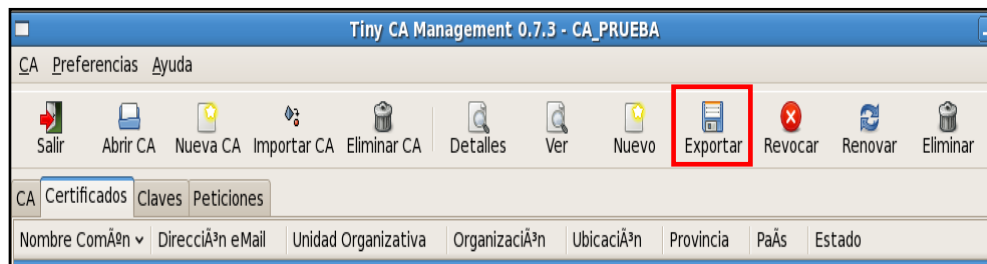
Después de haber ingresado todos los datos correctamente, se procede a aceptar.

- Finalmente para generar el certificado en el servidor y que éste quede firmado correctamente, se debe ingresar el “password” del operador y el tiempo de validez del certificado, luego se acepta.

- Luego se muestra la siguiente información, la cual informa que el certificado fue firmado correctamente. Con este paso se da término al procedimiento de creación del certificado, quedando el certificado listo para ser exportado.



- Para exportar el certificado digital se procede como se explica en el punto C.5.5.2.1.



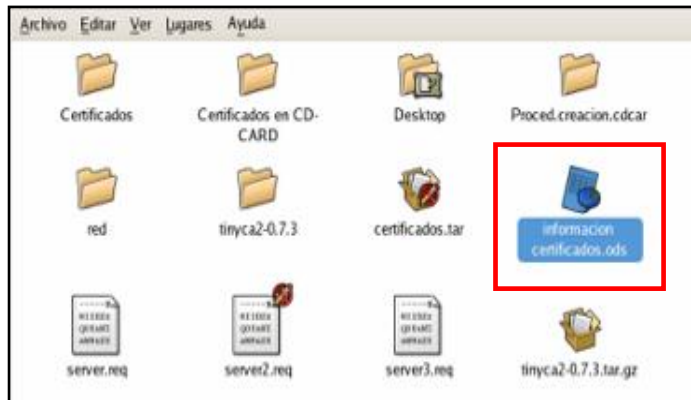
C.5.5.1.4 Registro de datos en tabla de datos



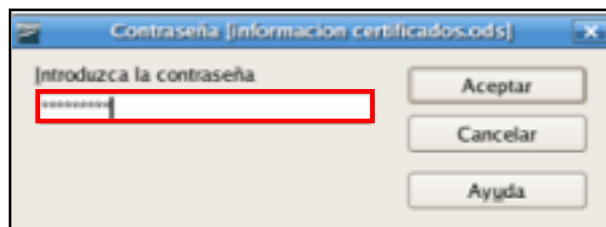
- Para ingresar los datos en respectiva la tabla de datos, se debe ingresar a la carpeta con nombre “Carpeta personal ca”, que se indica a continuación.



- Esta carpeta contiene un archivo, el cual debe ser abierto. Este archivo tiene el siguiente nombre: “Información certificados. ods”.

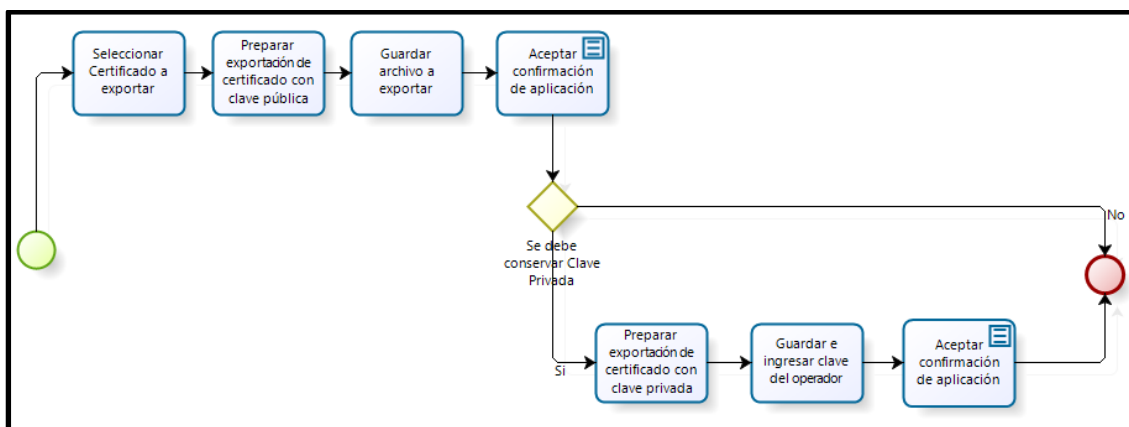


3. Para acceder al archivo, se debe introducir el “password” del operador del servidor.



4. Luego se ingresan los datos de la persona que solicita el certificado digital y finalmente, se debe guardar el archivo.

C.5.5.2.1 Exportar certificado digital



1. En la “pantalla de operación principal”, se debe seleccionar el nombre del usuario o unidad que solicitó el certificado, en “Certificados” o “Peticiónes” respectivamente, y elegir la opción “Exportar”.



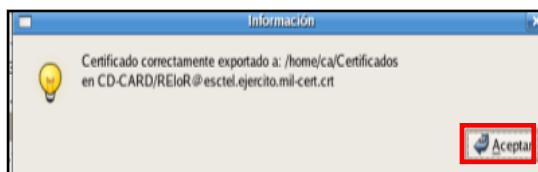
2. Luego se prepara la exportación del certificado con la clave pública, para lo cual se debe seleccionar la opción “DER”, y en el casillero “Fichero” se debe colocar la extensión del certificado: mil-cert.crt.



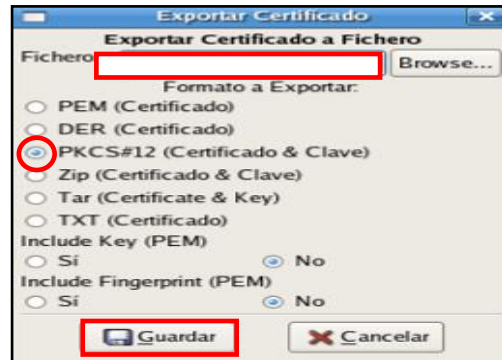
3. Luego de se selecciona la opción “Guardar”, durante este paso se está exportando la clave pública.



4. Para terminar de exportar el certificado se debe “Aceptar” en la pantalla siguiente.



5. Para preparar la exportación del Certificado con clave privada y pública en archivo de extensión PKCS#12, se debe seleccionar el archivo indicado “PKCS#12 (Certificado & Clave)”, este archivo se “Guarda” con la misma extensión que tiene.



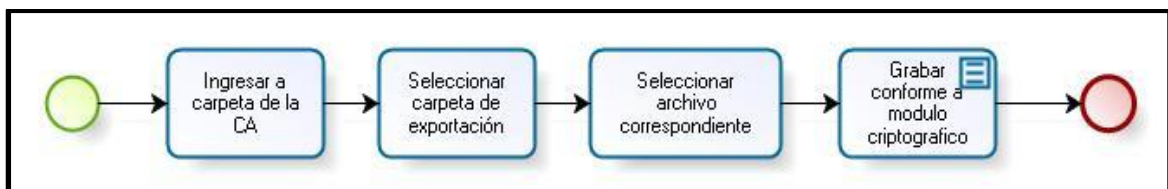
6. Al seleccionar la opción “Guardar” aparece una pantalla donde se debe ingresar un “password”. Este es necesario para poder exportar el certificado con la clave privada.

El “password” ingresado en el casillero correspondiente, debe ser la misma que ingresó el usuario en la solicitud del certificado. Se debe tener especial cuidado entre las minúsculas y mayúsculas

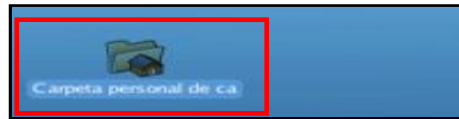


7. En el paso siguiente aparece una pantalla donde se informa que el Certificado y la Clave han sido exportados correctamente. Se procede a “Aceptar” y se da término al proceso de exportar el certificado digital.

C.5.5.2.2 Grabar certificado digital



1. Para realizar este procedimiento, se debe ingresar a la carpeta con el nombre “Carpeta personal de ca”, donde hay varias carpetas diferentes.

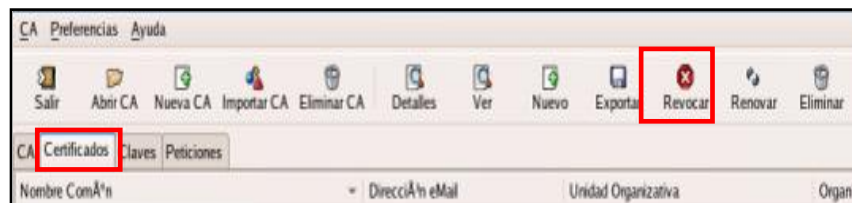


2. Se debe seleccionar la carpeta donde fueron enviados los archivos, al momento de guardarlos.
3. Al abrir esta carpeta, se debe seleccionar el archivo de certificado con clave privada, conforme al nombre de la persona a la que se le está confeccionando el certificado digital.
4. Grabar conforme al método correspondiente al módulo criptográfico que almacenará el certificado.

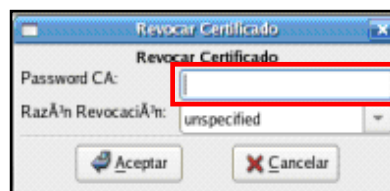
C.5.5.3.1 Revocar certificados



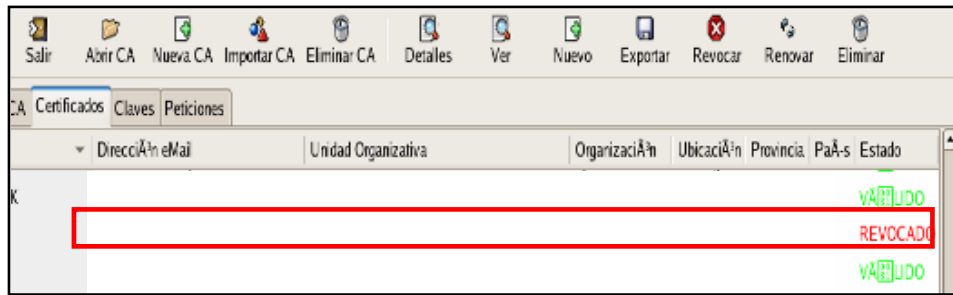
1. En la “pantalla de operación principal”, se debe ingresar a la opción “Certificados” y se selecciona el certificado a revocar.



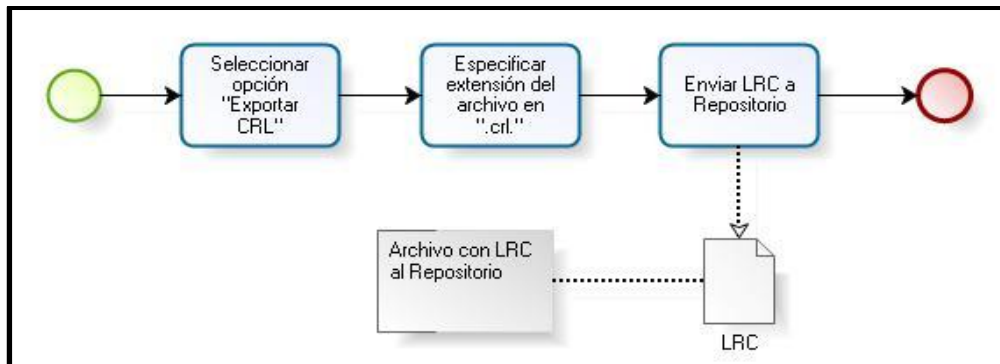
2. Luego se debe seleccionar la opción revocar, debiendo especificar una de las razones por cual será revocado el certificado, ingresando el “password” del operador y seleccionar aceptar.



3. El procedimiento anterior, termina cuando se verifica el estado del certificado, el cual cambia de VÁLIDO a REVOCADO, como se muestra en la siguiente pantalla.

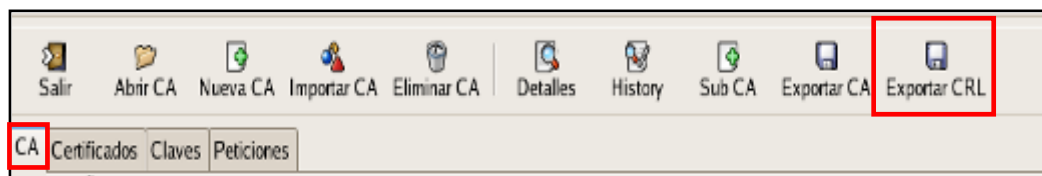


C.5.5.3.2 Exportar lista de revocación de certificados



1. Luego de revocar el certificado, se debe exportar la lista certificados revocados, con la finalidad de actualizar el repositorio donde están publicados todos los certificados que están vigentes.

Para realizar este paso, en la “pantalla de operación principal”, se debe seleccionar la opción “CA” y luego “Exportar CRL”.

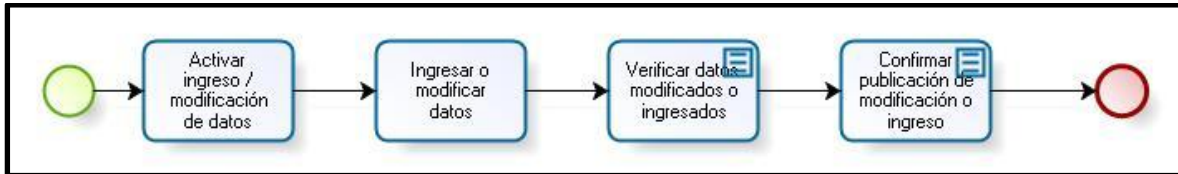


2. Aquí se debe especificar la extensión del archivo en la opción “Fichero”, que debe quedar con la extensión “.crl” y con la opción “Formato a Exportar”, seleccionada en la opción “DER”. Luego se debe ingresar el “password” del operador y finalmente se “Guarda”.



Con este paso se da término al procedimiento de exportar la lista de certificados revocados.

C.5.6.1 Publicar certificados (Claves públicas)



1. Una vez realizados los pasos anteriores, se debe ingresar al sitio web de intranet de la comunidad objetivo, aquí se puede activar el ingreso o modificación de datos, para esto se debe seleccionar la opción “Agregar” que se indica a continuación.

Dirección | hto

TABLA: directorio [Exportar a Excel](#) [Exportar a Word](#) [Exportar a XML](#)

Nombre contiene

Apellido contiene

Puesto contiene

Unidad contiene Seleccione uno

[Mostrar todos](#)

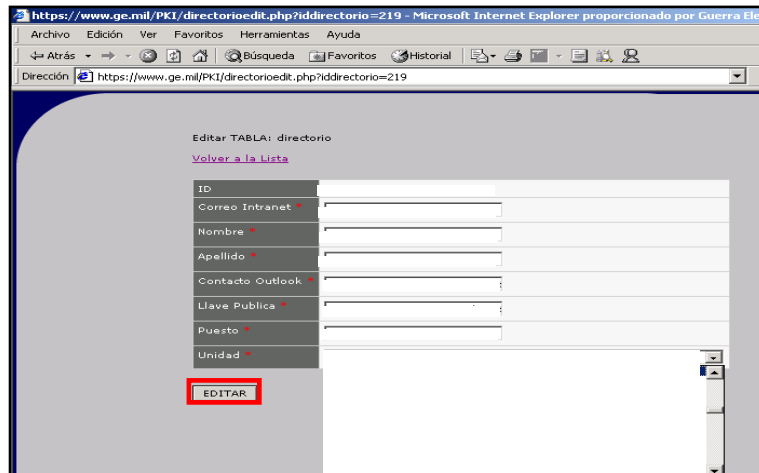
Frase exacta Todas la Palabras Cualquier Palabra

Página 1 de 11

Registros 1 to 20 de 209

ID	Correo Intranet (*)	Nombre (*)	Apellido (*)	Contacto Outlook (*)

2. Luego se proyecta la pantalla donde se deben ingresar los datos a publicar:
Estos datos deben ser ingresados como se indica.
 - Nombres
 - Apellidos
 - Dirección de correo electrónico
 - Puesto
 - Unidad
3. Finalmente, se procede a verificar los datos y confirmar la publicación seleccionando “Editar” o si se está ingresando datos nuevos seleccionando “Guardar”.



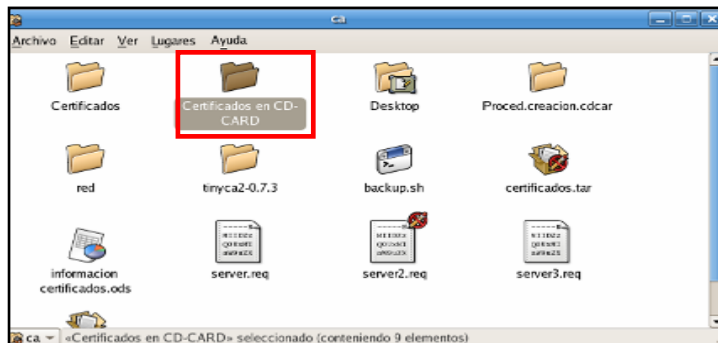
C.5.6.2 Publicar LRC



1. Después de haber exportado la LRC, se debe actualizar el servidor con los datos de los certificados que han sido caducados o revocados.
2. Seleccionar y abrir la carpeta con LRCs en el servidor de la AC de nombre: “Carpeta de personal ca”.



3. Dentro de esta carpeta se debe abrir la sub carpeta de nombre “Certificados”, y buscar el archivo que se nombra a continuación.



4. El archivo tiene el nombre de “Intranet.crl” con la fecha del día de modificación, eso demostrará que ha sido actualizado y que contiene nuevos datos. Se debe copiar en un medio extraíble para ser llevado al servidor del repositorio.

The image shows a screenshot of a file explorer window with a menu bar containing 'Archivo', 'Editar', 'Ver', 'Lugares', and 'Ayuda'. Below the menu bar is a table with columns for 'Nombre', 'Tamaño', 'Tipo', and 'Fecha de modificación'. The first row, 'INTRANET-ctrl.crl', is highlighted in blue. The second row, 'INTRANET-ctrl.pem', is in a lighter shade. The table data is as follows:

Nombre	Tamaño	Tipo	Fecha de modificación
INTRANET-ctrl.crl	2,8 Kib	desconocido	mar 03 jul 2007 13:28:12 CLT
INTRANET-ctrl.pem	2,7 Kib	Certificado X.509 codificado con DER/PEM/Netscape	jue 01 mar 2007 11:08:06 CLST

5. Se debe transferir el archivo “Intranet.crl” a la carpeta del servidor del repositorio que contiene las LRC.
6. Con este paso se da término a la actualización de la lista de revocación de certificados, lo cual ser debe verificado en la página web del repositorio.