



Implantación y certificación del servicio de firma electrónica en la Universidad de las Fuerzas Armadas “ESPE” – Sede Latacunga, utilizando ITIL V4

Jaramillo Araujo, Brandon Steven

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Trabajo de titulación previo, a la obtención del título de Ingeniero en Tecnologías de la Información

Ing. Ron Egas, Mario Bernabé

09 de junio del 2023

Resultados de la herramienta para verificación y/o análisis de similitud de contenidos

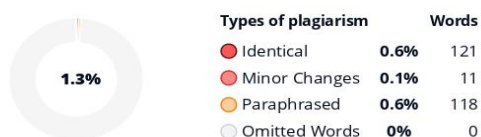


2. Tesis Jaramillo Brandon Word.docx

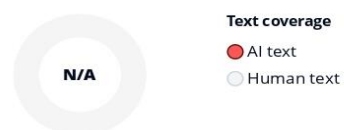
Scan details

Scan time: October 10th, 2023 at 21:12 UTC Total Pages: 78 Total Words: 19484

Plagiarism Detection



AI Content Detection



🔍 Plagiarism Results: (12)

🌐 FISE • ¿Qué es y para qué sirve la Firma Electrónica? 0.4%

http://web.uaemex.mx/fise/0_1_inciso.html

...

🌐 DSpace ESPOCH.: Desarrollo del sistema informátic... 0.2%

<http://dspace.esPOCH.edu.ec/handle/123456789/9091?mode...>

Skip navigation ...

🌐 Infraestructura de clave pública - Wikipedia, la enci... 0.2%

https://es.wikipedia.org/wiki/infraestructura_de_clave_p%c3...

Colaboradores de los proyectos Wikimedia

Ir al contenido Menú principal Menú principal mover a la barra lateral ocultar Navega...





Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Certificación

Certifico que el trabajo de titulación: **“Implantación y certificación del servicio de firma electrónica en la Universidad de las Fuerzas Armadas “ESPE” – Sede Latacunga, utilizando ITIL V4”** fue realizado por el señor **Jaramillo Araujo, Brandon Steven**; el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 27 de septiembre del 2023



.....
Ing. Ron Egas, Mario Bernabé MSc.

C.C: 1704229747



Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Responsabilidad de Autoría

Yo, **Jaramillo Araujo, Brandon Steven**, con cédula de ciudadanía n° 1105992729, declaro que el contenido, ideas y criterios del trabajo de titulación: **Implantación y certificación del servicio de firma electrónica en la Universidad de las Fuerzas Armadas "ESPE" – Sede Latacunga, utilizando ITIL V4** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 26 de septiembre del 2023

.....Brandon Jaramillo.....

Jaramillo Araujo, Brandon Steven

C.C: 1105992729



Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Autorización de Publicación

Yo **Jaramillo Araujo, Brandon Steven**, con cédula de ciudadanía n° 1105992729, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación:

Título: Implantación y certificación del servicio de firma electrónica en la Universidad de las Fuerzas Armadas "ESPE" – Sede Latacunga, utilizando ITIL V4 en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 26 de septiembre del 2023

Jaramillo Araujo, Brandon Steven

C.C.:1105992729

Dedicatoria

A mis padres, quienes han sido un pilar fundamental para permitirme cumplir con esta meta; quienes han sido mi mayor motivación para continuar hacia adelante y levantarme cada día a ser mejor.

A la persona más fuerte, dedicada y responsable que puedo conocer: yo.

Brandon Steven Jaramillo Araujo

Agradecimientos

Agradezco a mis padres, quienes me brindaron su apoyo incondicional para cumplir con esta meta. Su cariño, confianza y paciencia me impulsaron siempre a perseguir este sueño y nunca abandonarlo pese a las adversidades.

Brandon Steven Jaramillo Araujo

Índice de contenido

Resultados de la herramienta para verificación y/o análisis de similitud de contenidos ..	2
Certificación.....	3
Responsabilidad de autoría	4
Autorización de publicación	5
Dedicatoria	6
Agradecimientos.....	7
Índice de tablas	12
Índice de figuras	13
Resumen.....	16
Abstract	17
Capítulo I.....	18
Introducción	18
Planteamiento del problema	19
Justificación	19
Objetivos.....	20
Objetivo general	20
Objetivos específicos.....	20
Alcance	21
Hipótesis	23
Metodología.....	24
Metodología Science Research.....	24

Capítulo II.....	26
Fundamentación teórica.....	26
ITIL.....	26
Seguridad y criptografía	27
Firma electrónica.....	30
Certificado digital.....	33
Infraestructura de clave pública (PKI).....	33
Jerarquía PKI	34
Arquitecturas de PKI.....	36
Funcionamiento de una PKI	36
Tecnologías para la implementación de una PKI.....	38
Marco legal.....	39
Estado del Arte	42
Planteamiento de la revisión de literatura preliminar.....	43
Capítulo III.....	50
Implantación del servicio de firma electrónica	50
Objetivos	50
Alcance	50
Indicadores de cumplimiento	50
Recursos	50
Actividades a realizar	51

	10
Ejecución de actividades	51
Análisis de certificación.....	100
Objetivos	100
Alcance	100
Indicadores de cumplimiento	100
Recursos	100
Actividades a realizar	101
Ejecución de actividades	101
Capítulo IV	106
Análisis técnico de pre certificación	106
Objetivos	106
Alcance	106
Indicadores de cumplimiento	106
Recursos	106
Actividades a realizar	106
Ejecución de actividades	107
Capítulo V	116
Mejora del servicio y resolución de las no conformidades.....	116
Objetivo	116
Alcance	116
Indicadores de cumplimiento	116

Recursos	116
Actividades a realizar	116
Elaboración de las recomendaciones de mejora para la instalación del servicio ..	117
Elaboración de las recomendaciones de mejora para la arquitectura del servicio	119
Evaluación del cumplimiento del plan de mejora	124
Elaboración de alternativas de recaudación de presupuesto	125
Capítulo VI	126
Conclusiones	126
Recomendaciones	126
Referencias	128

Índice de tablas

Tabla 1 <i>Objetivos y preguntas</i>	22
Tabla 2 <i>Palabras clave de búsqueda de literatura</i>	43
Tabla 3 <i>Clasificación de los trabajos relacionados</i>	45
Tabla 4 <i>Actividades para la implantación del servicio de firma electrónica</i>	51
Tabla 5 <i>Actividades para el análisis de certificación del servicio de firma electrónica</i> .	101
Tabla 6 <i>Resumen de presupuesto de certificación</i>	105
Tabla 7 <i>Actividades para la evaluación técnico informático del servicio de firma electrónica</i>	106
Tabla 8 <i>Variables de evaluación del servicio de firma electrónica</i>	109
Tabla 9 <i>Matriz de evaluación del servicio de firma electrónica</i>	111
Tabla 10 <i>Actividades del plan de mejora</i>	116
Tabla 11 <i>Matriz de evaluación del plan de mejora para el servicio de firma electrónica</i>	124

Índice de figuras

Figura 1 <i>Firma electrónica: proceso de firma</i>	31
Figura 2 <i>Firma electrónica: proceso de verificación</i>	31
Figura 3 <i>Funcionamiento de una PKI</i>	36
Figura 4 <i>Diseño Jerarquía PKI</i>	53
Figura 5 <i>Arquitectura del servicio de firma electrónica</i>	54
Figura 6 <i>Instalación MariaDB</i>	56
Figura 7 <i>Configuración segura de MariaDB</i>	56
Figura 8 <i>Creación de una base de datos para EJBCA</i>	58
Figura 9 <i>Instalación Docker en CentOS</i>	59
Figura 10 <i>Instalación EJBCA</i>	60
Figura 11 <i>Servicio EJBCA ejecutándose</i>	60
Figura 12 <i>Página de bienvenida EJBCA</i>	60
Figura 13 <i>Creando perfil de certificado para Autoridad Certificadora Raíz</i>	62
Figura 14 <i>Configurando perfil de certificado para Autoridad Certificadora Raíz</i>	62
Figura 15 <i>Creando token criptográfico para Autoridad Certificadora Raíz</i>	64
Figura 16 <i>Configuración del token criptográfico para la Autoridad Certificadora Raíz</i> ..65	65
Figura 17 <i>Creación de la Autoridad Certificadora Raíz</i>	65
Figura 18 <i>Configuración de la Autoridad Certificadora Raíz</i>	66
Figura 19 <i>Creando perfil de certificado para Autoridad Certificadora Subdelegada</i>	68
Figura 20 <i>Configurando perfil de certificado para Autoridad Certificadora Subdelegada</i>	68
Figura 21 <i>Creando token criptográfico para Autoridad Certificadora Subdelegada</i>	70
Figura 22 <i>Configuración del token criptográfico para la Autoridad Certificadora Subdelegada</i>	70
Figura 23 <i>Creación de la Autoridad Certificadora Subdelegada</i>	71

Figura 24 Configuración de la Autoridad Certificadora Subdelegada	71
Figura 25 Creación de perfil de certificado para Entidad Final Superadministrador	73
Figura 26 Configuración de perfil de certificado para Entidad Final Superadministrador	73
.....	
Figura 27 Creación Entidad Final Superadministrador	75
Figura 28 Configuración de Entidad Final Superadministrador	75
Figura 29 Creación de perfil de certificado para Entidad Final Autoridad Registro	77
Figura 30 Configuración de perfil de certificado para Entidad Final Autoridad Registro	77
.....	
Figura 31 Creación Entidad Final Autoridad Registro	79
Figura 32 Configuración de Entidad Final Autoridad Registro	79
Figura 33 Creación de perfil de certificado para Entidad Final Estudiante	81
Figura 34 Configuración de perfil de certificado para Entidad Final Estudiante	81
Figura 35 Creación Entidad Final Estudiante	83
Figura 36 Configuración de Entidad Final Estudiante	83
Figura 37 Creación de Certificado Digital Superadministrador	85
Figura 38 Solicitud Certificado Digital Superadministrador	85
Figura 39 Descarga Certificado Digital Superadministrador	86
Figura 40 Selección de ubicación del almacen a instalar el certificado	87
Figura 41 Selección del certificado a instalar	87
Figura 42 Verificación de contraseña del servidor	88
Figura 43 Selección automática del almacén donde se instalará el certificado	88
Figura 44 Finalizando la instalación del certificado	89
Figura 45 Autenticación Superadministrador	89
Figura 46 Verificando autenticación	90

Figura 47 <i>Agregando el usuario al grupo de miembros de usuarios</i>	
<i>Superadministradores</i>	90
Figura 48 <i>Eliminando el miembro de acceso público del grupo de</i>	
<i>Superadministradores</i>	91
Figura 49 <i>Eliminando rol de acceso público</i>	91
Figura 50 <i>Descarga Certificado Digital Autoridad Registro</i>	92
Figura 51 <i>Creación Autoridad Registro Rol</i>	92
Figura 52 <i>Agregando usuario al grupo de miembro del Rol Autoridad Registro</i>	93
Figura 53 <i>Configuración de reglas de acceso para el Rol Autoridad Registro</i>	93
Figura 54 <i>Creación Estudiante Rol</i>	94
Figura 55 <i>Configuración de miembros para el Rol Estudiante</i>	95
Figura 56 <i>Configuración reglas de acceso del Rol Estudiante</i>	95
Figura 57 <i>Creación Perfil Aprobación Estudiante</i>	97
Figura 58 <i>Configuración Perfil Aprobación Estudiante</i>	97
Figura 59 <i>Asignación del Perfil Aprobación Estudiante al Perfil de Certificado</i>	
<i>Estudiante</i>	99
Figura 60 <i>Jerarquía PKI mejorada</i>	119
Figura 61 <i>Arquitectura del servicio mejorada</i>	120

Resumen

Este trabajo de investigación aborda la implementación y certificación de un servicio de firma electrónica para la Universidad de las Fuerzas Armadas ESPE sede Latacunga. Teniendo como referencia el proyecto de investigación “Transición, operación y mejora del servicio de firma electrónica del ESPE-CERT en el Departamento de Ciencias de la Computación utilizando ITIL V4”, se realizó una implementación mejorada del servicio en los laboratorios del ESPE CERT del DCCO sede Sangolquí, para que pueda ser usado por la comunidad universitaria de esta sede y la sede Latacunga. En esta nueva implementación se consideraron aspectos técnicos que deben tenerse en cuenta para certificar el servicio, acorde a lo establecido en los requerimientos de certificación especificados por la ARCOTEL.

Se ha realizado un análisis de certificación, en el que se determinó los requerimientos económicos, legales y técnicos necesarios para poder certificar el servicio de firma electrónica con el organismo de control gubernamental correspondiente. Con estos requerimientos se evaluó de forma técnica e informática el servicio implantado, identificando áreas de mejora en la seguridad y distribución de los servicios, requiriendo una mayor asignación de recursos e infraestructura de TI. Estos hallazgos resaltan la importancia de continuar desarrollando el servicio de firma electrónica para brindar una solución confiable y segura a la comunidad universitaria.

A través de esta evaluación, se realizó un plan de mejora en el que se propone acciones y recomendaciones, para que el servicio cumpla con los requisitos técnicos de certificación.

Palabras clave: Infraestructura de clave pública, firma electrónica, certificado digital, certificación, software libre.

Abstract

This research work addresses the implementation and certification of an electronic signature service for the University of the Armed Forces ESPE, Latacunga campus. Taking as reference the research project "Transition, operation, and improvement of the electronic signature service of ESPE-CERT in the Department of Computer Science using ITIL V4," an enhanced implementation of the service was carried out in the ESPE CERT labs at the DCCO, Sangolquí campus, to be used by the university community at this campus and the Latacunga campus. This new implementation considered technical aspects that must be taken into account for service certification, following the certification requirements specified by ARCOTEL. A certification analysis was conducted, determining the economic, legal, and technical requirements necessary to certify the electronic signature service with the corresponding government regulatory body. Based on these requirements, a technical and computer evaluation of the implemented service was performed, identifying areas for improvement in security and service distribution, requiring a greater allocation of resources and IT infrastructure. These findings underscore the importance of continuing to develop the electronic signature service to provide a reliable and secure solution to the university community. Through this evaluation, an improvement plan was developed that proposes actions and recommendations to ensure the service meets the technical certification requirements.

Key words: Public key infrastructure, electronic signature, digital certificate, certification, software open source.

Capítulo I

Introducción

En la era digital actual, la tecnología ha revolucionado prácticamente todos los aspectos de nuestras vidas, incluida la forma en que manejamos y procesamos la información. En este contexto, uno de los campos que ha experimentado un cambio significativo, es el ámbito de la firma de documentos de manera tradicional, es decir en papel, a través de la firma manuscrita. Frente a esto ha surgido la firma electrónica, como una alternativa para la firma de documentos de manera digital, que brinda numerosos beneficios en términos de agilidad, seguridad y sustentabilidad.

El presente trabajo se centra en la implantación de un servicio de firma electrónica para la Universidad de las Fuerzas Armadas ESPE – Sede Latacunga, contemplando todas las fases de implantación del servicio. A su vez se investigará y se realizará los procesos necesarios para acreditar a la Universidad de las Fuerzas Armadas ESPE como una Entidad de Certificación. La adopción de esta tecnología permitirá a la institución y diferentes sedes, dar un paso hacia la modernización y la eficiencia en la gestión de documentos, agilizando los procesos administrativos y mejorando la experiencia de todos los miembros de la comunidad universitaria.

Mediante un análisis exhaustivo de las herramientas y tecnologías disponibles para la implementación del servicio de firma electrónica, así como de los procesos necesarios para la acreditación, se buscará establecer un marco sólido que garantice la eficiencia y seguridad en la gestión documental de la comunidad universitaria. Se espera que los resultados de esta investigación no solo beneficien a la sede Latacunga, sino que también sienten las bases para la expansión del servicio a las diferentes sedes de la Universidad de las Fuerzas Armadas ESPE, mejorando así la eficiencia y la seguridad en todas las áreas de la institución.

Planteamiento del problema

Actualmente, la firma manuscrita en la Universidad de las Fuerzas Armadas ESPE, es uno de los medios más utilizados por la comunidad universitaria, particularmente por los estudiantes, para vincular legalmente un documento con un estudiante en concreto. Este método presenta algunas falencias como la falsificación de firmas y dificultad para verificarlas.

Además, los procesos de gestión para la firma de documentos en papel implican un uso considerable de recursos y tiempo, además de presentar posibles riesgos de pérdida, alteración o extravío de la documentación.

La falta de un servicio de firma electrónica en la Universidad, implica una dependencia excesiva del formato en papel, lo que dificulta la eficiencia y agilidad en la gestión documental, así como la posibilidad de acceder y compartir información de manera rápida y segura entre los diferentes actores de la comunidad universitaria.

Asimismo, la ausencia de una acreditación por parte del organismo de control correspondiente, limita la validez legal de las firmas electrónicas y su uso en el ámbito universitario. Esto puede generar desconfianza por parte de los usuarios y puede suponer un obstáculo en los procesos administrativos y la validez jurídica de los documentos emitidos y firmados electrónicamente.

Justificación

Adoptar un servicio de firma electrónica permitirá que la gestión de documentos en los procesos administrativos, se pueda realizar de manera digital, mejorando así la eficiencia y agilidad de los mismos, generando un impacto positivo en términos de reducción de tiempos y costos relacionados a la gestión documental en papel, como lo son el transporte y almacenamiento físico de documentos.

En términos de seguridad, la firma electrónica es un gran aliado, puesto que brinda un alto nivel de seguridad en la gestión de documentos. La utilización de técnicas criptográficas,

garantiza la integridad de un documento y la autenticidad de las firmas, teniendo como resultado documentos inalterables y fuera de objeto de fraude.

La acreditación del servicio por parte del organismo de control, les otorga el respaldo legal y su validez jurídica correspondiente a las firmas electrónicas, y documentos emitidos electrónicamente dentro de la Universidad. Además, permite que la firma electrónica pueda usarse para realizar trámites dentro y fuera del ámbito universitario.

Objetivos

Objetivo general

Implantar el Servicio de Firma Electrónica para la Universidad de las Fuerzas Armadas ESPE, sede Latacunga, en la comunidad conformada por docentes, estudiantes y personal administrativo de la Sede, realizar los procesos necesarios para obtener la certificación por parte del organismo de control para estar en capacidad de ampliar el servicio a las diferentes sedes de la Universidad.

Objetivos específicos

- Establecer el estado del Arte
- Implantar el Servicio de firma electrónica en la Sede Latacunga de la ESPE, utilizando ITIL V4.
- Determinar los requisitos técnico-legales para la certificación del Servicio de firma digital con las características diseñadas e implantado en el ESPE-CERT para la comunidad de la ESPE sede Latacunga.
- Evaluación técnico informática de pre certificación del servicio de firma digital para la ESPE sede Latacunga.
- Mejora del Servicio y resolución de las no conformidades.

Alcance

Realizar una instalación mejorada del servicio de firma electrónica, actualmente implantado en el ESPE CERT del Departamento de Ciencias de la Computación de la sede Sangolquí, de manera que se pueda prestar el servicio para la comunidad universitaria de esta sede, así como la sede Latacunga. Determinar los requisitos, procesos y estándares necesarios para obtener la acreditación como Entidad de Certificación por parte del organismo de control correspondiente. Realizar un análisis de certificación, que permita demostrar si la Universidad de las Fuerzas Armadas ESPE está en capacidad de obtener una acreditación como Entidad Certificadora.

En base a los objetivos específicos planteados se establecerá el estado del arte necesario para crear una base sólida de conocimiento y de esa forma, implementar y administrar un servicio de Firma Electrónica, teniendo en cuenta aspectos técnicos, legales y de infraestructura necesarios para garantizar la interoperabilidad y la uniformidad del servicio, de tal forma que se pueda estar en capacidad de extender el servicio en todas las sedes de la ESPE. Posteriormente, realizar una evaluación y mejora del servicio de Firma Electrónica en base a observaciones y recomendaciones del mismo.

Para la nueva instalación del servicio, se utilizarán los recursos de infraestructura disponibles en el laboratorio H402 del Departamento de Ciencias de la Computación. Los recursos de software requeridos para realizar la implementación del servicio, es de código abierto, por lo que no se requiere de una inversión económica por parte de la institución. Como resultado de este trabajo, se espera que la comunidad universitaria de la sede Sangolquí y Latacunga, tengan un certificado digital que les permita firmar y legalizar documentos de manera digital.

El desarrollo de la investigación tiene como guía responder a los objetivos planteados, por lo que se elabora las siguientes preguntas de investigación, que ayudarán a la recopilación de información necesaria para llevar a cabo esta investigación.

Tabla 1*Objetivos y preguntas*

Objetivo específico	Pregunta de investigación
Establecer el estado del Arte	¿Cuál es el impacto implementar un servicio de firma electrónica para la ESPE sede Latacunga? ¿Cómo se realizará la implementación del servicio de firma electrónica? ¿Qué principios de ITIL V4 deben utilizarse para poder implementar un servicio de firma electrónica?
Implantar el Servicio de firma electrónica en la Sede Latacunga de la ESPE, utilizando ITIL V4.	¿Cuáles son los pasos y procesos requeridos para implementar el servicio de firma electrónica utilizando la metodología ITIL V4 en la Universidad de las Fuerzas Armadas ESPE, sede Latacunga? ¿Cuáles son los requisitos técnicos-legales específicos que deben cumplirse para obtener la certificación del servicio de firma electrónica?
Determinar los requisitos técnico-legales para la certificación del Servicio de firma digital con las características diseñadas e implantado en el ESPE-CERT para la comunidad de la ESPE sede Latacunga.	¿Cuáles son los marcos normativos y regulaciones legales relevantes que deben considerarse para la certificación del servicio de firma electrónica?
Evaluación técnico informática de pre certificación del servicio de firma digital para	¿Cuáles son los criterios de evaluación técnica e informática necesarios para evaluar la

Objetivo específico	Pregunta de investigación
<p>la ESPE sede Latacunga.</p> <p>Mejora del Servicio y resolución de las no conformidades.</p>	<p>funcionalidad del servicio de firma electrónica antes de su certificación?</p> <p>¿Cuáles son las mejoras y ajustes necesarios identificados durante la evaluación técnico informática del servicio de firma electrónica en la ESPE sede Latacunga?</p> <p>¿Cuáles son las principales áreas de mejora identificadas y las no conformidades detectadas en el servicio de firma electrónica en la ESPE sede Latacunga?</p> <p>¿Cuál es el impacto de las mejoras implementadas en el servicio de firma electrónica en la comunidad de la ESPE sede Latacunga?</p>

Hipótesis

La implementación del servicio de Firma Electrónica en la Universidad de las Fuerzas Armadas ESPE, sede Latacunga, y la obtención de la acreditación como Entidad de Certificación, mejorará la eficiencia, seguridad y confiabilidad de los procesos administrativos, proporcionando una solución ágil y legalmente válida para la firma y legalización de documentos digitales. Esto conducirá a una mayor adopción y aceptación del servicio por parte de la comunidad universitaria, abriendo la posibilidad de poder extender el servicio a las diferentes sedes de la institución, mejorando la experiencia de los usuarios y optimizando la gestión de documentos en la institución.

Metodología

Design Science Research (DSR), es la metodología escogida para el desarrollo de este proyecto. Se utiliza principalmente en el ámbito de ciencias de la computación y la ingeniería de sistemas de información. Esta metodología tiene como objetivo el diseño y desarrollo de artefactos, entendiéndose por artefactos como sistemas, algoritmos, modelos, etc. (Olsina et al., 2020).

Metodología Science Research

Esta metodología puede variar dependiendo de las necesidades, pero según (Peppers et al., s. f.) quien propone y adecúa esta metodología en el ámbito de los sistemas de información, esta metodología consta de 6 pasos:

- Identificación y justificación del problema
- Objetivos de la solución
- Diseño y desarrollo
- Demostración
- Evaluación
- Comunicación

En el primer y segundo paso se aborda partes esenciales correspondientes al Capítulo I de esta investigación, en las cuales se identifica un problema y se justifica la razón por cuál debe ser resuelto, para posteriormente establecer los objetivos que ayuden a resolver dicho problema. En el tercer paso se realiza un análisis sobre requerimientos técnicos y funcionales necesarios para la implementación del servicio y posteriormente la implementación del mismo.

El cuarto paso corresponde a la realización de pruebas del servicio implementado para demostrar su eficacia y funcionalidad. Con los resultados del cuarto paso, en el quinto paso se evalúa el resultado obtenido de la implementación del servicio, de tal forma que se pueda medir

la eficacia y rendimiento del mismo. Para complementar esto se puede realizar encuestas a los usuarios que utilizaron el servicio para identificar áreas de mejora.

Por último, en el sexto paso se presentan los resultados de la investigación, así como la solución propuesta, dando a conocer su utilidad, rigor e impacto a las audiencias correspondientes.

Capítulo II

Fundamentación teórica

La implementación de un servicio de firma electrónica requiere conocer conceptos relacionados a la misma, como pueden ser criptografía, firmas electrónicas, certificados digitales, infraestructura de clave pública (PKI), tecnologías afines para llevar a cabo la implementación, conocimiento acerca de lo que es ITIL. En lo que respecta la certificación del servicio, es importante conocer el marco legal que se rige a este tipo de servicios, así como también, es necesario conocer los requisitos técnicos, legales y económicos para conseguir la acreditación del servicio. Con todos estos conceptos se puede llegar a consolidar una base de conocimiento y bibliográfica para desarrollar este proyecto.

ITIL

ITIL o por sus siglas en inglés “Information Technology Infrastructure Library”, es una biblioteca de conceptos y mejores prácticas que ayudan a consolidar un servicio de TI de acuerdo a las necesidades del negocio. Con ayuda de esta biblioteca, se garantiza que una organización que depende de las Tecnologías de la Información y Comunicación, para cumplir con sus objetivos corporativos y necesidades de negocios, brinde servicios de calidad a sus clientes (Remache Típan, 2022).

ITIL V4.

Esta versión es la más actual de ITIL, lanzada en el 2019. Apareció como una necesidad de adaptarse a la transformación digital y a la aparición nuevas tecnologías, que han cambiado la manera en la que opera una organización de TI. Esta versión tiene un diseño flexible, ágil y centrado en el usuario; enfocándose en el ciclo de vida del servicio e introduciendo un nuevo concepto como la orientación del servicio hacia el valor (Remache Típan, 2022).

Sistema de valor del servicio (SVS).

El sistema de valor del servicio, es un enfoque holístico, que consiste en hacer que los miembros de una organización en conjunto con las acciones que se realizan, trabajen como una sola estructura para poder crear valor. El SVS se compone de componentes, actividades y prácticas que trabajan juntos para lograr los objetivos y resultados deseados (Montesinos Flores & Jhonatan Rober, 2022).

Los componentes claves del SVS son los siguientes:

- **Gobierno:** Se refiere al conjunto de políticas, roles, responsabilidades y procesos para guiar y controlar el uso efectivo de los recursos de TI y la toma de decisiones estratégicas.
- **Gestión de servicios:** Es el conjunto de capacidades que se enfocan en proporcionar valor a los clientes mediante el diseño, la entrega y la mejora de servicios de calidad.
- **Mejora continua:** Es la capacidad de evaluar y mejorar constantemente el desempeño de los servicios y los procesos, basándose en el aprendizaje y la retroalimentación obtenida a través de la experiencia y la medición de resultados.
- **Prácticas de gestión de servicios:** Son enfoques específicos y recomendaciones para realizar actividades y lograr resultados en la gestión de servicios de TI. ITIL v4 define una serie de prácticas, como gestión de incidentes, gestión de cambios, gestión de problemas, gestión de servicios de TI, entre otras.

Seguridad y criptografía

La necesidad de mantener segura la información ha cambiado en las últimas décadas. Antes de la llegada de las computadoras y la era digital, la seguridad de la información era manejada a través de medios físicos como por ejemplo el uso de cajas fuertes. Con la llegada

de la computadora, se introdujeron nuevos métodos para mantener segura la información de manera digital, como lo son los sistemas criptográficos.

Criptografía.

El término criptografía proviene de un vocablo griego Kriptos, que significa ocultar y Graphos, que significa escritura. En conjunto estos términos darían el significado de ocultar la información, utilizando alguna técnica que permita que un mensaje sea ininteligible. La criptografía es una disciplina que nace de una rama de las matemáticas conocida como “Teoría de la Información”, este término fue acuñado por el matemático Claude Elwood Shannon en 1948. El objetivo principal de esta disciplina es proteger la información mediante el uso de códigos y algoritmos matemáticos.

Cuando hablamos de proteger la información no solo se refiere al hecho de ocultar la información, en este sentido aparecen 3 conceptos claves que se deben tener en cuenta para mantener segura la información, estos conceptos se definen como confidencialidad, integridad y autenticidad. El concepto de confidencialidad se refiere al hecho de que un mensaje sea inteligible únicamente por las partes interesadas, para el resto de personas este mensaje debe estar oculto. Con integridad se pretende que el mensaje no se vea alterado su contenido durante el transporte del mismo y se garantice que su contenido siempre sea el mismo. La autenticidad pretende que se pueda verificar la procedencia del mensaje, que esta sea una fuente confiable. Para lograr esto se hace uso de técnicas como la firma digital, certificados digitales, entre otros.

Métodos de criptografía.

Actualmente existen dos métodos criptográficos modernos: la encriptación de llave privada o criptografía simétrica y encriptación de llave pública o criptografía asimétrica. El término de llave es un concepto que se relaciona a la forma para restringir accesos de manera física usando una cerradura o candado, la cual puede abrirse usando una llave única. Por tanto, en términos de criptografía se entiende por llave como una herramienta digital que sirve

para para bloquear y desbloquear información, esta llave suele ser una cadena de texto con la característica de que debe ser única y confidencial.

Criptografía simétrica.

Este tipo de criptografía hace uso de una sola llave para cifrar y descifrar un mensaje, por ejemplo, si una persona a la que llamaremos Bob, desea compartir un mensaje confidencial con otra persona a la que llamaremos Alice, lo primero que debe hacer Bob es cifrar el mensaje con su llave para posteriormente enviar el mensaje a Alice, pero para que Alice pueda descifrar el mensaje, esta debe conocer la llave de Bob para hacerlo. Este método funciona bien en la mayoría de los casos, pero supone un problema porque en primer lugar Bob debe compartir su llave privada con Alice y, además, si quisiera compartir un mensaje con otras personas debería generar n llaves privadas para cada una de las personas.

Criptografía asimétrica.

Este método hace uso de dos tipos de llaves, una pública y una privada, con la llave privada se cifra el mensaje y con la llave pública se descifra el mensaje, siguiendo el ejemplo anterior, para que Bob comparta un mensaje confidencial con Alice, este debe cifrar el mensaje con su llave privada y enviar el mensaje a Alice, y para que Alice pueda descifrar el mensaje, esta debe conocer la llave pública de Bob, con esto se soluciona el problema de compartir la llave privada para descifrar el mensaje, y además ya no se necesita generar n llaves privadas, en cambio se debe generar n llaves públicas.

Hashing.

El hashing es un método criptográfico que hace uso de funciones hash o funciones de resumen para encriptar un mensaje. Estas funciones hash hacen uso de una llave o secreto para encriptar un mensaje. La particularidad de este método es que solo se realiza en un único camino, es decir, solo se puede encriptar, no se puede desencriptar; además de eso, al encriptar un mensaje, el hash o resumen resultante, siempre es el mismo, sin importar cuantas veces se aplique la función hash al mensaje original.

Este método suele ser habitualmente utilizado para guardar contraseñas en bases de datos y actualmente, ha ganado mucha popularidad dentro de la tecnología blockchain, debido a las características mencionadas.

Firma electrónica

La firma electrónica está conformada por un conjunto de datos, tales como información personal acerca del firmante y otros aspectos técnicos definidos en su creación, los cuales sirven como un medio para identificar al firmante, otorgando el mismo valor que tiene la firma manuscrita. (ELECTRÓNICA, F. (2014). Firma electrónica.).

Para poder realizar la firma electrónica, se debe obtener un certificado digital, que no es más que un documento digital, que contiene información personal de una persona y que ayuda a identificar al mismo. Este documento es otorgado por una Autoridad Certificadora y es esta quien se encarga de validar y verificar los datos personales, y con ello certificar a esta persona, para que pueda realizar la firma electrónica.

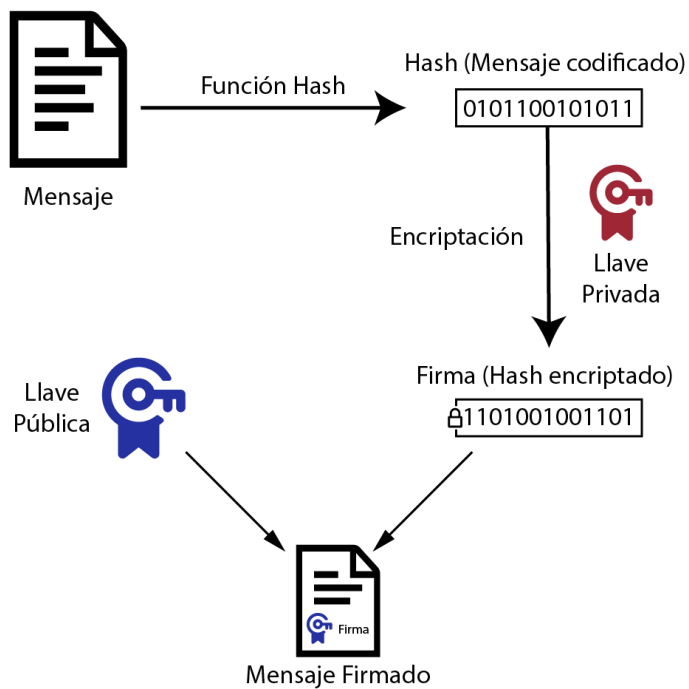
La firma electrónica a través de un conjunto de tecnologías, se crea una herramienta tecnológica que permite garantizar la autenticidad, integridad y no repudio de mensaje de datos por medio de los canales digitales de comunicación. Cuando una persona hace uso de la firma electrónica para firmar un documento, los datos de esta persona, como su identificación, correo, etc, se incrustan en dicho documento; con esto, el firmante de cierta forma, está aprobando y reconociendo el contenido del documento. De esta forma, cualquier persona que reciba este documento, puede verificar fácilmente su procedencia y su autenticidad, confiando en la información presente de dicho documento.

Funcionamiento de la firma electrónica.

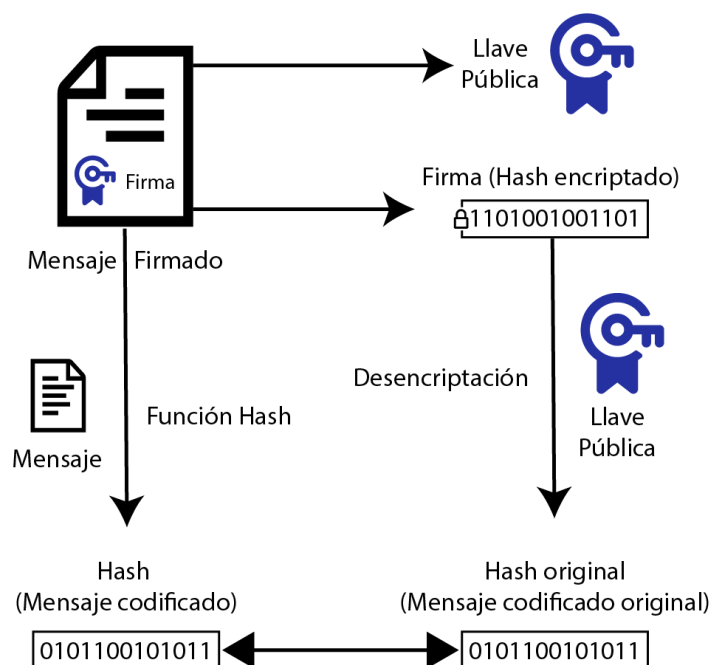
El funcionamiento de la firma electrónica se basa en el uso de técnicas criptográficas asimétricas para vincular digitalmente la identidad de una persona con el contenido de un documento.

Figura 1

Firma electrónica: proceso de firma

**Figura 2**

Firma electrónica: proceso de verificación



El proceso básico de funcionamiento de la firma electrónica se describe a continuación:

- **Firma:** En primer lugar, se crea un hash o resumen del mensaje de datos aplicando funciones de hash. De esto se obtiene un mensaje codificado, conocido como hash resultante o simplemente hash. El hash es encriptado con la llave privada del firmante, de esa manera obtenemos un hash encriptado, que se conoce como la firma. Esta firma se adjunta al mensaje de datos original, junto con la llave pública del firmante, de esta forma se ha firmado de forma electrónica un mensaje de datos.
- **Verificación de la firma:** La persona que recibe el mensaje de datos firmado electrónicamente, extrae de estas tres cosas: el mensaje de datos, la firma y la llave pública del firmante. Para proceder con la verificación, la persona verificadora vuelve a aplicar una función hash al mensaje de datos. Luego, de la firma extraída o el hash encriptado, se desencripta usando la llave pública del firmante, de esa manera se obtiene el hash original que realizó el firmante. Finalmente, la persona verificadora, compara el hash que acaba de crear con el hash que creó el firmante,

si ambos hashes son iguales, se dice que la firma es válida, caso contrario, se rechaza.

Certificado digital

El certificado digital es un tipo de documento digital especial, que se otorga a las personas para que puedan realizar la firma de documentos de forma electrónica. Este documento almacena información personal sobre la persona o titular del certificado.

La firma electrónica se basa en el uso de técnicas criptográficas asimétricas, para lo cual se necesita un par de llaves criptográficas: llave privada y llave pública. Este par de llaves también están contenidas dentro del certificado digital.

Infraestructura de clave pública (PKI)

Una Infraestructura de Clave Pública se basa en el uso de tecnologías de la información y estándares de seguridad, entre otros, para gestionar y administrar el despliegue de certificados digitales, los cuales son utilizados en diferentes ámbitos, siendo uno de ellos, la firma electrónica. La base de una infraestructura de clave pública está definida en la recomendación ITU-T X.509. X.509 es un estándar que define el formato de los certificados digitales emitidos por una PKI. Este estándar es quien define que información debe contener los certificados digitales acerca de la identidad de una persona. También se debe incluir información adicional como el periodo de validez del certificado y el nombre de la autoridad de certificación que lo emitió.

Elementos de una PKI.

Una PKI se compone de los siguientes elementos:

- **Autoridad de Certificación:** Es una entidad encargada de emitir los certificados digitales hacia los usuarios finales.
- **Registro de Claves Públicas:** Es un almacén de claves públicas en donde se guarda las claves públicas de los usuarios.

- **Política de Certificación:** Son un conjunto de reglas definidos por la Autoridad de Certificación que se deben cumplir para administrar los certificados digitales, como pueden ser su emisión, renovación o revocación. En otras palabras, define los requisitos para manejar el ciclo de vida de un certificado.
- **Certificado Digital:** Documento digital que contiene la información necesaria para identificar a una persona. Además, contiene un par de llaves criptográficas. Esta información está definida por el estándar X.509.
- **Infraestructura de Validación:** Es un conjunto de servicios que permiten verificar y validar la autenticidad de los certificados digitales, así como el ciclo de vida de los mismos.

Jerarquía PKI

Una jerarquía de PKI es un sistema organizado de certificados digitales que establece relaciones de confianza entre las entidades que emiten y utilizan los certificados. Al hablar de jerarquía de PKI, se entiende por una organización de múltiples niveles representados por una autoridad de certificación en cada nivel, en otras palabras, es una jerarquía de CA's. Es recomendable usar este tipo de jerarquía para tener un mejor control en la emisión de certificados digitales.

En este contexto, se recomienda usar una jerarquía de al menos dos niveles, conformada por una Autoridad Certificadora Raíz (RootCA) y múltiples Autoridades Certificadoras Subordinadas (SubCA) según sea la necesidad. Con este tipo de jerarquía, una RootCA únicamente emite certificados a SubCA's y las SubCA's se encargarían de emitir certificados únicamente a las entidades finales o crear niveles de SubCA adicionales. Con esto se lograría que el tiempo de validez de la RootCA permanezca por un mayor tiempo o tengan una mayor longevidad, mientras que una SubCA puede tener un tiempo de vida más corta e incluso ser removida. De esta manera se evita la necesidad de actualizar y reemplazar los certificados de RootCA.

Dentro de una jerarquía de PKI aparecen otros conceptos como RA, VA, EE y Auditor, estos conceptos se explican a continuación:

- **Autoridad de Registro (RA):** Puede entenderse como un conjunto de servicios que se utilizar para gestionar el ciclo de vida de los certificados digitales, así como de, el registro de los usuarios, validando previamente su información. En una jerarquía de PKI pueden existir múltiples RA's según sea la necesidad.
- **Autoridad de Validación (VA):** Es una entidad que se encarga de verificar y validar los certificados digitales existentes en el repositorio de certificados, es decir se encarga de validar si un certificado se encuentra en vigencia o si ha sido revocado, entre otras acciones.
- **Auditor:** Esta entidad se encarga únicamente de revisar los logs del sistema.
- **Entidad Final (EE):** Esta entidad puede referirse a una persona o usuario que está solicitando un certificado digital, pero en otros escenarios puede referirse también a dispositivos como un servidor.

La Autoridad de Validación, a su vez se conforma por un par de servicios que sirven para verificar la validez de un certificado digital, los cuales se describen a continuación.

- **CRL:** Por sus siglas en inglés, significa Lista de Certificados Revocados. Este es un archivo que contiene los ID's de todos aquellos certificados que han sido revocados. Para obtener este archivo se configura un endpoint a través del cual descargarlo, en la Autoridad de Certificación. Este endpoint es utilizado por la Autoridad de Validación. El problema de esto, es que este archivo puede ir aumentando de tamaño considerablemente según se revoquen certificados digitales, por ello, se configura el siguiente servicio.
- **OCSP:** Es un Protocolo de Verificación de Certificados en línea, según sus siglas en inglés. Igualmente es un endpoint que se configura en la Autoridad de Certificación

para que pueda ser utilizado en la Autoridad de Validación. A diferencia del CRL, este endpoint sirve para consultar por un único ID de certificado a la vez, sin tener que descargar toda la lista de certificados revocados.

Arquitecturas de PKI

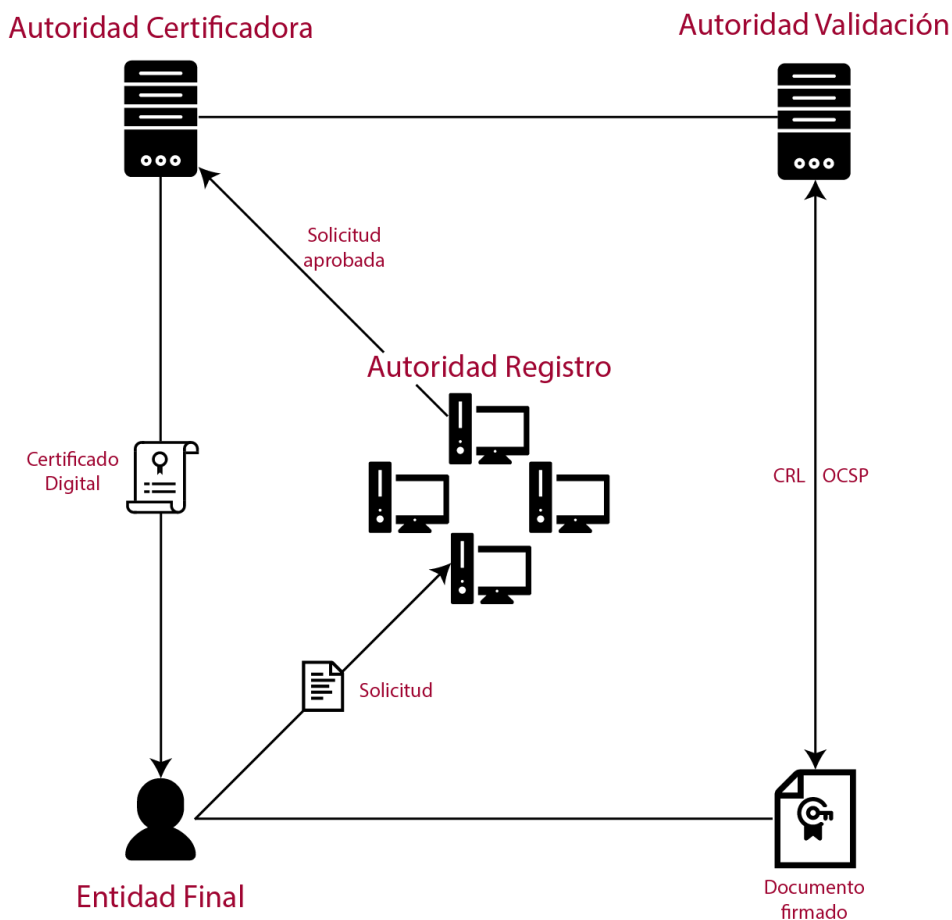
Cuando hablamos de arquitecturas de infraestructura de clave pública, se refiere a como se puede implementar y diseñar una jerarquía de PKI.

- **Arquitectura Simple:** Se refiere a una PKI implementada en un mismo servidor. Este tipo de arquitectura es de las más sencillas de implementar, donde toda la jerarquía de PKI se encuentra alojada en un simple servidor. Sin embargo, en términos de eficiencia no suele ser lo mejor puesto que puede sobrecargar el servidor.
- **Arquitectura Distribuida:** Este tipo de arquitectura se refiere a la implementación de una jerarquía de PKI en múltiples servidores, por ejemplo, el RootCA y una SubCA en un mismo servidor y diferentes RA's y VA's en múltiples servidores.
- **Arquitectura Híbrida:** Los dos tipos de arquitecturas anteriores se conocen como un tipo de arquitectura privada, ya que todo se encuentra implementado dentro de la organización. Una arquitectura híbrida se refiere a implementar una PKI tanto local o dentro de la organización y en la nube. Por ejemplo, se puede tener a las CA's más sensibles como RootCA en las instalaciones de la organización y las RA's en la nube.

Funcionamiento de una PKI

Figura 3

Funcionamiento de una PKI



El funcionamiento de una PKI involucra la interacción de todas las componentes mencionadas anteriormente. En primer lugar, una entidad final realiza una solicitud para obtener su certificado digital a la autoridad de registro, para lo cual proporciona información personal como sus nombres completos, email, teléfono, entre otros. La autoridad de registro revisa la solicitud y valida los datos proporcionados por la entidad final. Si la solicitud es correcta, se notifica a la autoridad certificadora que emita un nuevo certificado digital hacia la entidad final.

Luego, cuando la entidad final hace uso del certificado digital para firmar un documento, la persona que reciba este documento firmado y abra este documento a través de un software especial, como Adobe Reader, al abrir el documento este se emite una solicitud hacia la autoridad de validación para verificar si el certificado digital con el que se ha firmado sigue

siendo válido o no ha sido revocado. Esta verificación se realiza a través de los servicios CRL y OCSP.

Tecnologías para la implementación de una PKI

Cuando hablamos de tecnologías para implementar una PKI, nos referimos al uso de herramientas de software que nos permitan cumplir con el objetivo. Implementar este tipo de servicios no requiere de una excesiva recopilación de software, existen proyectos o frameworks ya desarrollados que nos permiten implementar este tipo de servicio, como pueden ser PGP, OPENCA, EJBCA, XCA.

Cada una de estas herramientas tiene sus ventajas y desventajas, pero según (Carrera López & Celi Jiménez, 2022) quienes realizaron un análisis sobre las funcionalidades y características de las herramientas mencionadas, destacan principalmente OPENCA y EJBCA como principales alternativas para la implementación de este tipo de servicio, siendo EJBCA la favorita por tener una versión de código abierto y tener más características a las que da soporte.

Si bien esta herramienta nos ofrece todo lo necesario para implementar una PKI, existen otras herramientas que nos pueden ayudar en el proceso, como pueden ser un motor base de datos para lograr la persistencia de la información generada en tiempo de ejecución y tecnologías de virtualización que nos permitan tener un mejor control sobre el ambiente de ejecución. En este ámbito se puede mencionar a MariaDB como motor de base de datos, y Docker, como tecnología de virtualización.

EJBCA.

Enterprise Java Bean Certificate Authority, es una de las plataformas de infraestructura de clave pública (PKI) más populares en el mundo. Incluye todos los componentes necesarios de una PKI, como la Autoridad de certificación (CA), la Autoridad de registro (RA) y la Autoridad de validación (RA) (*About EJBCA@*, s. f.).

EJBCA es un proyecto de código abierto patrocinado por Keyfactor y está disponible bajo la licencia LGPL v2.1. Esto significa que está disponible para su descarga y uso sin costo alguno (*About EJBCA®*, s. f.).

EJBCA es independiente de la plataforma y proporciona flexibilidad y escalabilidad para admitir casi cualquier caso de uso de PKI, incluidos DevOps, Internet of Things (IoT), Industrial IoT, Enterprise PKI y más. Además de integraciones sin interrupciones en sistemas de terceros para la automatización completa y la facilidad de operación. Soporta múltiples usuarios y puede alojar múltiples CA y PKI en una sola instalación del servidor (*About EJBCA®*, s. f.).

Docker.

Docker es una tecnología de virtualización a nivel de sistema operativo, es decir es un hipervisor tipo 2, gracias a esto nos permite crear aplicaciones muy ligeras y portátiles. Esto se debe a que comparte los recursos del anfitrión, a diferencia de los hipervisores tipo 1, que segmentan los recursos del anfitrión, de esta forma, al virtualizar una aplicación se aprovecha de una manera más eficiente los recursos proporcionados para esa aplicación.

Docker se basa en el concepto de “contenedores” para crear aplicaciones. Un contenedor es un conjunto de elementos de software necesarios para crear un ambiente ejecución completo, para correr una aplicación, independientemente del sistema operativo anfitrión.

MariaDB.

MariaDB, una base de datos desarrollada por la comunidad de MySQL, con la diferencia de que es de código abierto, con una licencia GPL v2. Se dice que es una versión mejorada de MySQL, otorgando mayores funcionalidades que mejoran la escalabilidad y rendimiento de las bases de datos al realizar consultas SQL.

Marco legal

Acercas de las normas y políticas que se rigen al comercio electrónico, las firmas digitales y los certificados digitales, es importante estar familiarizado y cumplir con un marco

legal y regulador. En la legislación ecuatoriana existen varios proyectos que resaltan la importancia de las políticas y procedimientos en las transacciones a nivel electrónico.

Ley de comercio electrónico, Firmas y Mensajes de datos.

La Ley de Comercio Electrónico, Firmas y Mensajes de Datos del Ecuador, también conocida como la Ley de Comercio Electrónico (LEC), es una legislación que regula las transacciones comerciales realizadas a través de medios electrónicos en el país. Fue aprobada el 10 de abril de 2002 y ha sido actualizada desde entonces para adaptarse al desarrollo tecnológico.

El objetivo principal de esta ley es establecer un marco legal que promueva y regule el uso del comercio electrónico, las firmas digitales y los mensajes de datos, con el fin de facilitar las transacciones electrónicas y brindar seguridad y confianza a los participantes en dichas transacciones.

Capítulo I: De las firmas electrónicas.

Este capítulo provee de conceptos y normas relacionadas a la firma electrónica tales como su significado, importancia, requisitos para su obtención y obligaciones respecto a su uso. A continuación, se resume los artículos relacionados presentes en este capítulo.

El artículo 13 define el concepto sobre lo que es la firma electrónica y cuál es su propósito, el cual tiene por objeto, identificar al firmante y aprobar el contenido de un documento. El artículo 14 establece que la firma electrónica tiene la misma validez jurídica que la firma manuscrita. El artículo 15 detalla los requisitos legales que debe presentar una persona para poder obtener la firma electrónica, como, por ejemplo, documentos que respalden su identificación y que permitan confiar en quien el sujeto dice ser. El artículo 16 establece que la firma debe adherirse al documento, como signo de que el firmante valida la información de dicho documento. El artículo 17 enumera las obligaciones que tiene el titular de la firma electrónica para garantizar su seguridad y control. El artículo 18 establece que las firmas electrónicas tienen duración indefinida y pueden revocarse según las regulaciones. Por último,

el artículo 19 enumera las razones válidas para extinguir una firma electrónica, incluyendo la voluntad del titular y eventos como fallecimiento o disolución de la entidad titular.

Capítulo II: De los certificados de firma electrónica.

Este capítulo provee de conceptos y normas relacionadas a los certificados electrónicos tales como su significado, importancia, requisitos para su obtención y obligaciones respecto a su uso. A continuación, se resume los artículos relacionados presentes en este capítulo.

El artículo 20 define el concepto sobre lo que es un certificado electrónico, el cual menciona que es un documento digital que contiene información sobre una persona o titular. El artículo 21 especifica que el certificado se utiliza para certificar la identidad del titular de una firma electrónica y otros fines según la ley y sus regulaciones. El artículo 22 detalla los requisitos para que un certificado sea válido, incluyendo la identificación de la entidad emisora, datos del titular, método de verificación, fechas de emisión y expiración, entre otros. El artículo 23 establece que la duración del certificado se determina según los reglamentos internos de la entidad emisora. El artículo 24 enumera las razones para extinguir un certificado, como la solicitud del titular o la expiración. También considera casos fortuitos como fallecimiento o desaparición del titular. El artículo 25 menciona los casos en los que un certificado puede ser suspendido temporalmente, como por falsedad en los datos del titular o incumplimiento contractual. Finalmente, el artículo 26 enumera las razones para revocar un certificado, como el cese de actividades de la entidad emisora o su quiebra técnica.

Capítulo III: De las entidades de certificación de información.

Este capítulo contiene conceptos y normas relacionados con los temas de certificación de información, su significado, requisitos para su obtención y responsabilidades relacionadas con sus funciones. A continuación, se presenta un resumen de los artículos relevantes de este capítulo.

El artículo 29 establece que las agencias de certificación se refieren a instituciones autorizadas por el Consejo Nacional de Telecomunicaciones para emitir certificados de firma electrónica y prestar servicios relacionados. El artículo 30 establece los requisitos que deben cumplir estas entidades, entre ellos registro legal, acreditación de solvencia técnica y financiera, garantizar la confidencialidad y seguridad en la prestación del servicio, mantener copias de seguridad de la información, suspensión o revocación de certificados por orden de la Autoridad Reguladora de Telecomunicaciones, publicación del estado de los certificados emitidos, proporcionando formas de informar riesgos de abuso y proporcionando garantías de responsabilidad. El artículo 31 define la responsabilidad de los organismos de certificación por los daños causados por el incumplimiento de la ley o el uso inadecuado de los certificados, incluida la responsabilidad de los organismos de certificación si la garantía no cubre completamente el daño. El artículo 32 enfatiza la obligación de proteger los datos personales obtenidos durante las actividades de certificación. El artículo 33 permite a terceros gestionar total o parcialmente los servicios de certificación, siempre que tengan relación con el organismo de certificación. El artículo 34 prevé la rescisión del contrato entre el organismo de certificación y sus suscriptores de conformidad con la ley sobre organización de la protección de los derechos del consumidor. Finalmente, el artículo 35 impone la obligación de notificar al organismo de control con al menos 90 días de antelación si el organismo certificado deja de funcionar.

Estado del Arte

En esta sección se examinará estudios previos, investigaciones y teorías relevantes relacionados con el tema en cuestión, para establecer un marco de referencia necesario para el desarrollo de la investigación propuesta. Se realizará una búsqueda respecto a la firma electrónica y su implementación en organizaciones educativas, enfocándose en los procedimientos legales de certificación o acreditación, para que una institución pueda ser reconocida como entidad certificadora de información. Para esto se tomará en cuenta las fases

de descripción de las preguntas de investigación, inspección de los objetivos, manejo de la búsqueda, exposición de la información y clasificación de los trabajos más importantes.

Planteamiento de la revisión de literatura preliminar

La finalidad que tiene realizar la revisión de la literatura, es establecer las variables adecuadas para realizar el estado del arte, para este proceso se establecen las siguientes etapas: formular la pregunta de investigación, definir la estrategia de búsqueda y finalmente la selección de los trabajos relacionados.

Preguntas de investigación.

Teniendo en cuenta que el objetivo de esta investigación es la implementación de un servicio de firma electrónica y la acreditación por parte del organismo de control correspondiente para que la institución sea reconocida como una entidad certificadora, se plantea la siguiente pregunta de investigación: ¿Cuál es el impacto de implantar un servicio de firma electrónica, legalmente constituido y acreditado, para la gestión documental en instituciones educativas de nivel universitario, en términos de agilidad y seguridad para la firma de documentos digitales?

Estrategia de búsqueda.

Para la búsqueda de trabajos relacionados se utilizó el repositorio digital de Google, llamado Google Scholar. Para filtrar los estudios se utilizó el siguiente parámetro de búsqueda: (firma electrónica OR firma digital) AND (infraestructura de clave pública) AND (acreditación OR certificación) AND (entidad de certificación OR entidad certificadora) AND (implementación OR despliegue).

Tabla 2

Palabras clave de búsqueda de literatura

Concepto	Términos alternativos	Conector
implementación	(implementación OR despliegue)	AND

Concepto	Términos alternativos	Conector
infraestructura de clave pública	(infraestructura de clave pública)	AND
firma electrónica	(firma electrónica OR firma digital)	AND
acreditación	(acreditación OR certificación)	AND
entidad de certificación	(entidad de certificación OR entidad certificadora)	

Selección de trabajos relacionados.

De la búsqueda realizada en el repositorio de Google Scholar, se obtuvo un total de 16900 resultados. Para evaluar y filtrar de mejor manera estos resultados como válidos, se tomó en cuenta el título del trabajo y el resumen del mismo. Además, se aplicaron los siguientes criterios de inclusión:

- Incluye una metodología de implementación de un servicio de firma electrónica.
- Incluye una metodología de acreditación de la institución como entidad certificadora.
- Incluye resultados del proceso de acreditación para entidad de certificación.
- Incluye o presenta la elaboración de la documentación de los requisitos necesarios para la acreditación.
- Incluye resultados del uso del servicio de firma electrónica.
- El artículo está publicado entre 2018-2023.
- Artículos en idioma español e inglés.

Evaluación de la calidad.

Para evaluar la calidad de los trabajos seleccionados, se aplicó el siguiente cuestionario de cuatro preguntas de carácter cerrado (preguntas de si o no):

- El trabajo muestra la implementación de un servicio de firma electrónica.
- El trabajo muestra el proceso de acreditación para entidad de certificación.

- El trabajo muestra la elaboración de la documentación de los requisitos para la acreditación.
- El trabajo realiza la implementación del servicio de firma electrónica con software libre.
- El trabajo realiza la implementación en una institución educativa.
- El trabajo realiza el proceso de acreditación en una institución educativa.

Para poder considerar un trabajo relacionado, este debe responder de manera afirmativa con tres de las seis preguntas planteadas.

Estrategia de extracción de datos.

De acuerdo a la pregunta de investigación planteada, se pretende encontrar posibles respuestas a la misma, tratando de conseguir un criterio en común de todos los trabajos seleccionados.

Pregunta de investigación: ¿Cuál es el impacto de implantar un servicio de firma electrónica, legalmente constituido y acreditado, para la gestión documental en instituciones educativas de nivel universitario, en términos de agilidad y seguridad para la firma de documentos digitales?

Tabla 3

Clasificación de los trabajos relacionados

Opción	Descripción
Positiva	La implementación de un servicio de firma electrónica legalmente constituido y acreditado, muestra un impacto positivo en la gestión documental de instituciones educativas de nivel universitario en términos de agilidad y seguridad para firma de documentos digitales.
Incierta	No se muestran resultados de la implementación de un

Opción	Descripción
Negativa	<p data-bbox="678 252 1325 357">servicio firma electrónica legalmente constituido y acreditado.</p> <p data-bbox="630 394 1377 693">La implementación de un servicio de firma electrónica legalmente constituido y acreditado, no soluciona problemas en la gestión documental de instituciones educativas de nivel universitario en términos de agilidad y seguridad para firma de documentos digitales.</p>

Métodos de síntesis.

Para establecer la calidad de los resultados obtenidos se implementa datos cuantitativos para la cantidad de trabajos relacionados y datos cualitativos para su contenido.

Etapas de conducción.

Después de aplicar la estrategia de búsqueda, se pudo encontrar 20 trabajos relacionados de gran aporte, de los cuales, después de una revisión, se seleccionó 5 de ellos.

Resumen de los trabajos relacionados.

Implementación de la plataforma de firma digital para el proceso de emisión de documentos académicos en la Universidad Nacional de Barranca (Ampuero Herrera, 2021).

Este trabajo realiza la implementación de una plataforma de firma digital en la Universidad Nacional de Barranca, para optimizar el proceso de emisión de documentos académicos. Primero realiza una investigación sobre cuál es el proceso actual para emitir un documento académico como un record académico, para lo cual describe un proceso manual y presencial, que involucra más de una parte para legalizar este documento, donde se requiere la firma manuscrita de cada una de ellas. Luego de realizar la implementación de la firma digital y realizar encuestas acerca del mismo, establece que la firma digital tiene un impacto positivo en

el proceso de emisión de documentos académicos, mejorando significativamente la optimización de estos procesos.

Desarrollo e implementación de una aplicación web con firma electrónica y certificado digital, para mejorar la gestión de notas de los estudiantes del SENATI ZONAL LORETO 2019 (Vela Gonzales & Macedo Rojas, 2020).

En esta investigación se implementa un servicio de firma electrónica con el propósito de validar y asegurar el registro de notas en un sistema ERP. Este trabajo le da un principal enfoque a la seguridad que ofrece la firma electrónica para garantizar la seguridad de un documento a través de los medios digitales. Como resultado, demuestra a través de encuestas realizadas, que implementar la firma digital para el registro de notas en el ERP de la institución proporciona un alto nivel de seguridad a este proceso realizado por docentes.

Implementación de una PKI no acreditada utilizando estándares internacionales para garantizar la integridad de los documentos firmados digitalmente (Carrera López & Celi Jiménez, 2022).

Este trabajo realiza una investigación acerca de las tecnologías disponibles para implementar una PKI; tras una comparación de las mismas, se selecciona la que se considera más completa para implementar una PKI y realiza una implementación de la misma, usando la herramienta seleccionada.

Desarrollo e implementación del Sistema de Firmas Electrónicas y Certificados Digitales del Estado e implantación de la autoridad administrativa competente (Vermejo Ruiz, 2020).

Este estudio muestra el diseño de una PKI robusta, utilizando una arquitectura de implementación profesional, segmentando las diferentes componentes y funciones de una PKI en múltiples servidores, lo que proporciona un servicio de alta escalabilidad. Además, muestra a detalle el nivel de seguridad a considerar en cada una de las capas de esta arquitectura, utilizando controles de acceso físico, firewalls, zonas desmilitarizadas, etc.

Transición, operación y mejora del servicio de firma electrónica del ESPE-CERT en el Departamento de Ciencias de la Computación utilizando ITIL V4 (Arcos Poma & Espín Flores, 2022).

En este trabajo se realiza una mejora de una PKI implementada en la ESPE y una nueva implementación de la misma, así como una evaluación de usabilidad y funcionalidad del servicio. Con los resultados de esta evaluación presenta un plan de mejora del servicio de firma electrónica y de la PKI.

Resumen general y conclusión del estado del arte.

Resumen General.

Luego de realizar la búsqueda de trabajos relacionados sobre la implementación de la firma digital en instituciones educativas y el proceso de acreditación para establecer una institución como entidad certificadora, se aplicó un análisis de los trabajos seleccionados considerando las preguntas de investigación planteadas, para poder obtener y establecer un estado del arte que sirva de guía para el propósito de esta investigación.

Durante este proceso se encontró trabajos relacionados con planteamientos prometedores, sin embargo, la conducción y resultados de algunos de ellos, perdían el hilo del objetivo principal de investigación, de esta manera se pudo descartar trabajos irrelevantes o con información que no conducían a ningún lado.

Por último, se presenta aquellos trabajos que aportan un gran valor al desarrollo de esta investigación.

Conclusión del estado del arte.

Como resultado de la revisión de trabajos relacionados, se puede concluir que la implementación de un servicio de firma electrónica, genera un impacto positivo en la gestión de procesos administrativos en instituciones educativas, mejorando los mismos en términos de eficacia y agilidad. Por otra parte, se concluye, que este tipo de servicios mejora

considerablemente la seguridad en la transacción los tramites a través de los medios digitales, generando mayor confianza entre las partes involucradas.

Sin embargo, si bien se pudo encontrar información acerca de la implementación de la firma digital y sus beneficios en instituciones educativas, no se logró encontrar trabajos relacionados que incluyeran información acerca del proceso para acreditar a la institución como entidad certificadora, siendo este aspecto, aún inédito en este tipo de instituciones.

Capítulo III

Implantación del servicio de firma electrónica

Objetivos

- Implantar el Servicio de firma electrónica en la Sede Latacunga de la ESPE, utilizando ITIL V4.

Alcance

Realizar una implantación mejorada del servicio de Firma Electrónica en el ESPE CERT del DCCO, en un plazo de 1 mes desde el inicio de la implantación, de manera que se pueda estar en capacidad de dar servicio a los estudiantes del DCCO y poder extender el servicio hacia la ESPE Sede Latacunga, para que pueda ser utilizada por toda la comunidad universitaria estudiantil de esta Sede. La implantación se tomará como realizada cuando el DCCO y la ESPE Sede Latacunga tengan el servicio a su disposición.

Indicadores de cumplimiento

- Disponibilidad del servicio.
- Tiempo de entrega
- Cumplimiento de términos y condiciones de acuerdo a trabajos anteriores.
- Errores y fallos.

Recursos

- Humanos: Se dispone de un estudiante a cargo del proyecto de titulación y del docente tutor del mismo.
- Financieros: Para esta fase de implantación no se requiere de recursos financieros.
- Hardware: Dos servidores disponibles en el laboratorio H401, computadora personal.
- Software: EJBCA, MariaDB, Docker.
- Conocimientos: Investigación previa.

Actividades a realizar

El siguiente cronograma indica todas las actividades a realizar, necesarias para realizar la implantación del servicio.

Tabla 4

Actividades para la implantación del servicio de firma electrónica

Tarea	Responsable	Duración	Comienzo	Fin
Diseño de una Jerarquía PKI.	Estudiante	2 días	12 jun	13 jun
Diseño de la arquitectura del servicio de firma electrónica.	Estudiante	2 días	14 jun	15 jun
Implantación del servicio de firma electrónica.	Estudiante	7 días	16 jun	19 jun
Capacitación de usuarios.	Estudiante	10 días	20 jun	03 jul
Operación y pruebas del servicio	Estudiante	9 días	04 jul	14 jul

Ejecución de actividades

Diseño de una Jerarquía PKI.

Durante la fase de investigación acerca de la firma electrónica, se logró determinar que, para poder utilizarla, es necesario el uso o la creación de certificados digitales, los cuales son emitidos a través de una PKI. Por lo cual, para poder crear un servicio de firma electrónica es necesario en primer lugar, crear una PKI con todas las componentes y estándares necesarios.

Una Jerarquía PKI se refiere a una estructura jerárquica que permite mejorar la confianza y organización en la forma en como una PKI emite sus certificados digitales. Dentro de una Jerarquía PKI se pueden encontrar varios niveles jerárquicos de certificación, donde los

niveles superiores, autorizan o certifican a los niveles inferiores, respectivamente. En base a esto, se ha diseñado la siguiente Jerarquía PKI.

Jerarquía PKI.

En primer lugar, se han definido los siguientes componentes de PKI:

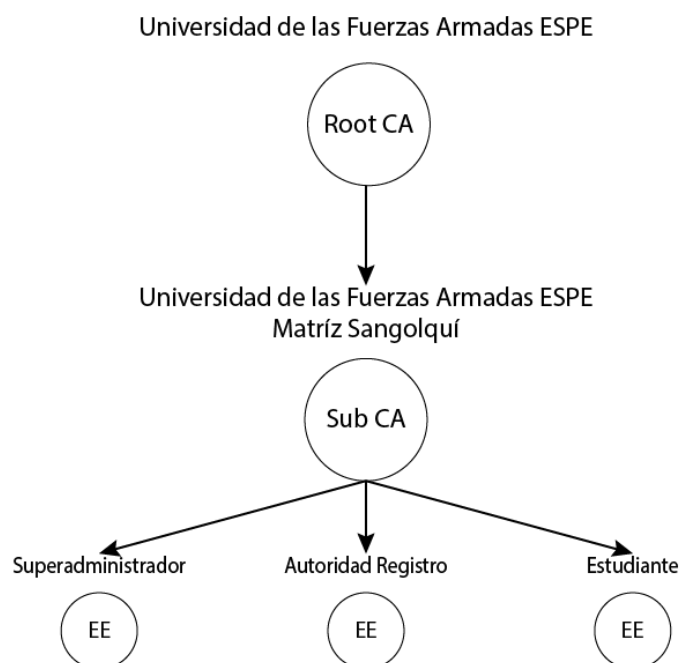
- RootCA: Este componente es una Autoridad Certificadora, pero se le agrega el nombre o nivel jerárquico “Root” o Raíz. Como su nombre lo indica, este RootCA es el nodo principal de toda la jerarquía PKI. Su propósito es firmar o autorizar Autoridades Certificadoras Subdelegadas o de niveles inferiores, es decir, emite certificados digitales a autoridades de niveles inferiores, y, además, al ser el primer nodo de toda la Jerarquía PKI, este tiene la característica de firmarse a sí misma, puesto que no existen nodos superiores a esta. Para identificar a esta Autoridad Certificadora Raíz, se le ha otorgado del nombre de la organización a la cuál va a pertenecer este servicio, que es Universidad de las Fuerzas Armadas ESPE.
- SubCA: Igualmente, este componente es una Autoridad Certificadora con el nombre jerárquico “Subordinate” o Subdelegada. Este nodo se encuentra el siguiente nivel inferior al nodo raíz o en niveles muchos bajos. Este nodo es firmado por la Autoridad Certificadora Raíz y tiene el propósito de emitir certificados digitales a Entidades Finales y no está autorizada para firmar otras Autoridades Certificadoras. Para estas Autoridades Certificadoras Subdelegadas se ha considerado las distintas Sedes de la ESPE, pero en primera instancia únicamente se ha considerado la Sede Sangolquí.
- EE: Por último, se tiene las Entidades Finales, que serán los distintos usuarios de la comunidad universitaria a los cuales se les otorgará los certificados digitales, de los cuales se ha considerado en primer lugar a los estudiantes. Además, se ha considerado usuarios para administrar la PKI como Autoridades

de Registro, que serán los encargados de administrar el ciclo de vida de los certificados digitales de los estudiantes, y el Superadministrador, que será el encargado de administrar la PKI en general.

Una vez definido todos los componentes de la PKI, se ha realizado el siguiente diseño de la Jerarquía PKI a implementar:

Figura 4

Diseño Jerarquía PKI



Como se puede observar en el diagrama, se encuentran especificados todos los componentes mencionados anteriormente. Como nodo principal de la Jerarquía PKI se toma el contexto global de la organización, que es Universidad de las Fuerzas Armadas ESPE, este nodo certificará a las distintas sedes de la ESPE, cada una de las sedes podría funcionar como una Autoridad Certificadora Subdelegada; para este proyecto se ha autorizado únicamente a la Universidad de las Fuerzas Armadas ESPE Sede Sangolquí como Autoridad Certificadora

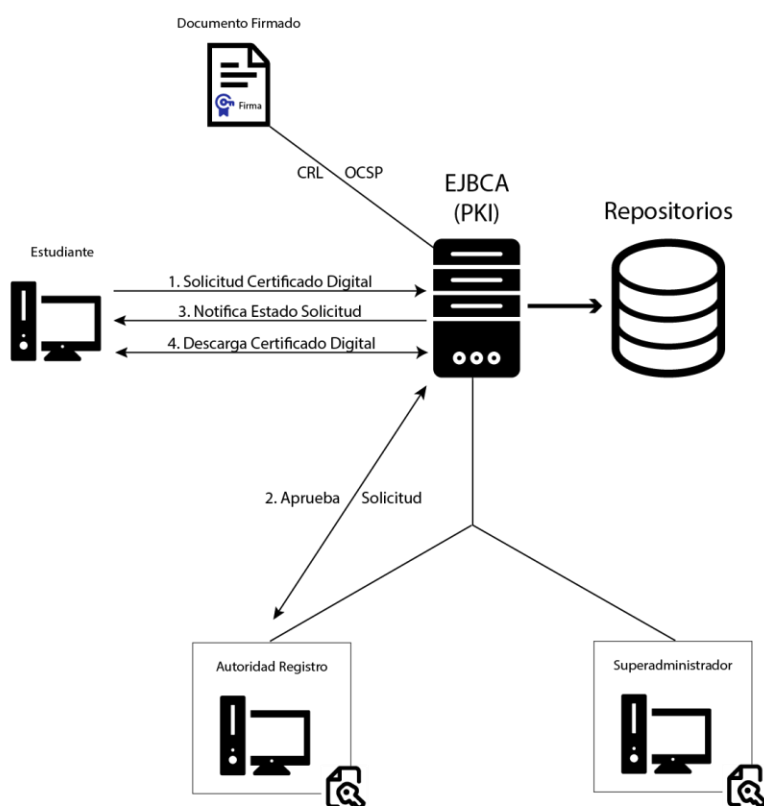
Subdelegada, que será la encargada de emitir los certificados digitales tanto a estudiante de la misma Sede como estudiantes de la Sede Latacunga.

Diseño de la arquitectura del servicio de firma electrónica.

A continuación, se detalla la arquitectura de cómo se implantó el servicio de firma electrónica.

Figura 5

Arquitectura del servicio de firma electrónica



Para la implantación del servicio de firma electrónica se utilizó dos servidores, en los que se instaló el software para la creación de la PKI y el motor de base de datos MariaDB para almacenar los certificados digitales, llaves criptográficas, entre otros.

Una vez instalado el servicio de base de datos y el servicio de la PKI, se procede a configurar el sistema para la emisión de los certificados digitales, roles y reglas de acceso para

la administración y uso del sistema, teniendo en cuenta la Jerarquía PKI diseñada anteriormente.

Para la administración del sistema se ha creado dos roles o perfiles de usuarios, un perfil de Superadministrador, que tiene acceso a todas las funciones del sistema, y un perfil de Autoridad de Registro, que tiene acceso únicamente a las funciones para manejar el ciclo de vida de los certificados digitales. Estos dos usuarios se autentican con el servicio haciendo uso de certificados digitales.

Para la emisión de nuevos certificados digitales para estudiantes, se ha configurado un rol o perfil de usuario de Estudiante, el cual es un perfil de acceso público, es decir, no necesita de certificados digitales para autenticarse con el servidor. Este perfil tiene acceso únicamente a las funciones para llenar el formulario de solicitud de un certificado digital, ver el estado del proceso y descargar el certificado digital.

Por último, se configura los servicios CRL y OCSP para la Autoridad de Validación, los cuales no necesitan autenticación, es decir, son servicios públicos sin restricción.

Funcionamiento del servicio de firma electrónica.

El proceso para la emisión de los certificados digitales se describe a continuación.

1. El estudiante accede al sistema, proporciona sus datos personales y realiza una nueva solicitud para la emisión de un certificado digital.
2. El sistema notifica al estudiante que se ha registrado su solicitud.
3. La Autoridad de Registro revisa la solicitud, valida la información proporcionada por el estudiante y procede a aprobar su solicitud si esta es válida, caso contrario, rechaza la solicitud.
4. El sistema notifica al estudiante que su solicitud ha sido aprobada y que puede proceder a descargar su certificado digital.
5. El estudiante accede al sistema y descarga su certificado digital.

Implantación del servicio de firma electrónica.

A continuación se describe el proceso de instalación y configuración del servicio, teniendo presente la Jerarquía PKI y la arquitectura del servicio descritas anteriormente.

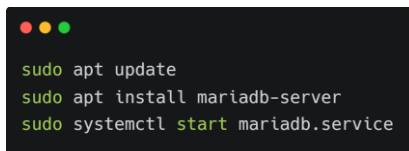
Instalación y configuración de la base de datos.

Para almacenar y persistir la información de los certificados digitales emitidos y configuraciones del servicio de firma electrónica, es necesario el uso de un motor de bases de datos para guardar dicha información. Para ello se ha elegido el motor de base de datos MariaDB, recomendado por el mismo software que se usará para implementar la PKI y con ello el servicio de firma electrónica. La instalación de MariaDB se detalla a continuación.

1. Se realiza una actualización del sistema mediante el comando: `sudo apt update`
2. Se instala el paquete de MariaDB: `sudo apt install mariadb-server`
3. Iniciamos el servicio de MariaDB: `sudo systemctl start mariadb.service`

Figura 6

Instalación MariaDB



```
sudo apt update
sudo apt install mariadb-server
sudo systemctl start mariadb.service
```

4. Ejecutamos un script para configurar MariaDB de manera segura: `sudo mysql_secure_installation`

Figura 7

Configuración segura de MariaDB


```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!
```

```
In order to log into MariaDB to secure it, we will need the current
password for the root user. If you have just installed MariaDB, and
you have not set the root password yet, the password will be blank,
so you should just press enter here.
```

```
Enter current password for root (enter for none): ****
OK, successfully used password, moving on...
```

```
Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.
```

```
You already have a root password set, so you can safely answer 'n'.
```

```
Change the root password? [Y/n] n
... skipping.
```

```
By default, a MariaDB installation has an anonymous user, allowing
anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.
```

```
Remove anonymous users? [Y/n] y
... Success!
```

```
Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.
```

```
Disallow root login remotely? [Y/n] y
... Success!
```

```
By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.
```

```
Remove test database and access to it? [Y/n] y
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!
```

```
Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.
```

```
Reload privilege tables now? [Y/n] y
... Success!
```

```
Cleaning up...
```

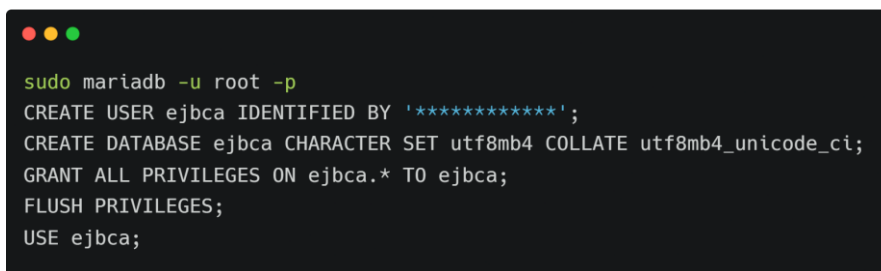
```
All done! If you have completed all of the above steps, your MariaDB
installation should now be secure.
```

```
Thanks for using MariaDB!
```

5. El software de la PKI requiere inicializar una base de datos y un usuario para conectarse a la misma.
 - 5.1. Nos conectamos a la base de datos a través del usuario root: `sudo mariadb -u root -p`
 - 5.2. Creamos un nuevo usuario y contraseña: `CREATE USER ejbca IDENTIFIED BY "*****";`
 - 5.3. Creamos la base de datos: `CREATE DATABASE ejbca CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;`
 - 5.4. Otorgamos al usuario creado todos los privilegios para usar la base de datos creada en el paso anterior: `GRANT ALL PRIVILEGES ON ejbca.* TO ejbca;`
 - 5.5. Restablecemos privilegios: `FLUSH PRIVILEGES;`
 - 5.6. Seleccionamos la base de datos creada: `USE ejbca;`

Figura 8

Creación de una base de datos para EJBCA



```
sudo mariadb -u root -p
CREATE USER ejbca IDENTIFIED BY '*****';
CREATE DATABASE ejbca CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
GRANT ALL PRIVILEGES ON ejbca.* TO ejbca;
FLUSH PRIVILEGES;
USE ejbca;
```

Instalación de EJBCA.

Este software tiene una plantilla o imagen de Docker lista para poder implementar una PKI. Por lo que en primer lugar se realiza la instalación de Docker.

1. Se remueve cualquier instalación previa de docker: `sudo yum remove docker docker-client docker-client-latest docker-client-latest docker-common docker-latest docker-latest-logrotate docker-logrotate docker-engine`

2. Instalamos una herramienta necesaria para administrar librerías del sistema operativo CentOS: `sudo yum install -y yum-utils`
3. Agregamos el repositorio de Docker a las librerías del sistema: `sudo yum-config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo`
4. Se instala Docker: `sudo yum install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin`
5. Iniciamos el servicio de Docker: `sudo systemctl start docker`
6. Verificamos que Docker se ha instalado correctamente: `sudo docker run hello-world`

Figura 9

Instalación Docker en CentOS

```

sudo yum remove docker \
    docker-client \
    docker-client-latest \
    docker-common \
    docker-latest \
    docker-latest-logrotate \
    docker-logrotate \
    docker-engine

sudo yum install -y yum-utils
sudo yum-config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo
sudo yum install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin
sudo systemctl start docker
sudo docker run hello-world

```

7. Una vez instalado Docker, procedemos a instalar EJBCA:

```

sudo docker run -it -d --name espekki -p 80:8080 -p 444:8443 -h 10.9.9.242
-e "DATABASE_JDBC_URL=jdbc:mariadb://10.9.9.243:3306/ejbca"
-e "DATABASE_USER=ejbca"
-e "DATABASE_PASSWORD=*****"
-e "SMTP_DESTINATION=smtp.gmail.com"
-e "SMTP_DESTINATION_PORT=587"
-e "SMTP_FROM=firmadigital@espe.edu.ec"
-e "SMTP_USERNAME=firmadigital@espe.edu.ec"
-e "SMTP_PASSWORD=*****"

```

```
-e "SMTP_TLS_ENABLED=true"
-e "SMTP_SSL_ENABLED=false"

keyfactor/ejbca-ce
```

Figura 10

Instalación EJBCA

```
sudo docker run -it -d --name espepki -p 80:8080 -p 444:8443 -h 10.9.9.242
-e "DATABASE_JDBC_URL=jdbc:mariadb://10.9.9.243:3306/ejbca"
-e "DATABASE_USER=ejbca"
-e "DATABASE_PASSWORD=*****"
-e "SMTP_DESTINATION=smtp.gmail.com"
-e "SMTP_DESTINATION_PORT=587"
-e "SMTP_FROM=firmadigital@espe.edu.ec"
-e "SMTP_USERNAME=firmadigital@espe.edu.ec"
-e "SMTP_PASSWORD=*****"
-e "SMTP_TLS_ENABLED=true"
-e "SMTP_SSL_ENABLED=false"
keyfactor/ejbca-ce
```

Figura 11

Servicio EJBCA ejecutándose

```
18:20:58+00:00;ACCESS_CONTROL;SUCCESS;ACCESSCONTROL;CORE;ejbca;;;resource0=/ca/190662683
2023-07-04 18:20:58,625+0000 INFO [org.ejbca.ui.cli.ca.GetAdminTruststoreCommand] (main)
/opt/keyfactor/tmp/tmp.6G0tbhDh2w/truststore.jks created.
2023-07-04 18:21:06,305+0000 INFO [org.jboss.as.protocol] (management task-1) WFLYPRT0057:
cancelled task by interrupting thread Thread[management-handler-thread - 1,5,management-handler-
thread]
2023-07-04 18:21:06,399+0000 INFO [/opt/keyfactor/bin/start.sh] (process:1) Enabling HTTPS
listener on 0.0.0.0:8443 with optional client certificate authentication.
2023-07-04 18:21:14,052+0000 INFO [org.jboss.as.protocol] (management task-1) WFLYPRT0057:
cancelled task by interrupting thread Thread[management-handler-thread - 1,5,management-handler-
thread]
2023-07-04 18:21:21,305+0000 INFO [/opt/keyfactor/bin/start.sh] (process:1) Enabling HTTP
listener on 0.0.0.0:8080.
2023-07-04 18:21:28,606+0000 INFO [/opt/keyfactor/bin/start.sh] (process:1) Enabling HSTS
2023-07-04 18:21:35,825+0000 INFO [org.jboss.as.protocol] (management task-1) WFLYPRT0057:
cancelled task by interrupting thread Thread[management-handler-thread - 1,5,management-handler-
thread]
```

Figura 12

Página de bienvenida EJBCA



Enroll
Create Certificate from CSR
Create Keystore
Create CV certificate
Register
Request Registration
Retrieve
Fetch CA Certificates
Fetch CA CRLs
List User's Certificates
Fetch User's Latest Certificate
Inspect
Inspect certificate/CSR
Check Certificate Status
Miscellaneous
Administration

The EJBCA Public Web has been deprecated and will be removed in an upcoming version of EJBCA. Please move your workflows to the EJBCA RA UI

Welcome to the public EJBCA pages

Enroll

- Create Certificate from CSR - Send a PKCS#10 certificate request generated by your server, and receive a certificate that can be installed on the server. Consult your server documentation.
- Create Keystore - Create a server generated keystore in PEM, PKCS#12 or JKS format and save to your disc. This keystore can be installed in a server, browser or in other applications.
- Create CV Certificate - Used for EU EAC ePassport PKI. Send a CVC certificate request generated by an Inspection System, and receive a CV certificate. Note: this can not be used for regular certificates, CV certificates are completely different.

Retrieve

- Fetch CA Certificates - Browse and download CA certificates.
- Fetch CA CRLs - Download Certificate Revocation Lists.
- Fetch User's Latest Certificate - Download the last issued certificate for a user for whom you know the certificate Distinguished Name.

Inspect

- Inspect certificate/CSR - Inspect a dump of a CSR or a certificate. This gives an output of a CVC or ASN.1 dump, suitable for technical inspection and debugging.

Miscellaneous

- List User's Certificates - List certificates for a user for whom you know the certificate Distinguished Name.
- Check Certificate Status - Check revocation status for a certificate where you know the Issuer Distinguished Name and the serial number.
- Administration - Go to the EJBCA Admin-GUI. Requires client certificate authentication.

Configuración de la Jerarquía PKI.

Una vez instalado todo el software necesario para el servicio de firma electrónica, se procede a configurar la Jerarquía PKI propuesta. Para esto, en la consola de administración de EJBCA se deben crear perfiles de certificados, autoridades de certificación, tokens criptográficos y perfiles de entidades finales para cumplir con dicha Jerarquía.

1. Creación de la Autoridad Certificadora Raíz (RootCA)

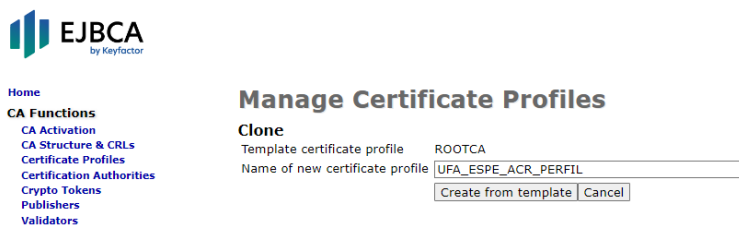
1.1. Crear perfil de certificado

En primer lugar, se debe crear un perfil de certificado, esto es una plantilla donde se define las características que van a tener los certificados finales emitidos por esta Autoridad Certificadora. Entre las características más relevantes se destaca el algoritmo de encriptación a usar, el tiempo de validez de este certificado.

- 1.1.1. Desde las funciones de CA en la consola de administración, nos dirigimos a Perfiles de Certificados y clonamos el perfil existente ROOTCA, le asignamos el nombre UFA_ESPE_ACR_PERFIL.

Figura 13

Creando perfil de certificado para Autoridad Certificadora Raíz



- 1.1.2. Una vez creado el perfil de certificado, procedemos a editarlo de la siguiente manera. Elegimos el algoritmo ECDSA para la creación de las llaves criptográficas.
- 1.1.3. Determinamos el tiempo de validez que tendrá este certificado, en este caso 30 años y proporcionamos una descripción a dicho perfil de certificado.
- 1.1.4. El resto de parámetros configuramos como se muestra en la siguiente figura.

Figura 14

Configurando perfil de certificado para Autoridad Certificadora Raíz



- Home
- CA Functions**
 - CA Activation
 - CA Structure & CRLs
 - Certificate Profiles
 - Certification Authorities
 - Crypto Tokens
 - Publishers
 - Validators
- RA Functions**
 - Add End Entity
 - End Entity Profiles
 - Search End Entities
 - User Data Sources
- VA Functions**
 - OCSF Responders
- Supervision Functions**
 - Approval Profiles
 - Approve Actions
- System Functions**
 - Roles and Access Rules
 - Remote Authentication Services
- System Configuration**
 - CMP Configuration
 - SCPE Configuration
 - System Configuration
- My Preferences**
- RA Web**
- Public Web**

Edit

Certificate Profile: UFA_ESPE_ACR_PERFIL

Back to Certificate Profiles	
Certificate Profile ID	1886171444
Type	<input type="radio"/> End Entity <input type="radio"/> Sub CA <input checked="" type="radio"/> Root CA
Available Key Algorithms	DSA ECDSA RSA Ed25519 Ed448
Available ECDSA curves	K-409 / sect409k1 K-571 / sect571k1 P-192 / prime192v1 / secp192r1 P-224 / secp224r1 P-256 / prime256v1 / secp256r1
Available Bit Lengths	No algorithm/curve with selectable key sizes selected.
Signature Algorithm	Inherit from issuing CA
Validity or end date of the certificate	30y ISO 8601 date: [yyyy-MM-dd HH:mm:ssZ]: "2023-07-04 18:47:17+00:00" (*y "mo "d "h "m "s) - y=365 days, mo=30 days
Validity Offset	<input type="checkbox"/> Use...
Expiration Restrictions	<input type="checkbox"/> Use...
Profile Description	Perfil de Certificado para Autoridad Certificadora Raiz Universidad de las Fuerzas Armadas ESPE
Permissions	
Allow Validity Override	<input checked="" type="checkbox"/> Allow
Allow Extension Override	<input type="checkbox"/> Allow...
Allow certificate serial number override	<input type="checkbox"/> Allow
Allow Subject DN Override by CSR	<input type="checkbox"/> Allow
Allow Subject DN Override by End Entity Information	<input type="checkbox"/> Allow
Allow Key Usage Override	<input type="checkbox"/> Allow
Allow Backdated Revocation	<input type="checkbox"/> Allow
X.509v3 extensions	
Basic Constraints	<input checked="" type="checkbox"/> Use... <input checked="" type="checkbox"/> Critical
Path Length Constraint	<input type="checkbox"/> Add... Value 0
Authority Key ID	<input type="checkbox"/> Use
Subject Key ID	<input checked="" type="checkbox"/> Use
X.509v3 extensions Usages	
Key Usage	<input checked="" type="checkbox"/> Use... <input checked="" type="checkbox"/> Critical
Key Usage:	<input checked="" type="checkbox"/> Digital Signature <input type="checkbox"/> Data encipherment <input checked="" type="checkbox"/> CRL sign <input type="checkbox"/> Non-repudiation <input type="checkbox"/> Key agreement <input type="checkbox"/> Encipher only <input type="checkbox"/> Key encipherment <input checked="" type="checkbox"/> Key certificate sign <input type="checkbox"/> Decipher only
Extended Key Usage	<input type="checkbox"/> Use... <input type="checkbox"/> Critical
Certificate Policies	<input type="checkbox"/> Use... <input type="checkbox"/> Critical
X.509v3 extensions Names	
Subject Alternative Name	<input type="checkbox"/> Use... <input type="checkbox"/> Critical <input checked="" type="checkbox"/> Search enabled (search enabled SAN use more storage)
Issuer Alternative Name	<input type="checkbox"/> Use... <input type="checkbox"/> Critical
Subject Directory Attributes	<input type="checkbox"/> Use
Name Constraints	<input type="checkbox"/> Use... <input type="checkbox"/> Critical
X.509v3 extensions Validation data	
CRL Distribution Points	<input type="checkbox"/> Use... <input type="checkbox"/> Critical
Freshest CRL (a.k.a. Delta CRL DP)	<input type="checkbox"/> Use...
Authority Information Access	<input type="checkbox"/> Use...
Private Key Usage Period	<input type="checkbox"/> Start offset... (*y "mo "d "h "m "s)
	<input type="checkbox"/> Period length... (*y "mo "d "h "m "s)
QC Statements extension	
Qualified Certificates Statements	<input type="checkbox"/> Use... <input type="checkbox"/> Critical
Other Extensions	
OCSF No Check	<input type="checkbox"/> Use
Microsoft Certificate Template Name	<input type="checkbox"/> Add... Value DomainController (only the name, not the actual template)
Use Microsoft ObjectSid Security Extension	<input checked="" type="checkbox"/> Use
ePassport	
ICAO Document Type List	<input type="checkbox"/> Use... <input type="checkbox"/> Critical
Approval Settings	
Add/Edit End Entity	None
Key Recovery	None
Revocation	None
Other Data	
LDAP DN order	<input type="checkbox"/> Use
Custom Subject DN Order	<input type="checkbox"/> Use... <input type="checkbox"/> Apply LDAP DN order settingValue (comma separated list of DN components)
CN postfix	<input type="checkbox"/> Add... Value (text appended after first CN field)
Subset of Subject DN	<input type="checkbox"/> Restrict...
Subset of Subject Alt. Name	<input type="checkbox"/> Restrict...
Available CAs	Any CA ManagementCA UFA_ESPE_ACR UFA_ESPE_SANGOLQUI_ACS
Account Binding Namespace	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

1.2. Crear token criptográfico

Lo siguiente es crear un token criptográfico con el que la Autoridad Certificadora Raíz firmará los certificados finales. Es recomendable crear un token criptográfico para cada Autoridad Certificadora.

- 1.2.1. Desde las funciones de CA, nos dirigimos a la opción de tokens criptográficos y creamos uno nuevo con el nombre UFA_ESPE_CRYPTOTOKEN. Además, marcamos la opción de auto activación del token, esto quiere decir, que, si el servicio se reinicia, este token volverá a activarse de manera automática, y por último establecemos una contraseña para este token.

Figura 15

Creando token criptográfico para Autoridad Certificadora Raíz

The screenshot shows the EJBCA web interface. On the left is a navigation menu with 'Home', 'CA Functions', and 'RA Functions'. Under 'CA Functions', 'Crypto Tokens' is selected. The main content area is titled 'New Crypto Token' and contains the following form fields:

- Name: UFA_ESPE_CRYPTOTOKEN
- Type: SOFT (dropdown menu)
- Auto-activation: Use
- Use explicit ECC parameters (ICAO CSCA and DS certificates): Use
- Allow export of private keys: Allow
- Authentication Code: [masked with dots]
- Repeat Authentication Code: [masked with dots]
- Save: [button]

- 1.2.2. Una vez creado el token criptográfico para la Autoridad Certificadora Raíz, procedemos a crear tres de llaves criptográficas.

1.2.2.1. Creamos una llave de firma con el algoritmo ECDSA con el nombre UFA_ESPE_SIGN_KEY

1.2.2.2. Creamos una llave de encriptación con el algoritmo RSA con el nombre UFA_ESPE_ENCRYPT_KEY

1.2.2.3. Creamos una llave de prueba con el algoritmo ECDSA con el nombre UFA_ESPE_TEST_KEY

Figura 16

Configuración del token criptográfico para la Autoridad Certificadora Raíz

EJBCA
by KeyFactor

Home
CA Functions
 CA Activation
 CA Structure & CRLs
 Certificate Profiles
 Certification Authorities
 Crypto Tokens
 Publishers
 Validators
RA Functions
 Add End Entity
 End Entity Profiles
 Search End Entities
 User Data Sources
VA Functions
 OSCP Responders
Supervision Functions
 Approval Profiles
 Approve Actions
System Functions
 Roles and Access Rules
 Remote Authentication
 Services
System Configuration
 CMP Configuration
 SCEP Configuration
 System Configuration
 My Preferences
 RA Web
 Public Web

Crypto Token : UFA_ESPE_CRYPTOTOKEN

Back to Crypto Token overview Switch to edit mode

ID: -1137771164
 Name: UFA_ESPE_CRYPTOTOKEN
 Type: SoftCryptoToken
 Used:
 Active:
 Auto-activation:
 Use explicit ECC parameters (ICAO CSCA and DS certificates):
 Allow export of private keys:

Alias	Key Algorithm	Key Specification	SubjectKeyID	Action
<input type="checkbox"/> UFA_ESPE_ENCRYPT_KEY	RSA	4096	b911058b894d6178ebfdf474b457dcab3862ad26	Test Remove Download Public Key
<input type="checkbox"/> UFA_ESPE_SIGN_KEY	ECDSA	prime256v1 / secp256r1 / P-256	54263166c440e5cd4a9ad3ab13017d80b9b422c8	Test Remove Download Public Key
<input type="checkbox"/> UFA_ESPE_TEST_KEY	ECDSA	prime256v1 / secp256r1 / P-256	40fd6e0967123e7f21bba1aa49ad052d9e4c91e5	Test Remove Download Public Key

Remove selected

signKey: RSA 4096 Generate new key pair

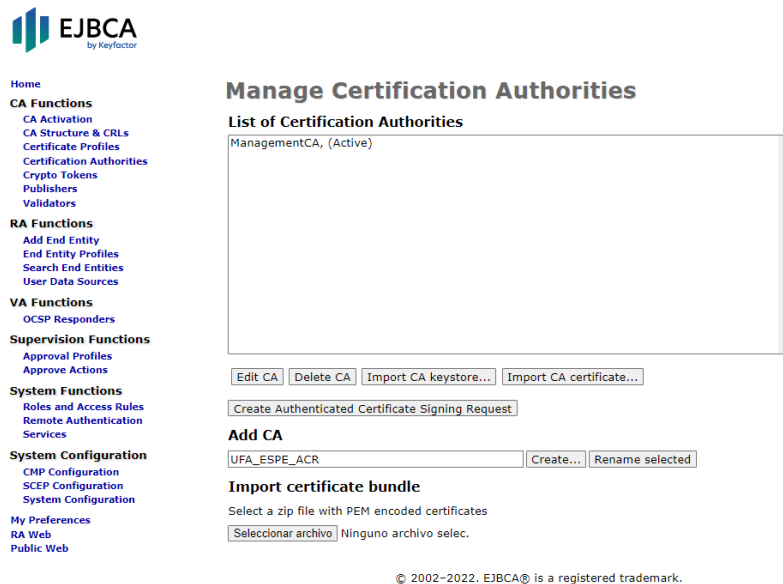
© 2002-2022. EJBCA® is a registered trademark.

1.3. Crear Autoridad Certificadora Raíz

- 1.3.1. Desde las funciones de CA, nos dirigimos a la opción de autoridades certificadoras y creamos una nueva con el nombre UFA_ESPE_ACR

Figura 17

Creación de la Autoridad Certificadora Raíz



EJBCA
by Keyfactor

Home

CA Functions

- CA Activation
- CA Structure & CRLs
- Certificate Profiles
- Certification Authorities
- Crypto Tokens
- Publishers
- Validators

RA Functions

- Add End Entity
- End Entity Profiles
- Search End Entities
- User Data Sources

VA Functions

- OCSF Responders

Supervision Functions

- Approval Profiles
- Approve Actions

System Functions

- Roles and Access Rules
- Remote Authentication Services

System Configuration

- CMP Configuration
- SCEP Configuration
- System Configuration

My Preferences
RA Web
Public Web

Manage Certification Authorities

List of Certification Authorities

ManagementCA, (Active)

Edit CA Delete CA Import CA keystore... Import CA certificate...

Create Authenticated Certificate Signing Request

Add CA

UFA_ESPE_ACR Create... Rename selected

Import certificate bundle

Select a zip file with PEM encoded certificates

Seleccionar archivo Ninguno archivo selec.

© 2002-2022. EJBCA® is a registered trademark.

1.3.2. Configuramos la Autoridad Certificadora Raíz como se muestra en la siguiente figura

Figura 18

Configuración de la Autoridad Certificadora Raíz



Home

CA Functions

CA Activation
CA Structure & CRLs
Certificate Profiles
Certification Authorities
Crypto Tokens
Publishers
Validators

RA Functions

Add End Entity
End Entity Profiles
Search End Entities
User Data Sources

VA Functions

OCSP Responders

Supervision Functions

Approval Profiles
Approve Actions

System Functions

Roles and Access Rules
Remote Authentication
Services

System Configuration

CMP Configuration
SCEP Configuration
System Configuration

My Preferences

RA Web
Public Web

Edit CA

CA Name : UFA_ESPE_ACR

Back to Certificate Authorities	
CA ID	-1342132618
CA Type	X509
Crypto Token	UFA_ESPE_CRYPTO_TOKEN
Signing Algorithm	SHA512withECDSA
defaultKey	UFA_ESPE_ENCRYPT_KEY
certSignKey	UFA_ESPE_SIGN_KEY
crSignKey	UFA_ESPE_SIGN_KEY
keyEncryptKey	UFA_ESPE_ENCRYPT_KEY
testKey	UFA_ESPE_TEST_KEY
Extended Services Key Specification	<input type="text" value="RSA 2048"/>
Key sequence format	<input type="text" value="numeric [0-9]"/>
Key sequence	<input type="text" value="00000"/>
Description	<input type="text" value="Autoridad Certificadora Raiz Universidad de las Fuerzas Armadas ESPE"/>
Directives	
Enforce unique public keys	<input checked="" type="checkbox"/> Enforce
Enforce key renewal	<input type="checkbox"/> Enforce
Enforce unique DN	<input checked="" type="checkbox"/> Enforce
Enforce unique Subject DN SerialNumber	<input type="checkbox"/> Enforce
Use Certificate Request History	<input type="checkbox"/> Use
Use User Storage	<input checked="" type="checkbox"/> Use
Use Certificate Storage	<input checked="" type="checkbox"/> Use...
CA Certificate Data	
Subject DN	CN=Universidad de las Fuerzas Armadas ESPE,O=ESPE,C=EC
Issuer DN	CN=Universidad de las Fuerzas Armadas ESPE,O=ESPE,C=EC
Signed By	Self Signed
Certificate Profile	UFA_ESPE_ACR_PERFIL
Validity (*y *mo *d *h *m *s) or end date of the certificate	<input type="text" value="30y"/> (used when CA is renewed) ISO 8601 date:=[yyyy-MM-dd HH:mm:ssZZ]: '2023-07-04 19:21:24+00:00'.y=365 days, mo=30 days
Subject Alternative Name	None
Certificate Policy OID	None
Use UTF-8 in policy notice text	<input checked="" type="checkbox"/> Use
PrintableString encoding in DN	<input type="checkbox"/> Use
LDAP DN order	<input type="checkbox"/> Use
Serial Number Octet Size	<input type="text" value="20"/>
Name Constraints, Permitted	<input type="text"/> <small>List of domain names, IPv4/IPv6 address/netmask pairs, DNS, URIs and RFC 822 Names. One per line. Examples (without quotes): 'example.com' '198.51.100.0/24' 'CN=Name,O=Company' '@example.com' 'uri:example.com' 'uri:example.com'</small>
Name Constraints, Excluded	<input type="text"/> <small>Use 0.0.0.0/0 and ::/0 to disallow certificates for all plain IP addresses. Use a single . to disallow all DNS names.</small>
CA Certificate	<input type="button" value="View Certificate"/>
CA Alternate Cross Certificate Chains Used to construct end entity certificate chains with different root CAs for ACME enrollment.	None
CRL Specific Data	
Microsoft CA Compatibility Mode	<input type="checkbox"/> Use <small>Warning! Microsoft CA Compatibility Mode is irreversible.</small>
Authority Key ID	<input checked="" type="checkbox"/> Use <input type="checkbox"/> Critical
CRL Number	<input checked="" type="checkbox"/> Use <input type="checkbox"/> Critical
Issuing Distribution Point on CRLs	<input checked="" type="checkbox"/> Use <input type="checkbox"/> Critical
CA issuer URI	<input type="text"/>
Keep expired certificates on CRL	<input type="checkbox"/> Use
Use CRL partitions	<input type="checkbox"/> Use
CRL Expire Period (*y *mo *d *h *m)	<input type="text" value="3mo"/> y=365 days , mo=30 days
CRL Issue Interval (*y *mo *d *h *m)	<input type="text" value="0m"/> y=365 days , mo=30 days
CRL Overlap Time (*y *mo *d *h *m)	<input type="text" value="0m"/> y=365 days , mo=30 days
Delta CRL Period (*y *mo *d *h *m)	<input type="text" value="0m"/> y=365 days , mo=30 days (0m, if no delta CRLs are issued)
Generate CRL Upon Revocation	<input type="checkbox"/> Use A fresh CRL or delta CRL is generated after revocation or reactivation of a certificate.
Allow changing revocation reason	<input type="checkbox"/> Use
Publishers	<input type="text" value="CRL OCSP PUBLICADOR"/>
Default CA defined validation data	
Default CRL Distribution Point	<input type="text" value="http://192.168.110.190:80/ejbc/publicweb/webd"/> <input type="button" value="Generate"/> (used in CRL, and as default value)
Default CRL Issuer	<input type="text" value="CN=Universidad de las Fuerzas Armadas ESPE,O=ESPE,C=EC"/> <input type="button" value="Generate"/> (used in CRL, and as default value)
Default Freshest CRL Distribution Point	<input type="text"/> <input type="button" value="Generate"/> (used in CRL, and as default value)
OCSP service Default URI	<input type="text" value="http://192.168.110.190:80/ejbc/publicweb/status"/> <input type="button" value="Generate"/>

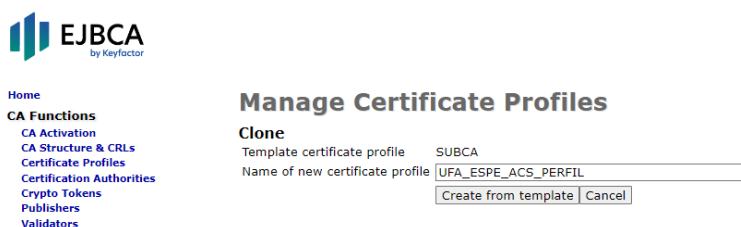
2. Creación de la Autoridad Certificadora Subdelegada (SubCA)

2.1. Crear perfil de certificado

- 2.1.1. Desde las funciones de CA en la consola de administración, nos dirigimos a Perfiles de Certificados y clonamos el perfil existente SUBCA, le asignamos el nombre UFA_ESPE_ACS_PERFIL.

Figura 19

Creando perfil de certificado para Autoridad Certificadora Subdelegada



- 2.1.2. Una vez creado el perfil de certificado, procedemos a editarlo de la siguiente manera. Elegimos el algoritmo ECDSA para la creación de las llaves criptográficas.
- 2.1.3. Determinamos el tiempo de validez que tendrá este certificado, en este caso 30 años y proporcionamos una descripción a dicho perfil de certificado.
- 2.1.4. El resto de parámetros configuramos como se muestra en la siguiente figura.

Figura 20

Configurando perfil de certificado para Autoridad Certificadora Subdelegada



- Home
- CA Functions**
 - CA Activation
 - CA Structure & CRLs
 - Certificate Profiles
 - Certification Authorities
 - Crypto Tokens
 - Publishers
 - Validators
- RA Functions**
 - Add End Entity
 - End Entity Profiles
 - Search End Entities
 - User Data Sources
- VA Functions**
 - OCSF Responders
- Supervision Functions**
 - Approval Profiles
 - Approve Actions
- System Functions**
 - Roles and Access Rules
 - Remote Authentication Services
- System Configuration**
 - CMP Configuration
 - SCEP Configuration
 - System Configuration
- My Preferences**
 - RA Web
 - Public Web

Edit

Certificate Profile: UFA_ESPE_ACS_PERFIL

Back to Certificate Profiles	
Certificate Profile ID	1020514169
Type	End Entity / Sub CA / Root CA
Available Key Algorithms	DSA ECDSA RSA Ed25519 Ed448
Available ECDSA curves	K-409 / sect409k1 K-571 / sect571k1 P-192 / prime192v1 / secp192r1 P-224 / secp224r1 P-256 / prime256v1 / secp256r1
Available Bit Lengths	No algorithm/curve with selectable key sizes selected.
Signature Algorithm	Inherit from issuing CA
Validity or end date of the certificate	30y ISO 8601 date: [yyyy-MM-dd HH:mm:ssZ]: 2023-07-04 20:07:03+00:00 (*y *mo *d *h *m *s) - y=365 days, mo=30 days
Validity Offset	<input type="checkbox"/> Use...
Expiration Restrictions	<input type="checkbox"/> Use...
Profile Description	Perfil de Certificado para Autoridad Certificadora Subdelegada Universidad de las Fuerzas Armadas ESPE Sede Matriz Sangolquí
Permissions	
Allow Validity Override	<input checked="" type="checkbox"/> Allow
Allow Extension Override	<input type="checkbox"/> Allow...
Allow certificate serial number override	<input type="checkbox"/> Allow
Allow Subject DN Override by CSR	<input type="checkbox"/> Allow
Allow Subject DN Override by End Entity Information	<input type="checkbox"/> Allow
Allow Key Usage Override	<input type="checkbox"/> Allow
Allow Backdated Revocation	<input type="checkbox"/> Allow
X.509v3 extensions	
Basic Constraints	<input checked="" type="checkbox"/> Use... <input checked="" type="checkbox"/> Critical
Path Length Constraint	<input checked="" type="checkbox"/> Add. Value 0
Authority Key ID	<input checked="" type="checkbox"/> Use
Subject Key ID	<input checked="" type="checkbox"/> Use
X.509v3 extensions Usages	
Key Usage	<input checked="" type="checkbox"/> Use... <input checked="" type="checkbox"/> Critical
Key Usage:	<input checked="" type="checkbox"/> Digital Signature <input type="checkbox"/> Data encipherment <input checked="" type="checkbox"/> CRL sign <input type="checkbox"/> Non-repudiation <input type="checkbox"/> Key agreement <input type="checkbox"/> Encipher only <input type="checkbox"/> Key encipherment <input checked="" type="checkbox"/> Key certificate sign <input type="checkbox"/> Decipher only
Extended Key Usage	<input type="checkbox"/> Use... <input type="checkbox"/> Critical
Certificate Policies	
Certificate Policies	<input type="checkbox"/> Use... <input type="checkbox"/> Critical
X.509v3 extensions Names	
Subject Alternative Name	<input checked="" type="checkbox"/> Use... <input type="checkbox"/> Critical <input checked="" type="checkbox"/> Search enabled (search enabled SAN use more storage)
Issuer Alternative Name	<input checked="" type="checkbox"/> Use... <input type="checkbox"/> Critical
Subject Directory Attributes	<input type="checkbox"/> Use...
Name Constraints	<input type="checkbox"/> Use... <input type="checkbox"/> Critical
X.509v3 extensions Validation data	
CRL Distribution Points	<input checked="" type="checkbox"/> Use... <input type="checkbox"/> Critical
Use CA defined CRL Distribution Point	<input checked="" type="checkbox"/> Use...
CRL Distribution Point URI	http://192.168.110.190:80/ejbc/publicweb/webdist/cer
CRL Issuer	CN=TestCA,O=AnaTom,C=SE
Freshest CRL (a.k.a. Delta CRL DP)	<input type="checkbox"/> Use...
Authority Information Access	
Use CA defined OSCP locator	<input checked="" type="checkbox"/> Use...
OCSP Service Locator URI	
Use CA defined CA issuer	<input checked="" type="checkbox"/> Use...
CA issuer URI	<input type="text"/> (Add)
Private Key Usage Period	<input type="checkbox"/> Start offset: <input type="text"/> (*y *mo *d *h *m *s) <input type="checkbox"/> Period length: <input type="text"/> (*y *mo *d *h *m *s)
QC Statements extension	
Qualified Certificates Statements	<input type="checkbox"/> Use... <input type="checkbox"/> Critical
Other Extensions	
OCSP No Check	<input type="checkbox"/> Use...
Microsoft Certificate Template Name	<input type="checkbox"/> Add. Value DomainController (only the name, not the actual template)
Use Microsoft ObjectSid Security Extension	<input checked="" type="checkbox"/> Use...
ePassport	
ICAO Document Type List	<input type="checkbox"/> Use... <input type="checkbox"/> Critical
Approval Settings	
Add/Edit End Entity	None
Key Recovery	None
Revocation	None
Other Data	
LDAP DN order	<input type="checkbox"/> Use
Custom Subject DN Order	<input type="checkbox"/> Use... <input type="checkbox"/> Apply LDAP DN order setting Value <input type="text"/> (comma separated list of DN components)
CN postfix	<input type="checkbox"/> Add. Value <input type="text"/> (text appended after first CN field)
Subset of Subject DN	<input type="checkbox"/> Restrict...
Subset of Subject Alt. Name	<input type="checkbox"/> Restrict...
Available CAs	Any CA ManagementCA UFA_ESPE_ACR UFA_ESPE_SANGOLQUI_ACS
Publishers	<input type="text"/>
Account Binding Namespace	<input type="text"/>
Save Cancel	

2.2. Crear token criptográfico

- 2.2.1. Desde las funciones de CA, nos dirigimos a la opción de tokens criptográficos y creamos uno nuevo con el nombre UFA_ESPE_ACS_CRYPTOTOKEN. Además, marcamos la opción de auto activación del token, esto quiere decir, que, si el servicio se reinicia, este token volverá a activarse de manera automática, y por último establecemos una contraseña para este token.

Figura 21

Creando token criptográfico para Autoridad Certificadora Subdelegada

The screenshot shows the EJBCA web interface for creating a new crypto token. The left sidebar contains a navigation menu with 'Home', 'CA Functions' (including CA Activation, CA Structure & CRLs, Certificate Profiles, Certification Authorities, Crypto Tokens, Publishers, and Validators), and 'RA Functions' (including Add End Entity, End Entity Profiles, Search End Entities, and User Data Sources). The main content area is titled 'New Crypto Token' and contains the following fields and options:

- Name: UFA_ESPE_ACS_CRYPTOTOKEN
- Type: SOFT
- Auto-activation: Use
- Use explicit ECC parameters (ICA0 CSCA and DS certificates): Use
- Allow export of private keys: Allow
- Authentication Code: [masked with dots]
- Repeat Authentication Code: [masked with dots]
- Save button

- 2.2.2. Una vez creado el token criptográfico para la Autoridad Certificadora Subdelegada, procedemos a crear tres de llaves criptográficas.

2.2.2.1. Creamos una llave de firma con el algoritmo ECDSA con el nombre UFA_ESPE_ACS_SIGN_KEY

2.2.2.2. Creamos una llave de encriptación con el algoritmo RSA con el nombre UFA_ESPE_ACS_ENCRYPT_KEY

2.2.2.3. Creamos una llave de prueba con el algoritmo ECDSA con el nombre UFA_ESPE_ACS_TEST_KEY

Figura 22

Configuración del token criptográfico para la Autoridad Certificadora Subdelegada

Crypto Token : UFA_ESPE_ACS_CRYPTOTOKEN

Back to Crypto Token overview Switch to edit mode

ID: -220954597
 Name: UFA_ESPE_ACS_CRYPTOTOKEN
 Type: SoftCryptoToken
 Used:
 Active:
 Auto-activation:
 Use explicit ECC parameters (ICA0 CSCA and DS certificates):
 Allow export of private keys:

	Alias	Key Algorithm	Key Specification	SubjectKeyID	Action
<input type="checkbox"/>	UFA_ESPE_ACS_ENCRYPT_KEY	RSA	4096	541541e45bb455c8d4134af9fe6324c3ebc300bc	Test Remove Download Public Key
<input type="checkbox"/>	UFA_ESPE_ACS_SIGN_KEY	ECDSA	prime256v1 / secp256r1 / P-256	ee4c0e10d4ea148439a2deb29953d58931ada95e	Test Remove Download Public Key
<input type="checkbox"/>	UFA_ESPE_ACS_TEST_KEY	ECDSA	prime256v1 / secp256r1 / P-256	0b835342741a56a2ecba5dd757d9e0ba24eb3b0a	Test Remove Download Public Key

Remove selected

signKey: RSA 4096 Generate new key pair

© 2002-2022. EJBCA® is a registered trademark.

2.3. Crear Autoridad Certificadora Subdelegada

2.3.1. Desde las funciones de CA, nos dirigimos a la opción de autoridades certificadoras y creamos una nueva con el nombre UFA_ESPE_SANGOLQUI_ACS

Figura 23

Creación de la Autoridad Certificadora Subdelegada

Manage Certification Authorities

List of Certification Authorities

- ManagementCA, (Active)
- UFA_ESPE_ACR, (Active)

Edit CA Delete CA Import CA keystore... Import CA certificate...

Create Authenticated Certificate Signing Request

Add CA

UFA_ESPE_SANGOLQUI_ACS Create... Rename selected

Import certificate bundle

Select a zip file with PEM encoded certificates

Seleccionar archivo Ninguno archivo selec.

© 2002-2022. EJBCA® is a registered trademark.

2.3.2. Configuramos la Autoridad Certificadora Subdelegada como se muestra en la siguiente figura

Figura 24

Configuración de la Autoridad Certificadora Subdelegada



Home

CA Functions

CA Activation
CA Structure & CRLs
Certificate Profiles
Certification Authorities
Crypto Tokens
Publishers
Validators

RA Functions

Add End Entity
End Entity Profiles
Search End Entities
User Data Sources

VA Functions

OCSF Responders

Supervision Functions

Approval Profiles
Approve Actions

System Functions

Roles and Access Rules
Remote Authentication
Services

System Configuration

CMP Configuration
SCEP Configuration
System Configuration

My Preferences

RA Web

Public Web

Edit CA

CA Name : UFA_ESPE_SANGOLQUI_ACS

Back to Certificate Authorities	
CA ID	190662683
CA Type	X509
Crypto Token	UFA_ESPE_ACS_CRYPTO_TOKEN
Signing Algorithm	SHA256withECDSA
defaultKey	UFA_ESPE_ACS_ENCRYPT_KEY
certSignKey	UFA_ESPE_ACS_SIGN_KEY
crfSignKey	UFA_ESPE_ACS_SIGN_KEY
keyEncryptKey	UFA_ESPE_ACS_ENCRYPT_KEY
testKey	UFA_ESPE_ACS_TEST_KEY
Extended Services Key Specification	<input type="text" value="RSA 2048"/>
Key sequence format	<input type="text" value="numeric [0-9]"/>
Key sequence	<input type="text" value="00000"/>
Description	Autoridad Certificadora Subdelegada Universidad de las Fuerzas Armadas ESPE Sede Matriz Sangolqui
Directives	
Enforce unique public keys	<input checked="" type="checkbox"/> Enforce
Enforce key renewal	<input type="checkbox"/> Enforce
Enforce unique DN	<input checked="" type="checkbox"/> Enforce
Enforce unique Subject DN SerialNumber	<input type="checkbox"/> Enforce
Use Certificate Request History	<input type="checkbox"/> Use
Use User Storage	<input checked="" type="checkbox"/> Use
Use Certificate Storage	<input checked="" type="checkbox"/> Use...
CA Certificate Data	
Subject DN	CN=Universidad de las Fuerzas Armadas ESPE Sangolqui,O=ESPE,C=EC
Issuer DN	CN=Universidad de las Fuerzas Armadas ESPE,O=ESPE,C=EC
Signed By	UFA_ESPE_ACR
Certificate Profile	UFA_ESPE_ACS_PERFIL
Validity (*y *mo *d *h *m *s) or end date of the certificate	<input type="text" value="30y"/> (used when CA is renewed) ISO 8601 date:=[yyyy-MM-dd HH:mm:ssZZ]: '2023-07-04 20:13:13+00:00'.y=365 days, mo=30 days
Subject Alternative Name	None
Certificate Policy OID	None
Use UTF-8 in policy notice text	<input checked="" type="checkbox"/> Use
PrintableString encoding in DN	<input type="checkbox"/> Use
LDAP DN order	<input type="checkbox"/> Use
Serial Number Octet Size	<input type="text" value="20"/>
Name Constraints, Permitted	<input type="text"/> <small>List of domain names, IPv4/IPv6 address/netmask pairs, DNS, URIs and RFC 822 Names. One per line. Examples (without quotes): 'example.com' '198.51.100.0/24' 'CN=Name,O=Company' '@example.com' 'uri:example.com' 'uri:.example.com'</small>
Name Constraints, Excluded	<input type="text"/> <small>Use 0.0.0.0/0 and ::0 to disallow certificates for all plain IP addresses. Use a single . to disallow all DNS names.</small>
CA Certificate	View Certificate
CA Alternate Cross Certificate Chains	None Used to construct end entity certificate chains with different root CAs for ACME enrollment.
CRL Specific Data	
Microsoft CA Compatibility Mode	<input type="checkbox"/> Use <small>Warning! Microsoft CA Compatibility Mode is irreversible.</small>
Authority Key ID	<input checked="" type="checkbox"/> Use <input type="checkbox"/> Critical
CRL Number	<input checked="" type="checkbox"/> Use <input type="checkbox"/> Critical
Issuing Distribution Point on CRLs	<input checked="" type="checkbox"/> Use <input type="checkbox"/> Critical
CA issuer URI	<input type="text"/>
Keep expired certificates on CRL	<input type="checkbox"/> Use
Use CRL partitions	<input type="checkbox"/> Use
CRL Expire Period (*y *mo *d *h *m)	<input type="text" value="1h"/> y=365 days , mo=30 days
CRL Issue Interval (*y *mo *d *h *m)	<input type="text" value="0m"/> y=365 days , mo=30 days
CRL Overlap Time (*y *mo *d *h *m)	<input type="text" value="0m"/> y=365 days , mo=30 days
Delta CRL Period (*y *mo *d *h *m)	<input type="text" value="0m"/> y=365 days , mo=30 days (0m, if no delta CRLs are issued)
Generate CRL Upon Revocation	<input type="checkbox"/> Use A fresh CRL or delta CRL is generated after revocation or reactivation of a certificate.
Allow changing revocation reason	<input type="checkbox"/> Use
Publishers	<input type="text"/>
Default CA defined validation data <small>Used as default values in certificate profiles using this CA</small>	
Default CRL Distribution Point	<input type="text" value="http://192.168.110.190:80/ejbca/publicweb/webd"/> Generate (used in CRL, and as default value)
Default CRL Issuer	<input type="text" value="CN=Universidad de las Fuerzas Armadas ESPE San"/> Generate (used in CRL, and as default value)
Default Freshest CRL Distribution Point	<input type="text"/> Generate (used in CRL, and as default value)
OCSF service Default URI	<input type="text" value="http://192.168.110.190:80/ejbca/publicweb/status"/> Generate
CA Issuer Default URI	<input type="text"/>

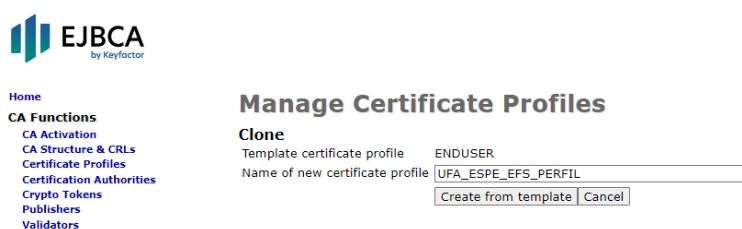
3. Crear Entidad Final Superadministrador.

3.1. Crear perfil de certificado

- 3.1.1. Desde las funciones de CA en la consola de administración, nos dirigimos a Perfiles de Certificados y clonamos el perfil existente ENDUSER, le asignamos el nombre UFA_ESPE_EFS_PERFIL.

Figura 25

Creación de perfil de certificado para Entidad Final Superadministrador



- 3.1.2. Configuramos el perfil de certificado como se muestra en la siguiente figura

Figura 26

Configuración de perfil de certificado para Entidad Final Superadministrador



Home

CA Functions

CA Activation
CA Structure & CRLs
Certificate Profiles
Certification Authorities
Crypto Tokens
Publishers
Validators

RA Functions

Add End Entity
End Entity Profiles
Search End Entities
User Data Sources

VA Functions

OCSP Responders

Supervision Functions

Approval Profiles
Approve Actions

System Functions

Roles and Access Rules
Remote Authentication
Services

System Configuration

CMP Configuration
SCEP Configuration
System Configuration

My Preferences

RA Web
Public Web

Edit

Certificate Profile: UFA_ESPE_EFS_PERFIL

Back to Certificate Profiles

Certificate Profile ID: 213175206

Type: End Entity Sub CA Root CA

Available Key Algorithms: DSA, ECDSA, RSA, Ed25519, Ed448

Available ECDSA curves: K-409 / sect409k1, K-571 / sect571k1, P-192 / prime192v1 / secp192r1, P-224 / secp224r1, P-256 / prime256v1 / secp256r1

Available Bit Lengths: No algorithm/curve with selectable key sizes selected.

Signature Algorithm: Inherit from issuing CA

Validity or end date of the certificate: Sy

ISO 8601 date: [yyyy-MM-dd HH:mm:ssZ]: 2023-07-04 20:23:37+00:00
(*y *mo *d *h *m *s) - y=365 days, mo=30 days

Validity Offset: Use...

Expiration Restrictions: Use...

Profile Description: Perfil de Certificado para Entidad Final Superadministrador Universidad de las Fuerzas Armadas ESPE

Permissions

Allow Validity Override: Allow

Allow Extension Override: Allow...

Allow certificate serial number override: Allow

Allow Subject DN Override by CSR: Allow

Allow Subject DN Override by End Entity Information: Allow

Allow Key Usage Override: Allow

Allow Backdated Revocation: Allow

Use Certificate Storage: Use (disable with caution)

Store Certificate Data: Use (see help for info on usage in combination with 'Use Certificate Storage')

X.509v3 extensions

Basic Constraints: Use... Critical

Authority Key ID: Use

Subject Key ID: Use

X.509v3 extensions

Key Usage: Use... Critical

Key Usage: Digital Signature Data encipherment CRL sign
 Non-repudiation Key agreement Encipher only
 Key encipherment Key certificate sign Decipher only

Extended Key Usage: Use... Critical

Any Extended Key Usage
CSN 369791 TLS client
CSN 369791 TLS server
client authentication
Code Signing
EAP over LAN (EAPOL)
EAP over PPP
ETSI TSL Signing
Email Protection
ICAO Deviation List Signing

Certificate Policies Use... Critical

X.509v3 extensions

Names: Use... Critical Search enabled (search enabled SAN use more storage)

Subject Alternative Name: Use... Critical

Issuer Alternative Name: Use... Critical

Subject Directory Attributes: Use

Name constraints: Use... Critical

X.509v3 extensions

CRL Distribution Points Use... Critical

Freshest CRL (a.k.a. Delta CRL DP): Use...

Authority Information Access Use...

Private Key Usage Period: Start offset... (*y *mo *d *h *m *s)
 Period length... (*y *mo *d *h *m *s)

QC Statements extension

Qualified Certificates Statements: Use... Critical

Other Extensions

OCSP No Check: Use

Microsoft Certificate Template Name: Add Value DomainController (only the name, not the actual template)

Use Microsoft ObjectSid Security Extension: Use

Card Number Extension: Use

CA/B Forum Organization Identifier: Use

ePassport

ICAO Document Type List: Use... Critical

Approval Settings

Add/Edit End Entity: None

Key Recovery: None

Revocation: None

Other Data

LDAP DN order: Use

Custom Subject DN Order: Use... Apply LDAP DN order settingValue (comma separated list of DN components)

CN postfix: Add Value (text appended after first CN field)

Subset of Subject DN: Restrict...

Subset of Subject Alt. Name: Restrict...

Available CAs: Any CA, ManagementCA, UFA_ESPE_ACR, UFA_ESPE_SANGOLQUI_ACS

Publishers: [dropdown]

Single Active Certificate Constraint: Use

Account Binding Namespace: [dropdown]

Save Cancel

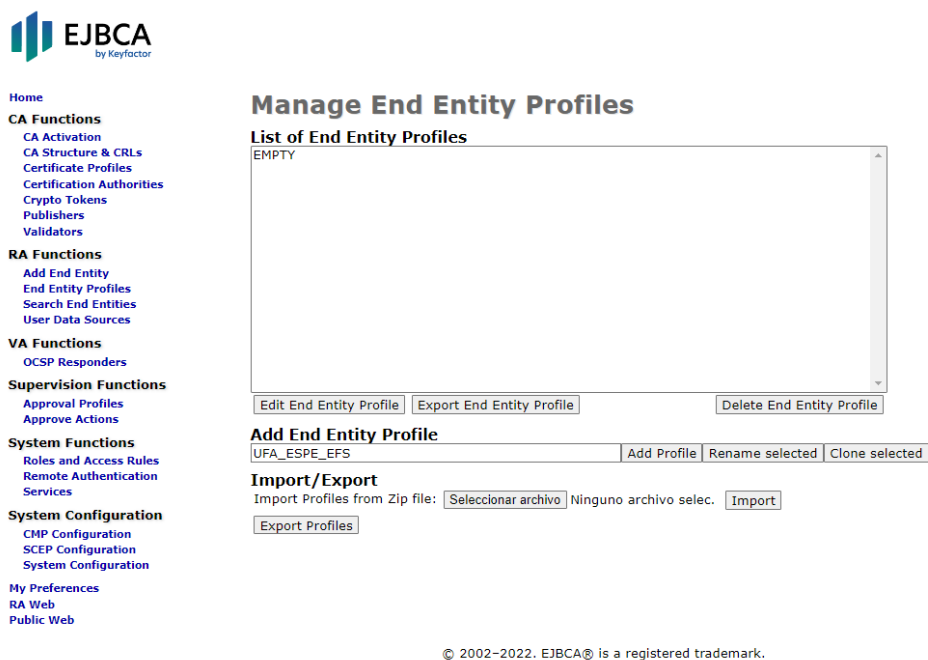
© 2002-2022. EJBCA® is a registered trademark.

3.2. Crear perfil de entidad final

- 3.2.1. Desde las funciones de RA, nos dirigimos a la opción de Perfiles de Entidad Final y agregamos el perfil de Entidad Final Superadministrador con el nombre UFA_ESPE_EFS

Figura 27

Creación Entidad Final Superadministrador



- 3.2.2. Configuramos el perfil de entidad final como se muestra en la siguiente figura

Figura 28

Configuración de Entidad Final Superadministrador



- Home
- CA Functions**
- CA Activation
- CA Structure & CRLs
- Certificate Profiles
- Certificate Authorities
- Crypto Tokens
- Publishers
- Validators
- RA Functions**
- Add End Entity
- End Entity Profiles
- Search End Entities
- User Data Sources
- VA Functions**
- OCSF Responders
- Supervision Functions**
- Approval Profiles
- Approve Actions
- System Functions**
- Roles and Access Rules
- Remote Authentication Services
- System Configuration**
- CMP Configuration
- SCEP Configuration
- System Configuration
- My Preferences**
- RA Web
- Public Web

Edit End Entity Profile

End Entity Profile: UFA_ESPE_EFS

Back to End Entity Profiles	
End Entity Profile ID	639762003
Username	<input type="text"/> <input type="checkbox"/> Auto-generated <input type="checkbox"/> Validation
Password (or Enrollment Code)	<input type="text"/> <input checked="" type="checkbox"/> Required <input type="checkbox"/> Auto-generated English letters and digits of length 8
Minimum password strength (bits)	0
Maximum number of failed login attempts	<input type="checkbox"/> Use Default: <input type="text"/> <input checked="" type="checkbox"/> Unlimited <input checked="" type="checkbox"/> Modifiable
Batch generation (clear text pwd storage)	<input type="checkbox"/> Use: Default = <input type="checkbox"/> Required
End Entity E-mail	<input checked="" type="checkbox"/> Use (Use only the domain part of the address, without the '@' character) <input type="text"/> espe.edu.ec <input checked="" type="checkbox"/> Required <input type="checkbox"/> Modifiable
Profile Description	<input type="text"/> Perfil de Entidad Final Superadministrador Universidad de las Fuerzas Armadas ESPE
Directives	
Reverse Subject DN and Subject Alt Name Checks	<input type="checkbox"/> Use
Allow merge DN for all interfaces	<input type="checkbox"/> Allow
Allow multi-valued RDNs	<input type="checkbox"/> Allow (do not use by default, only to be used in special cases)
Subject DN Attributes	
Select for Removal	Subject DN Attributes emailAddress, E-mail address in DN <input type="button" value="Add"/>
<input type="checkbox"/>	CN, Common name <input type="text"/> <input checked="" type="checkbox"/> Required <input checked="" type="checkbox"/> Modifiable <input type="checkbox"/> Validation
<input type="checkbox"/>	O, Organization ESPE <input checked="" type="checkbox"/> Required <input type="checkbox"/> Modifiable <input type="checkbox"/> Validation
<input type="checkbox"/>	C, Country (ISO 3166) EC <input checked="" type="checkbox"/> Required <input type="checkbox"/> Modifiable <input type="checkbox"/> Validation
<input type="button" value="Remove"/>	
Other Subject Attributes	
Subject Alternative Name	RFC 822 Name (e-mail address) <input type="button" value="Add"/>
Subject Directory Attributes	Date of birth (YYYYMMDD) <input type="button" value="Add"/>
Main Certificate Data	
Default Certificate Profile	UFA_ESPE_EFS_PERFIL
Available Certificate Profiles	OCSPSIGNER SERVER SUBCA UFA_ESPE_ACS_PERFIL UFA_ESPE_EFAR_PERFIL UFA_ESPE_EFE_PERFIL UFA_ESPE_EFS_PERFIL
Default CA	UFA_ESPE_SANGOLQUI_ACS
Available CAs	Any CA ManagementCA UFA_ESPE_ACR UFA_ESPE_SANGOLQUI_ACS
Default Token	P12 file
Available Tokens	User Generated P12 file BCFKS file JKS file PEM file
Other Certificate Data	
Custom certificate serial number	<input type="checkbox"/> Use
Certificate Validity Start Time	<input type="checkbox"/> Use: Value: <input type="text"/> <input checked="" type="checkbox"/> Modifiable (ISO 8601 date: [yyyy-MM-dd HH:mm:ssZ]: '2023-07-04 20:30:15+00:00' or days:hours:minutes)
Certificate Validity End Time	<input type="checkbox"/> Use: Value: <input type="text"/> <input checked="" type="checkbox"/> Modifiable (ISO 8601 date: [yyyy-MM-dd HH:mm:ssZ]: '2023-07-04 20:30:15+00:00' or days:hours:minutes)
Card number	<input type="checkbox"/> Use <input type="checkbox"/> Required
Name Constraints, Permitted	<input type="checkbox"/> Use <input type="checkbox"/> Required
Name Constraints, Excluded	<input type="checkbox"/> Use <input type="checkbox"/> Required
Custom certificate extension data	<input type="checkbox"/> Use
ETSI PSD2 QC Statement	<input type="checkbox"/> Use
CA/B Forum Organization Identifier	<input type="checkbox"/> Use Value: <input type="text"/> <input type="checkbox"/> Required <input checked="" type="checkbox"/> Modifiable
Other Data	
Number of allowed requests	<input type="checkbox"/> Use: Default = 1
Allow renewal before expiration	<input type="checkbox"/> Use: Days before expiration: -1
Revocation reason to set after certificate issuance	<input type="checkbox"/> Use Value: Active <input checked="" type="checkbox"/> Modifiable
Send Notification	<input type="checkbox"/> Use: Default = <input type="checkbox"/> Required <input type="button" value="Add"/>
Printing of user data	
Printer Name	<input type="checkbox"/> Use: Default = <input type="checkbox"/> Required Error no printer found.
Printed Copies	1
Current Template	No Printing template is uploaded.
Path to template (Must be in SVG format, max 2 MB)	<input type="button" value="Seleccionar archivo"/> Ninguno archivo selec. <input type="button" value="Upload Template"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

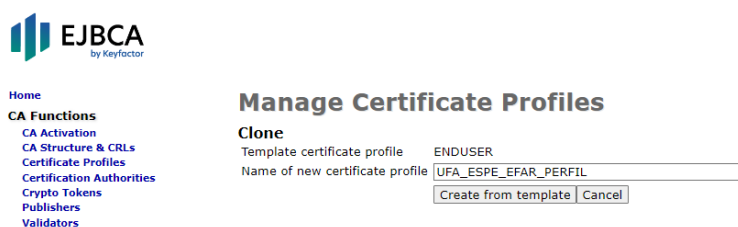
4. Crear Entidad Final Autoridad Registro.

4.1. Crear perfil de certificado

- 4.1.1. Desde las funciones de CA en la consola de administración, nos dirigimos a Perfiles de Certificados y clonamos el perfil existente ENDUSER, le asignamos el nombre UFA_ESPE_EFAR_PERFIL.

Figura 29

Creación de perfil de certificado para Entidad Final Autoridad Registro



- 4.1.2. Configuramos el perfil de certificado como se muestra en la siguiente figura

Figura 30

Configuración de perfil de certificado para Entidad Final Autoridad Registro



- Home
- CA Functions**
 - CA Activation
 - CA Structure & CRLs
 - Certificate Profiles
 - Certification Authorities
 - Crypto Tokens
 - Publishers
 - Validators
- RA Functions**
 - Add End Entity
 - End Entity Profiles
 - Search End Entities
 - User Data Sources
- VA Functions**
 - OCSP Responders
- Supervision Functions**
 - Approval Profiles
 - Approve Actions
- System Functions**
 - Roles and Access Rules
 - Remote Authentication
 - Services
- System Configuration**
 - CHP Configuration
 - SCP Configuration
 - System Configuration
- My Preferences**
 - RA Web
 - Public Web

Edit

Certificate Profile: UFA_ESPE_EFAR_PERFIL

[Back to Certificate Profiles](#)

Certificate Profile ID: 401095163

Type: End Entity Sub CA Root CA

Available Key Algorithms: DSA
ECDSA
RSA
Ed25519
Ed448

Available ECDSA curves: K-409 / sect409k1
K-571 / sect571k1
P-192 / prime192v1 / secp192r1
P-224 / secp224r1
P-256 / prime256v1 / secp256r1

Available Bit Lengths: No algorithm/curve with selectable key sizes selected.

Signature Algorithm: Inherit from issuing CA

Validity or end date of the certificate: 1y
ISO 8601 date: [yyyy-MM-dd HH:mm:ssZZ]: '2023-07-04 20:33:47+00:00'
 (*y *mo *d *h *m *s) - y=365 days, mo=30 days

Validity Offset: Use...

Expiration Restrictions: Use...

Profile Description: Perfil de Certificado para Autoridad Registro Universidad de las Fuerzas Armadas ESPE

Permissions

Allow Validity Override: Allow

Allow Extension Override: Allow...

Allow certificate serial number override: Allow

Allow Subject DN Override by CSR: Allow

Allow Subject DN Override by End Entity Information: Allow

Allow Key Usage Override: Allow

Allow Backdated Revocation: Allow

Use Certificate Storage: Use (disable with caution)

Store Certificate Data: Use (see help for info on usage in combination with 'Use Certificate Storage')

X.509v3 extensions

Basic Constraints: Use... Critical

Authority Key ID: Use

Subject Key ID: Use

X.509v3 extensions Usages

Key Usage: Use... Critical

Key Usage:

Digital Signature Data encipherment CRL sign

Non-repudiation Key agreement Encipher only

Key encipherment Key certificate sign Decipher only

Extended Key Usage: Use... Critical

Any Extended Key Usage

CSN 369791 TLS client
CSN 369791 TLS server
Client Authentication
Code Signing
EAP over LAN (EAPOL)
EAP over PPP
ETSI TSL Signing
Email Protection
ICAO Deviation List Signing

Certificate Policies: Use... Critical

X.509v3 extensions Names

Subject Alternative Name: Use... Critical Search enabled (search enabled SAN use more storage)

Issuer Alternative Name: Use... Critical

Subject Directory Attributes: Use...

Name Constraints: Use... Critical

X.509v3 extensions Validation data

CRL Distribution Points: Use... Critical

Freshest CRL (a.k.a. Delta CRL DP): Use...

Authority Information Access

Private Key Usage Period: Start offset... (*y *mo *d *h *m *s)
 Period length... (*y *mo *d *h *m *s)

QC Statements extension

Qualified Certificates Statements: Use... Critical

Other Extensions

OCSP No Check: Use

Microsoft Certificate Template Name: Add Value DomainController (only the name, not the actual template)

Use Microsoft ObjectSid Security Extension: Use

Card Number Extension: Use

CA/B Forum Organization Identifier: Use

ePassport

ICAO Document Type List: Use... Critical

Approval Settings

Add/Edit End Entity: None

Key Recovery: None

Revocation: None

Other Data

LDAP DN order: Use

Custom Subject DN Order: Use... Apply LDAP DN order settingValue
(comma separated list of DN components)

CN postfix: Add Value (text appended after first CN field)

Subset of Subject DN: Restrict...

Subset of Subject Alt. Name: Restrict...

Available CAs: Any CA
ManagementCA
UFA_ESPE_ACR
UFA_ESPE_SANGOLQUI_ACS

Publishers:

Single Active Certificate Constraint: Use

Account Binding Namespace:

4.2. Crear perfil de entidad final

- 4.2.1. Desde las funciones de RA, nos dirigimos a la opción de Perfiles de Entidad Final y agregamos el perfil de Entidad Final Autoridad Registro con el nombre UFA_ESPE_EFAR

Figura 31

Creación Entidad Final Autoridad Registro

EJBCA
by Keyfactor

Home
CA Functions
CA Activation
CA Structure & CRLs
Certificate Profiles
Certification Authorities
Crypto Tokens
Publishers
Validators
RA Functions
Add End Entity
End Entity Profiles
Search End Entities
User Data Sources
VA Functions
OCSP Responders
Supervision Functions
Approval Profiles
Approve Actions
System Functions
Roles and Access Rules
Remote Authentication Services
System Configuration
CMP Configuration
SCEP Configuration
System Configuration
My Preferences
RA Web
Public Web

Manage End Entity Profiles

List of End Entity Profiles

EMPTY
UFA_ESPE_EFS

Edit End Entity Profile | Export End Entity Profile | Delete End Entity Profile

Add End Entity Profile

UFA_ESPE_EFAR | Add Profile | Rename selected | Clone selected

Import/Export

Import Profiles from Zip file: Seleccionar archivo | Ninguno archivo selec. | Import

Export Profiles

© 2002-2022. EJBCA® is a registered trademark.

- 4.2.2. Configuramos el perfil de entidad final como se muestra en la siguiente figura

Figura 32

Configuración de Entidad Final Autoridad Registro



- Home
- CA Functions**
- CA Activation
- CA Structure & CRLs
- Certificate Profiles
- Certification Authorities
- Crypto Tokens
- Publishers
- Validators
- RA Functions**
- Add End Entity
- End Entity Profiles
- Search End Entities
- User Data Sources
- VA Functions**
- OCSF Responders
- Supervision Functions**
- Approval Profiles
- Approve Actions
- System Functions**
- Roles and Access Rules
- Remote Authentication Services
- System Configuration**
- CMP Configuration
- SCEP Configuration
- System Configuration
- My Preferences**
- RA Web
- Public Web

Edit End Entity Profile

End Entity Profile: UFA_ESPE_EFAR

Back to End Entity Profiles	
End Entity Profile ID	1595953593
Username	<input type="text"/> <input type="checkbox"/> Auto-generated <input type="checkbox"/> Validation
Password (or Enrollment Code)	<input type="text"/> <input checked="" type="checkbox"/> Required <input type="checkbox"/> Auto-generated English letters and digits of length 8
Minimum password strength (bits)	0
Maximum number of failed login attempts	<input type="checkbox"/> Use Default: <input type="text"/> <input type="checkbox"/> Unlimited <input checked="" type="checkbox"/> Modifiable
Batch generation (clear text pwd storage)	<input type="checkbox"/> Use: Default = <input type="checkbox"/> Required
End Entity E-mail	<input checked="" type="checkbox"/> Use (Use only the domain part of the address, without the '@' character) espe.edu.ec <input type="checkbox"/> Required <input checked="" type="checkbox"/> Modifiable
Profile Description	Perfil de Entidad Final Autoridad Registro Universidad de las Fuerzas Armadas ESPE
Directives	
Reverse Subject DN and Subject Alt Name Checks	<input type="checkbox"/> Use
Allow merge DN for all interfaces	<input type="checkbox"/> Allow
Allow multi-value RDNs	<input type="checkbox"/> Allow (do not use by default, only to be used in special cases)
Subject DN Attributes	
Select for Removal	Subject DN Attributes <input type="text" value="emailAddress, E-mail address in DN"/> <input type="button" value="Add"/>
<input type="checkbox"/>	CN, Common name <input type="text"/> <input checked="" type="checkbox"/> Required <input checked="" type="checkbox"/> Modifiable <input type="checkbox"/> Validation <input type="text"/>
<input type="checkbox"/>	O, Organization ESPE <input checked="" type="checkbox"/> Required <input type="checkbox"/> Modifiable <input type="checkbox"/> Validation <input type="text"/>
<input type="checkbox"/>	C, Country (ISO 3166) EC <input checked="" type="checkbox"/> Required <input type="checkbox"/> Modifiable <input type="checkbox"/> Validation <input type="text"/>
Other Subject Attributes	
Subject Alternative Name	RFC 822 Name (e-mail address) <input type="button" value="Add"/>
Subject Directory Attributes	Date of birth (YYYYMMDD) <input type="button" value="Add"/>
Main Certificate Data	
Default Certificate Profile	UFA_ESPE_EFAR_PERFIL
Available Certificate Profiles	<ul style="list-style-type: none"> ENDUSER OCSFSIGNER SERVER SUBCA UFA_ESPE_ACS_PERFIL UFA_ESPE_EFAR_PERFIL UFA_ESPE_EFE_PERFIL
Default CA	UFA_ESPE_SANGOLQUI_ACS
Available CAs	<ul style="list-style-type: none"> Any CA ManagementCA UFA_ESPE_ACR UFA_ESPE_SANGOLQUI_ACS
Default Token	P12 file
Available Tokens	<ul style="list-style-type: none"> User Generated P12 file BCFKS file JKS file PEM file
Other Certificate Data	
Custom certificate serial number	<input type="checkbox"/> Use
Certificate Validity Start Time	<input type="checkbox"/> Use: Value <input type="text"/> <input checked="" type="checkbox"/> Modifiable <small>(ISO 8601 date: [yyyy-MM-dd HH:mm:ssZ]: '2023-07-04 20:36:56+00:00' or days:hours:minutes)</small>
Certificate Validity End Time	<input type="checkbox"/> Use: Value <input type="text"/> <input checked="" type="checkbox"/> Modifiable <small>(ISO 8601 date: [yyyy-MM-dd HH:mm:ssZ]: '2023-07-04 20:36:56+00:00' or days:hours:minutes)</small>
Card number	<input type="checkbox"/> Use <input type="checkbox"/> Required
Name Constraints, Permitted	<input type="checkbox"/> Use <input type="checkbox"/> Required
Name Constraints, Excluded	<input type="checkbox"/> Use <input type="checkbox"/> Required
Custom certificate extension data	<input type="checkbox"/> Use
ETSI PSD2 QC Statement	<input type="checkbox"/> Use
CA/B Forum Organization Identifier	<input type="checkbox"/> Use Value <input type="text"/> <input type="checkbox"/> Required <input checked="" type="checkbox"/> Modifiable
Other Data	
Number of allowed requests	<input type="checkbox"/> Use: Default = 1
Allow renewal before expiration	<input type="checkbox"/> Use: Days before expiration: -1
Revocation reason to set after certificate issuance	<input type="checkbox"/> Use Value Active <input type="checkbox"/> Modifiable
Send Notification	<input type="checkbox"/> Use: Default = <input type="checkbox"/> Required <input type="button" value="Add"/>
Printing of user data	
Printer Name	<input type="checkbox"/> Use: Default = <input type="checkbox"/> Required Error no printer found.
Printed Copies	1
Current Template	No Printing template is uploaded.
Path to template (Must be in SVG format, max 2 MB)	<input type="button" value="Seleccionar archivo"/> Ninguno archivo selec. <input type="button" value="Upload Template"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

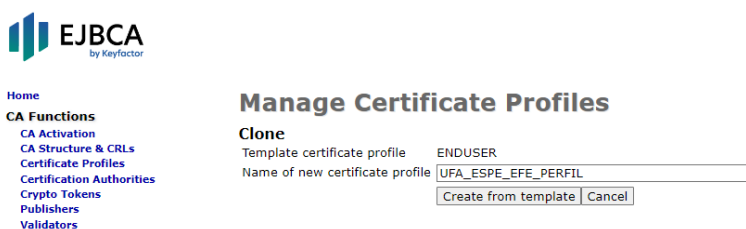
5. Crear Entidad Final Estudiante.

5.1. Crear perfil de certificado

- 5.1.1. Desde las funciones de CA en la consola de administración, nos dirigimos a Perfiles de Certificados y clonamos el perfil existente ENDUSER, le asignamos el nombre UFA_ESPE_EFE_PERFIL.

Figura 33

Creación de perfil de certificado para Entidad Final Estudiante



- 5.1.2. Configuramos el perfil de certificado como se muestra en la siguiente figura

Figura 34

Configuración de perfil de certificado para Entidad Final Estudiante



- Home
- CA Functions**
 - CA Activation
 - CA Structure & CRLs
 - Certificate Profiles
 - Certification Authorities
 - Crypto Tokens
 - Publishers
 - Validators
- RA Functions**
 - Add End Entity
 - End Entity Profiles
 - Search End Entities
 - User Data Sources
- VA Functions**
 - OCSF Responders
- Supervision Functions**
 - Approval Profiles
 - Approve Actions
- System Functions**
 - Roles and Access Rules
 - Remote Authentication Services
- System Configuration**
 - CHP Configuration
 - SCSP Configuration
 - System Configuration
- My Preferences**
 - RA Web
 - Public Web

Edit

Certificate Profile: UFA_ESPE_EFE_PERFIL

[Back to Certificate Profiles](#)

Certificate Profile ID: 1158641539

Type: End Entity Sub CA Root CA

Available Key Algorithms: DSA
ECDSA
RSA
E25519
Ed448

Available ECDSA curves: K-409 / sect409k1
K-571 / sect571k1
P-192 / prime192v1 / secp192r1
P-224 / secp224r1
P-256 / prime256v1 / secp256r1

Available Bit Lengths: No algorithm/curve with selectable key sizes selected.

Signature Algorithm: Inherit from issuing CA

Validity or end date of the certificate: Sy
ISO 8601 date: [yyyy-MM-dd HH:mm:ssZ]: '2023-07-04 20:39:19+00:00'
 (*y "mo "d "h "m "s) - y=365 days, mo=30 days

Validity Offset: Use...

Expiration Restrictions: Use...

Profile Description: Perfil de Certificado para Estudiante Universidad de las Fuerzas Armadas ESPE

Permissions

Allow Validity Override: Allow

Allow Extension Override: Allow...

Allow certificate serial number override: Allow

Allow Subject DN Override by CSR: Allow

Allow Subject DN Override by End Entity Information: Allow

Allow Key Usage Override: Allow

Allow Backdated Revocation: Allow

Use Certificate Storage: Use (disable with caution)

Store Certificate Data: Use (see help for info on usage in combination with 'Use Certificate Storage')

X.509v3 extensions

Basic Constraints: Use... Critical

Authority Key ID: Use

Subject Key ID: Use

X.509v3 extensions Usages

Key Usage: Use... Critical

Key Usage:

Digital Signature Data encipherment CRL sign

Non-repudiation Key agreement Encipher only

Key encipherment Key certificate sign Decipher only

Extended Key Usage

Use... Critical

Certificate Policies

Use... Critical

X.509v3 extensions Names

Subject Alternative Name: Use... Critical Search enabled (search enabled SAN use more storage)

Issuer Alternative Name: Use... Critical

Subject Directory Attributes: Use...

Name Constraints: Use... Critical

X.509v3 extensions Validation data

CRL Distribution Points Use... Critical

Use CA defined CRL Distribution Point: Use...

CRL Distribution Point URI: http://192.168.110.190:80/ejbc/publicweb/webdist/cer

CRL Issuer: CN=TestCA,O=AnaTom,C=SE

Freshest CRL (a.k.a. Delta CRL DP): Use...

Authority Information Access Use...

Use CA defined OCSF locator: Use...

OCSF Service Locator URI:

Use CA defined CA issuer: Use...

CA issuer URI: Add

Private Key Usage Period: Start offset... (*y "mo "d "h "m "s)
 Period length... (*y "mo "d "h "m "s)

QC Statements extension

Qualified Certificates Statements: Use... Critical

Other Extensions

OCSF No Check: Use

Microsoft Certificate Template Name: Add... Value: DomainController (only the name, not the actual template)

Use Microsoft ObjectSid Security Extension: Use

Card Number Extension: Use

CA/B Forum Organization Identifier: Use

ePassport

ICAO Document Type List: Use... Critical

Approval Settings

Add/Edit End Entity: UFA_ESPE_PAE

Key Recovery: None

Revocation: None

Other Data

LDAP DN order Use

Custom Subject DN Order: Use... Apply LDAP DN order setting/Value:
(comma separated list of DN components)

CN postfix: Add... Value: (text appended after first CN field)

Subset of Subject DN: Restrict...

Subset of Subject Alt. Name: Restrict...

Available CAs: Any CA
ManagementCA
UFA_ESPE_ACR
UFA_ESPE_SANGOLQUI_ACS

Publishers:

Single Active Certificate Constraint: Use

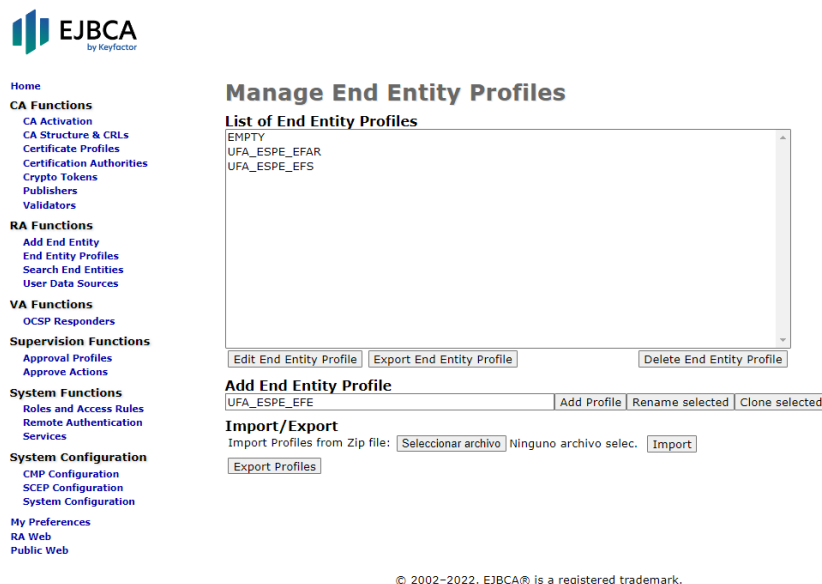
Account Binding Namespace:

5.2. Crear perfil de entidad final

- 5.2.1. Desde las funciones de RA, nos dirigimos a la opción de Perfiles de Entidad Final y agregamos el perfil de Entidad Final Estudiante con el nombre UFA_ESPE_EFE

Figura 35

Creación Entidad Final Estudiante



- 5.2.2. Este perfil se configura diferente a los otros perfiles, puesto que este se usará para emitir los certificados digitales a los estudiantes, aquí se definen que información debe proporcionar el estudiante para realizar su solicitud como el nombre de usuario, email institucional, ID institucional, nombres completos. Además, se configura los eventos para notificar al estudiante a través del email cuando su certificado ha sido creado o revocado. Configuramos el perfil de entidad final como se muestra en la siguiente figura

Figura 36

Configuración de Entidad Final Estudiante



- Home
- CA Functions
 - CA Activation
 - CA Structure & CRLs
 - Certificate Profiles
 - Certification Authorities
 - Crypto Tokens
 - Publishers
 - Validators
- RA Functions
 - Add End Entity
 - End Entity Profiles
 - Search End Entities
 - User Data Sources
- VA Functions
 - OCSP Responders
- Supervision Functions
 - Approval Profiles
 - Approval Actions
- System Functions
 - Rules and Access Rules
 - Remote Authentication Services
- System Configuration
 - CEP Configuration
 - SCEP Configuration
 - System Configuration
 - My Preferences
 - RA Web
 - Public Web

End Entity Profile: UFA_ESPE_EFE

Back to End Entity Profiles

End Entity Profile ID: 1555872988

Username: Auto-generated Validation

Password (or Enrollment Code): Auto-generated Required Modifiable

Minimum password strength (bits): 0 of length 8

Minimum number of failed login attempts: Use Default Unlimited Modifiable

Batch generation (clear text pvd storage): Use Default Required

End Entity E-mail: Use (Use only the domain part of the address, without the '@' character) Required Modifiable

Profile Description: Perfil de Entidad Final Estudiante Universidad de las Fuerzas Armadas ESPE

Directives

Reverse Subject DN and Subject Alt Name Checks: Use

Allow merge DN for all interfaces: Allow

Allow multi-value RDNs: Allow (do not use by default, only to be used in special cases)

Subject DN Attributes

Select for Removal:

Subject DN Attributes: emailaddress, E-mail address in DN Add

CA, Common name: Required Modifiable Validation [-1a-2a-60a4ef00a3]

emailaddress, E-mail address in DN: Required Modifiable Validation [-1a-2a-60a4ef00a3]

userid: Required Modifiable Validation [-1a-2a-60a4ef00a3]

O, Organization: ESPE Required Modifiable Validation

C, Country (ISO 3166): EC Required Modifiable Validation

userid: Required Modifiable Validation [-1a-2a-60a4ef00a3]

Other Subject Attributes

Subject Alternative Name: RFC 822 name (e-mail address) Add

Subject Directory Attributes: Date of birth (YYYYMMDD) Add

Main Certificate Data

Default Certificate Profile: UFA_ESPE_EFE_PERFIL

Available Certificate Profiles: ENDUSER, OCSPRESIGNER, SERVER, SOURCE, UFA_ESPE_ACS_PERFIL, UFA_ESPE_EFAR_PERFIL, UFA_ESPE_EFE_PERFIL

Default CA: UFA_ESPE_SANGOLQUI_ACS

Available CAs: Any CA, ManagementCA, UFA_ESPE_ACR, UFA_ESPE_SANGOLQUI_ACS

Default Token: P12 file

Available Tokens: User Generated, P12 file, BCFKS file, JKS file, PEM file

Other Certificate Data

Custom certificate serial number: Use

Certificate Validity Start Time: Use Value Modifiable

ISO 9601 date: [yyyy-MM-dd HH:mm:ssZ]: 2023-07-04 20:42:07+00:00 or days (hours:minutes)

Certificate Validity End Time: Use Value Modifiable

ISO 9601 date: [yyyy-MM-dd HH:mm:ssZ]: 2023-07-04 20:42:07+00:00 or days (hours:minutes)

Card number: Use Required

Name Constraints, Permitted: Use Required

Name Constraints, Excluded: Use Required

Custom certificate extension data: Use

ETSI PSD2 QC Statement: Use

CA/9 Forum Organization Identifier: Use Value Required Modifiable

Other Data

Number of allowed requests: Use Default = 1

Allow renewal before expiration: Use Days before expiration: -1

Revocation reason to set after certificate issuance: Use Value Active Modifiable

Use Default = Required

Notification Sender: soporte_pki@outlook.com

Notification Recipient: USER

Notification Events: STATUSNEW, STATUSFAILED, STATUSINITIALIZED, STATUSINPROCESS, STATUSGENERATED, STATUSREVOKED, STATUSHISTORICAL, STATUSKEYRECOVERY

Notification Subject: Certificado Digital

Notification Message: Estimado(a) Usuario(a)
Su Certificado Digital en ESPE PKI ha sido revocado, para más información contacte al administrador soporte_pki@outlook.com.

Notification Sender: soporte_pki@outlook.com

Notification Recipient: USER

Notification Events: STATUSNEW, STATUSFAILED, STATUSINITIALIZED, STATUSINPROCESS, STATUSGENERATED, STATUSREVOKED, STATUSHISTORICAL, STATUSKEYRECOVERY

Notification Subject: Solicitud Certificado Digital

Notification Message: Estimado(a) Usuario(a)
Su Certificado Digital en ESPE PKI ha sido aprobado con los siguientes datos:
Nombres y Apellidos: \$(CN)
ID: \$(UID)
Email: \$(userE)
Usuario: \$(USERNAME)
Contraseña: \$(PASSWORD)
Para obtener su Certificado Digital diríjase al siguiente enlace e Ingrese su usuario y contraseña provistos para descargar su certificado:
https://192.168.110.190/efca/ra/enroll?username.xhtml

Printing of user data: Use Default = Required

Printer Name: Error no printer found.

Printed Copies: 1

Current Template: No Printing template is uploaded.

Path to template (Must be in SVG format, max 2 MB): Ninguno archivo selec.

© 2002-2022. EJBCA® is a registered trademark.

Configuración de la arquitectura del servicio de firma electrónica.

Después de haber realizado la configuración de la Jerarquía PKI, se procede a configurar el sistema para que funcione de acuerdo a la arquitectura establecida. Para esto se deben configurar roles, reglas de acceso, perfiles de aprobación y emitir los certificados de administración del sistema para Autoridades de Registro y Superadministradores.

1. Configuración Rol Superadministrador

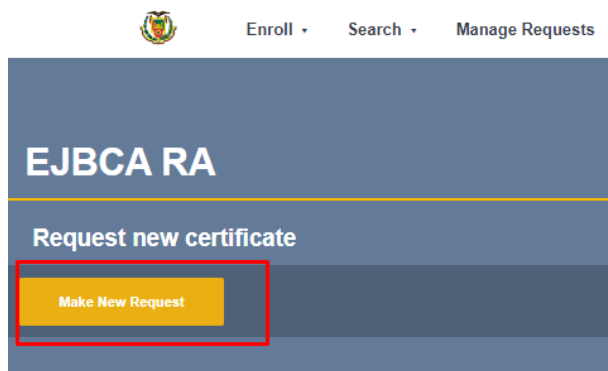
1.1. Emitir certificado digital de superadministrador

Este certificado servirá como medio de autenticación para poder acceder a todas las funciones del sistema.

- 1.1.1. Desde la consola de administración del RA, nos dirigimos a la opción de realizar una nueva solicitud.

Figura 37

Creación de Certificado Digital Superadministrador



- 1.1.2. Elegimos el perfil de certificado de superadministrador UFA_ESPE_EFS
- 1.1.3. Elegimos crear el par de claves criptográficas por la CA
- 1.1.4. Llenamos el formulario de la solicitud con los datos solicitados, proporcionar un usuario y contraseña.
- 1.1.5. Descargamos el certificado digital

Figura 38

Solicitud Certificado Digital Superadministrador

Make Request

Select Request Template

Certificate Type: Perfil de Entidad Final Superadministrador Universidad de las Fuerzas Armadas ESPE

Key-pair generation: By the CA Postpone [Show details](#)

Provide request info

Required Subject DN Attributes

CN, Common Name *

O, Organization = ESPE

C, Country (ISO 3166) = EC

Provide User Credentials

Username *

Enrollment code *

Confirm enrollment code *

Batch generation

Email

Confirm request

Issuer Distinguished Name	CN=Universidad de las Fuerzas Armadas ESPE Sangolqui,O=ESPE,C=EC
Subject Distinguished Name	C=EC,O=ESPE,CN=bjaramilloSA
Public Key Specification	ECDSA_P-256
Validity	5y

[Show details](#)

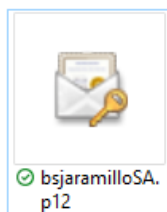
[Download PKCS#12](#)

[Reset](#)

© 2002–2022. EJBCA® is a registered trademark.

Figura 39

Descarga Certificado Digital Superadministrador



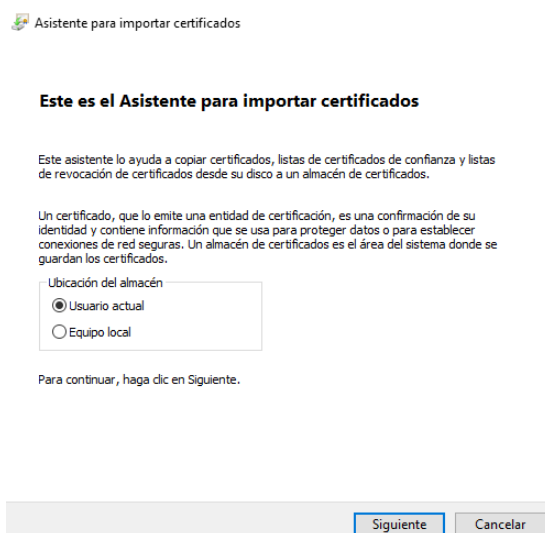
1.2. Configuración del rol superadministrador

1.2.1. Instalamos el Certificado Digital Superadministrador descargado anteriormente, haciendo doble clic sobre el mismo.

1.2.2. Se abre el asistente de Windows para importar certificados, elegimos el almacén donde se instalará el certificado.

Figura 40

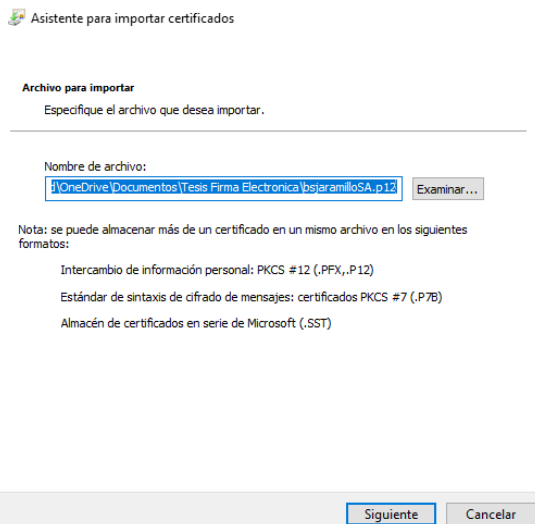
Selección de ubicación del almacén a instalar el certificado



1.2.3. Se selecciona el certificado digital a importar.

Figura 41

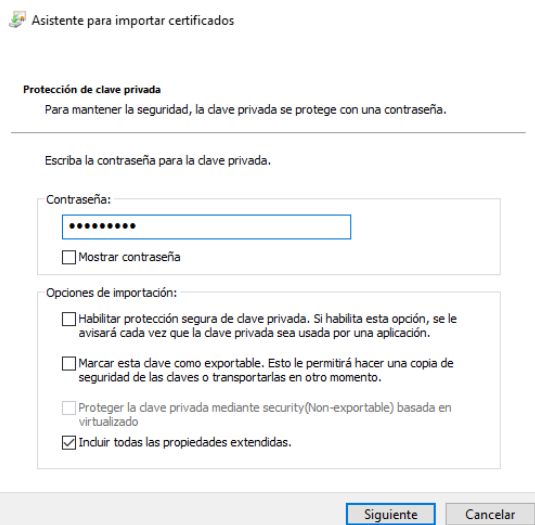
Selección del certificado a instalar



1.2.4. Ingresamos la contraseña del certificado.

Figura 42

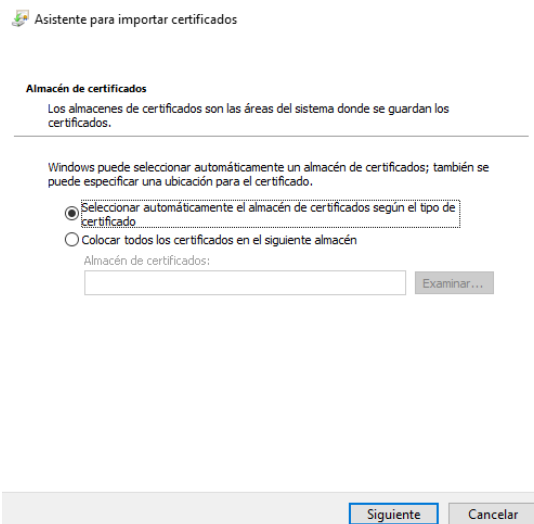
Verificación de contraseña del servidor



1.2.5. Dejamos marcada la opción para que se instale el certificado en el almacén según el tipo de certificado.

Figura 43

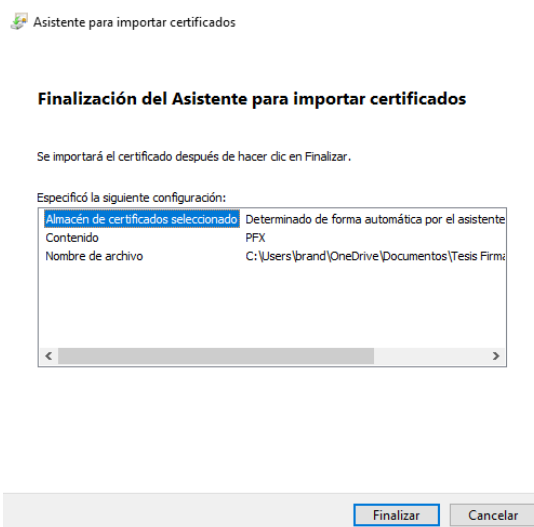
Selección automática del almacén donde se instalará el certificado



1.2.6. Finalizamos la importación.

Figura 44

Finalizando la instalación del certificado



1.2.7. Luego de haber instalado el certificado digital de superadministrador, cerramos y volvemos a acceder a la consola de administración, cuando el navegador nos pregunte que certificado usar, seleccionamos el recién instalado

Figura 45

Autenticación Superadministrador

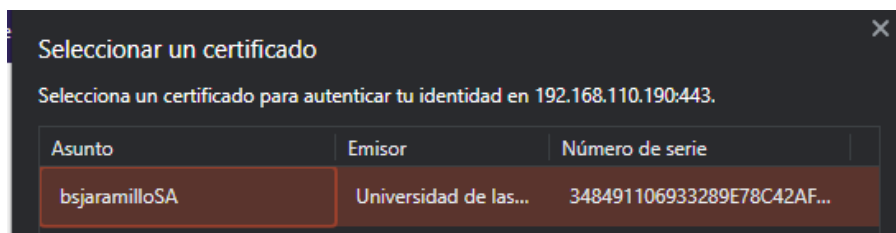


Figura 46

Verificando autenticación



1.2.8. Una vez autenticados, en la sección de Funciones del Sistema, nos dirigimos a la opción de Roles y Reglas de Acceso



Home

CA Functions

CA Activation
CA Structure & CRLs
Certificate Profiles
Certification Authorities
Crypto Tokens
Publishers
Validators

Roles Management

Role name

RA Styles

Role name	Members	Access Rules	RA Styles		
Public Access Role	Members	Access Rules	Default	Rename	Delete
Super Administrator Role	Members	Access Rules	espe	Rename	Delete

1.2.9. Hacemos clic en la opción de miembros del Rol Superadministrador y agregamos el usuario que creamos recientemente. Establecemos que el rol use los nombres completos para autenticar el usuario, es decir, que realice una comparación del nombre proporcionado en el certificado con el nombre que queremos que se valide.

Figura 47

Agregando el usuario al grupo de miembros de usuarios Superadministradores



Home
CA Functions
 CA Activation
 CA Structure & CRLs
 Certificate Profiles
 Certification Authorities
 Crypto Tokens
 Publishers
 Validators
RA Functions
 Add End Entity
 End Entity Profiles
 Search End Entities
 User Data Sources

Members

[Back to Roles Management](#)
[Edit Access Rules](#)

Role : Super Administrator Role

Match with	CA	Match Operator	Match Value	Description	Action
PublicAccessAuthenticationToken: Any transport (HTTP or HTTPS)				Initial rol	Add
CL: Username	-	Equal, case sens.	ejbca		Delete
PublicAccessAuthenticationToken: Any transport (HTTP or HTTPS)	-	Not Used		Initial rol	Delete
X509: CN, Common name	UFA_ESPE_SANGOLQUI_ACS	Equal, case sens.	SuperadministradorESPE	Rol de Acceso Superadministrador	Delete
X509: CN, Common name	UFA_ESPE_SANGOLQUI_ACS	Equal, case sens.	bsjaramilloSA	Rol de Acceso Superadministrador	Delete

1.2.10. Eliminamos el miembro de acceso público de este grupo

Figura 48

Eliminando el miembro de acceso público del grupo de Superadministradores



Home
CA Functions
 CA Activation
 CA Structure & CRLs
 Certificate Profiles
 Certification Authorities
 Crypto Tokens
 Publishers
 Validators
RA Functions
 Add End Entity
 End Entity Profiles
 Search End Entities
 User Data Sources
VA Functions

• Role member removed.

Members

[Back to Roles Management](#)
[Edit Access Rules](#)

Role : Super Administrator Role

Match with	CA	Match Operator	Match Value	Description	Action
PublicAccessAuthenticationToken: Any transport (HTTP or HTTPS)				Initial rol	Add
CL: Username	-	Equal, case sens.	ejbca		Delete
X509: CN, Common name	UFA_ESPE_SANGOLQUI_ACS	Equal, case sens.	SuperadministradorESPE	Rol de Acceso Superadministrador	Delete
X509: CN, Common name	UFA_ESPE_SANGOLQUI_ACS	Equal, case sens.	bsjaramilloSA	Rol de Acceso Superadministrador	Delete

1.2.11. Reiniciamos el servidor EJBCA para aplicar los cambios: sudo docker

restart espepki

1.2.12. Volvemos a ingresar a la consola de administración, autenticándonos con el certificado digital de Superadministrador.

1.2.13. Nos dirigimos a la opción de Roles y Reglas de Acceso, y eliminamos el rol de acceso público.

Figura 49

Eliminando rol de acceso público



Home
CA Functions
 CA Activation
 CA Structure & CRLs
 Certificate Profiles
 Certification Authorities
 Crypto Tokens
 Publishers
 Validators

Roles Management

Role name
 Super Administrator Role **Members** [Access Rules](#) RA Styles
 espe [Rename](#) [Delete](#)
[Add](#)

2. Configuración Rol Autoridad Registro

2.1. Emitir certificado digital de autoridad de registro

2.1.1. Desde la consola de administración del RA, nos dirigimos a la opción de realizar una nueva solicitud.

2.1.2. Elegimos el perfil de certificado de autoridad de registro
UFA_ESPE_EFAR

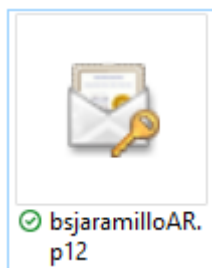
2.1.3. Elegimos crear el par de claves criptográficas por la CA

2.1.4. Llenamos el formulario de la solicitud con los datos solicitados,
proporcionar un usuario y contraseña.

2.1.5. Descargamos el certificado digital

Figura 50

Descarga Certificado Digital Autoridad Registro



2.2. Configuración Rol Autoridad Registro y reglas de acceso

2.2.1. Se procede a instalar el certificado de la misma forma que se instaló el certificado digital de superadministrador.

2.2.2. En la sección de Funciones del Sistema, nos dirigimos a la opción de Roles y Reglas de Acceso y creamos un nuevo rol con el nombre Autoridad Registro Rol

Figura 51

Creación Autoridad Registro Rol

2.2.3. Nos dirigimos a la opción de miembros del rol creado y agregamos el usuario creado anteriormente a este grupo de miembros

Figura 52

Agregando usuario al grupo de miembro del Rol Autoridad Registro

Match with	CA	Match Operator	Match Value	Description	Action
X509: Certificate serial number (Recommended)	ManagementCA				Add
X509: CN, Common name	UFA_ESPE_SANGOLQUI_ACS	Equal, case sens.	bsjaramilloARESPE	Miembro del rol AR	Delete
X509: CN, Common name	UFA_ESPE_SANGOLQUI_ACS	Equal, case sens.	sarajujoARESPE	Miembro del rol AR	Delete

2.2.4. Volvemos a la administración de roles, nos dirigimos a la opción de reglas de acceso del Rol Autoridad Registro y elegimos la plantilla de Administradores RA para aplicar estas reglas de acceso a este Rol Autoridad Registro. Además, seleccionamos que perfiles de entidades finales puede administrar este rol.

Figura 53

Configuración de reglas de acceso para el Rol Autoridad Registro



[Home](#)

CA Functions

[CA Activation](#)
[CA Structure & CRLs](#)
[Certificate Profiles](#)
[Certification Authorities](#)
[Crypto Tokens](#)
[Publishers](#)
[Validators](#)

RA Functions

[Add End Entity](#)
[End Entity Profiles](#)
[Search End Entities](#)
[User Data Sources](#)

VA Functions

[OCSP Responders](#)

Supervision Functions

[Approval Profiles](#)
[Approve Actions](#)

System Functions

[Roles and Access Rules](#)
[Remote Authentication Services](#)

System Configuration

[CMP Configuration](#)
[SCEP Configuration](#)
[System Configuration](#)

My Preferences

[RA Web](#)
[Public Web](#)

Edit Access Rules

[Back to Roles Management](#)

[Members](#)

[Advanced Mode](#)

Role : Autoridad Registro Role

Role Template	RA Administrators
Authorized CAs	All ManagementCA UFA_ESPE_ACR UFA_ESPE_SANGOLQUI_ACS
End Entity Rules	Approve End Entities Create End Entities Delete End Entities Edit End Entities Revoke End Entities View End Entities View History
End Entity Profiles	Available CAs in end entity profiles must also be authorized CAs in a role. All EMPTY UFA_ESPE_EFAR UFA_ESPE_EFE UFA_ESPE_EFS
Validators	All
Internal Keybinding Rules	Delete Modify View
Other Rules	View Audit Log
Save	

© 2002–2022. EJBCA® is a registered trademark.

3. Configuración Rol Estudiante

3.1. Creación Rol y reglas de acceso

3.1.1. Desde las Funciones del Sistema, nos dirigimos a la opción de roles y reglas de acceso, creamos un nuevo rol llamado Estudiante Rol.

Figura 54

Creación Estudiante Rol



[Home](#)

CA Functions

[CA Activation](#)
[CA Structure & CRLs](#)
[Certificate Profiles](#)
[Certification Authorities](#)
[Crypto Tokens](#)
[Publishers](#)
[Validators](#)

Roles Management

Role name

Role name	Members	Access Rules	RA Styles
Autoridad Registro Role	Members	Access Rules	espe Rename Delete
Estudiante Rol	Members	Access Rules	espe Rename Delete
Super Administrator Role	Members	Access Rules	espe Rename Delete

[Add](#)

- 3.1.2. Configuramos los miembros de este rol de manera que pueda ser accedido por cualquier persona a través del protocolo HTTPS.

Figura 55

Configuración de miembros para el Rol Estudiante



Home
CA Functions
 CA Activation
 CA Structure & CRLs
 Certificate Profiles
 Certification Authorities
 Crypto Tokens
 Publishers
 Validators
RA Functions

Members

[Back to Roles Management](#)
[Edit Access Rules](#)

Role : Estudiante Rol

Match with	CA	Match Operator	Match Value	Description	Action
PublicAccessAuthenticationToken: Confidential transport (HTTPS)				Miembro del Rol Estudiante	Add
PublicAccessAuthenticationToken: Confidential transport (HTTPS)	-	Not Used		Miembro del Rol Estudiante	Delete

- 3.1.3. Editamos las reglas de acceso de este rol, para que únicamente tenga acceso a las funciones para solicitar un nuevo certificado y descargarlo, para ello tenemos que acceder al modo avanzado de edición de reglas de acceso

Figura 56

Configuración reglas de acceso del Rol Estudiante



Home
CA Functions
 CA Activation
 CA Structure & CRLs
 Certificate Profiles
 Certification Authorities
 Crypto Tokens
 Publishers
 Validators
RA Functions
 Add End Entity
 End Entity Profiles
 Search End Entities
 User Data Sources
VA Functions
 OSCP Responders
Supervision Functions
 Approval Profiles
 Approve Actions
System Functions
 Roles and Access Rules
 Remote Authentication
 Services
System Configuration
 CMP Configuration
 SCEP Configuration
 System Configuration
My Preferences
 RA Web
 Public Web

Edit Access Rules

[Back to Roles Management](#)

[Members](#)

[Basic Mode](#)

[Summary](#)

Role : Estudiante Rol

Role Based Access Rules

/ Allow Deny Inherit (Deny)
 /administrator/ Allow Deny Inherit

Regular Access Rules

/ca_functionality/ Allow Deny Inherit
 /ca_functionality/activate_ca/ Allow Deny Inherit
 /ca_functionality/approve_caaction/ Allow Deny Inherit
 /ca_functionality/create_certificate/ Allow Deny Inherit
 /ca_functionality/create_crl/ Allow Deny Inherit
 /ca_functionality/edit_approval_profiles/ Allow Deny Inherit
 /ca_functionality/edit_blacklist/ Allow Deny Inherit
 /ca_functionality/edit_ca/ Allow Deny Inherit
 /ca_functionality/edit_certificate_profiles/ Allow Deny Inherit
 /ca_functionality/edit_publisher/ Allow Deny Inherit
 /ca_functionality/edit_validator/ Allow Deny Inherit
 /ca_functionality/renew_ca/ Allow Deny Inherit
 /ca_functionality/use_approval_request_id/ Allow Deny Inherit
 /ca_functionality/use_username/ Allow Deny Inherit
 /ca_functionality/view_approval_profiles/ Allow Deny Inherit
 /ca_functionality/view_ca/ Allow Deny Inherit
 /ca_functionality/view_certificate/ Allow Deny Inherit
 /ca_functionality/view_certificate_profiles/ Allow Deny Inherit
 /ca_functionality/view_publisher/ Allow Deny Inherit
 /ca_functionality/view_validator/ Allow Deny Inherit
 /ra_functionality/ Allow Deny Inherit
 /ra_functionality/approve_end_entity/ Allow Deny Inherit
 /ra_functionality/create_end_entity/ Allow Deny Inherit
 /ra_functionality/delete_end_entity/ Allow Deny Inherit
 /ra_functionality/edit_end_entity/ Allow Deny Inherit
 /ra_functionality/edit_end_entity_profiles/ Allow Deny Inherit
 /ra_functionality/edit_user_data_sources/ Allow Deny Inherit
 /ra_functionality/keyrecovery/ Allow Deny Inherit
 /ra_functionality/revoke_end_entity/ Allow Deny Inherit
 /ra_functionality/view_approvals/ Allow Deny Inherit
 /ra_functionality/view_end_entity/ Allow Deny Inherit
 /ra_functionality/view_end_entity_history/ Allow Deny Inherit
 /ra_functionality/view_end_entity_profiles/ Allow Deny Inherit
 /services/edit/ Allow Deny Inherit
 /services/view/ Allow Deny Inherit
 /system_functionality/ Allow Deny Inherit
 /system_functionality/edit_administrator_privileges/ Allow Deny Inherit
 /system_functionality/edit_available_custom_certificate_extensions/ Allow Deny Inherit
 /system_functionality/edit_available_extended_key_usages/ Allow Deny Inherit
 /system_functionality/edit_systemconfiguration/ Allow Deny Inherit
 /system_functionality/view_administrator_privileges/ Allow Deny Inherit
 /system_functionality/view_available_custom_certificate_extensions/ Allow Deny Inherit
 /system_functionality/view_available_extended_key_usages/ Allow Deny Inherit
 /system_functionality/view_systemconfiguration/ Allow Deny Inherit

CA Access Rules

/ca/ Allow Deny Inherit
 /ca/ManagementCA/ Allow Deny Inherit
 /ca/UFA_ESPE_ACR/ Allow Deny Inherit
 /ca/UFA_ESPE_SANGOLQUIT_ACS/ Allow Deny Inherit

Validator Access Rules

/validator/ Allow Deny Inherit

End Entity Profile Access Rules

/entityprofilesrules/ Allow Deny Inherit
 /entityprofilesrules/EHPTV/ Allow Deny Inherit
 /entityprofilesrules/EHPTV/approve_end_entity/ Allow Deny Inherit
 /entityprofilesrules/EHPTV/create_end_entity/ Allow Deny Inherit
 /entityprofilesrules/EHPTV/delete_end_entity/ Allow Deny Inherit
 /entityprofilesrules/EHPTV/edit_end_entity/ Allow Deny Inherit
 /entityprofilesrules/EHPTV/revoke_end_entity/ Allow Deny Inherit
 /entityprofilesrules/EHPTV/view_end_entity/ Allow Deny Inherit
 /entityprofilesrules/EHPTV/view_end_entity_history/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFAR/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFAR/approve_end_entity/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFAR/create_end_entity/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFAR/delete_end_entity/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFAR/edit_end_entity/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFAR/revoke_end_entity/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFAR/view_end_entity/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFAR/view_end_entity_history/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFE/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFE/approve_end_entity/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFE/create_end_entity/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFE/delete_end_entity/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFE/edit_end_entity/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFE/revoke_end_entity/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFE/view_end_entity/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFE/view_end_entity_history/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFS/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFS/approve_end_entity/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFS/create_end_entity/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFS/delete_end_entity/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFS/edit_end_entity/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFS/revoke_end_entity/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFS/view_end_entity/ Allow Deny Inherit
 /entityprofilesrules/UFA_ESPE_EFS/view_end_entity_history/ Allow Deny Inherit

4. Creación Perfil Aprobación Estudiante para la emisión de certificados digitales de estudiantes

Este perfil de aprobación sirve para tener un mejor control en la emisión de estos certificados, de manera que, cuando un estudiante realice una nueva solicitud para emitir su certificado digital, esta solicitud esté a la espera de que una autoridad de registro valide los datos proporcionados por el estudiante y apruebe esta solicitud solo en el caso de ser válido.

- 4.1. Desde las Funciones de Supervisión, nos dirigimos a la opción de perfiles de aprobación y creamos un nuevo perfil con el nombre UFA_ESPE_APE

Figura 57

Creación Perfil Aprobación Estudiante

The screenshot shows the EJBCA web interface. On the left is a navigation menu with the following items: Home, CA Functions, CA Activation, CA Structure & CRLs, Certificate Profiles, Certification Authorities, Crypto Tokens, Publishers, and Validators. The main content area is titled 'Manage Approval Profiles' and contains a 'List of Approval Profiles' table. The table has two columns: 'Approval profile name' and 'Actions'. The first row contains the profile name 'UFA_ESPE_PAE' and the actions 'View', 'Edit', 'Delete', 'Rename', and 'Clone'. Below the table, there is an 'Add' button.

Approval profile name	Actions
UFA_ESPE_PAE	View Edit Delete Rename Clone
	Add

- 4.2. Editamos este perfil de aprobación, en el tipo de perfil establecemos aprobación particionada.
- 4.3. La establecemos la expiración de la solicitud en siete días.
- 4.4. En los pasos de aprobación, llenamos los campos necesarios y establecemos los roles a los cuales se les asignará dicha solicitud para su revisión y aprobación, en este caso, el Rol Autoridad Registro
- 4.5. Agregamos una notificación de usuario, para notificar el estado de la solicitud cada vez que esta cambie.

Figura 58

Configuración Perfil Aprobación Estudiante



Home

CA Functions

CA Activation
CA Structure & CRLs
Certificate Profiles
Certification Authorities
Crypto Tokens
Publishers
Validators

RA Functions

Add End Entity
End Entity Profiles
Search End Entities
User Data Sources

VA Functions

OCSF Responders

Supervision Functions

Approval Profiles
Approve Actions

System Functions

Roles and Access Rules
Remote Authentication
Services

System Configuration

CMP Configuration
SCEP Configuration
System Configuration

My Preferences

RA Web
Public Web

Edit

Approval Profile: UFA_ESPE_PAE

Back to Approval Profiles	
Approval Profile ID	2104446703
Approval Profile Type	Partitioned Approval
Request Expiration Period (*y *mo *d *h *m)	7d y=365 days, mo=30 days
Approval Expiration Period (*y *mo *d *h *m)	7d y=365 days, mo=30 days
Max Extension Time (*y *mo *d *h *m)	0d y=365 days, mo=30 days. The maximum time an expired request may be extended for. Set to 0d to disallow request extension.
Allow Self Approved Request Editing	<input type="checkbox"/> Administrator will be able to edit requests without approval from an additional administrator.

Approval Steps:

Step: 1

Partition		Delete Partition
Name: Solicitud Certificado Digital		Add notification
Roles which may approve this partition:		Remove user notification
	Anybody Super Administrator Role Autoridad Registro Role	
Roles which may view this partition:	Anybody Super Administrator Role Autoridad Registro Role	
Datos Validos:	<input type="checkbox"/>	Remove Field
Observación:		Remove Field
User notification message email sender:	soporte_pki@outlook.com	
User notification message subject:	Estado Solicitud Certificado Digital	
User notification message body:	Estimado(a) Usuario(a) Se notifica el estado de su solicitud: Tipo solicitud: New Digital Certificate Estado solicitud: \${approvalRequest.WORKFLOWSTATE} Puede verificar el estado de su solicitud visitando el siguiente enlace: https://192.168.110.190/ejbca/ra/enrollwithrequestid.xhtml?requestId=\${approvalRequest.ID}	
Check Box		
Label:		
Add Field		
		Add Partition Delete Step
Approval will automatically execute after the final step has been approved.		
		Add Step
Save Cancel		

© 2002–2022. EJBCA® is a registered trademark.

4.6. Asignamos este perfil de aprobación, al perfil de certificado de estudiante
UFA_ESPE_EFE_PERFIL

4.6.1. Desde las funciones de CA, nos dirigimos a la opción de perfiles de
certificados y editamos el perfil UFA_ESPE_EFE_PERFIL

- 4.6.2. En la sección de Configuración de Aprobación, en el campo
Agregar/Editar Entidad Final, seleccionamos el perfil de aprobación
UFA_ESPE_PAE

Figura 59

Asignación del Perfil Aprobación Estudiante al Perfil de Certificado Estudiante

Approval Settings	
Add/Edit End Entity	UFA_ESPE_PAE ▼
Key Recovery	None ▼
Revocation	None ▼

Capacitación de usuarios.

Para capacitar a los estudiantes, de manera que puedan obtener un certificado digital sin antes haber utilizado la plataforma, se ha puesto a disposición un video tutorial y documento PDF como manual del usuario final. Para esto, se ha actualizado el manual de usuario propuesto por el proyecto “Transición, operación y mejora del servicio de firma electrónica del ESPE-CERT en el Departamento de Ciencias de la Computación utilizando ITIL V4”. Este manual se ha actualizado de acuerdo a los nuevos procedimientos establecidos en este proyecto. Este manual de usuario, contiene los pasos que se debe seguir para solicitar y obtener un nuevo certificado digital (ver anexo 1). Además, se muestra el proceso que se debe seguir para firmar electrónicamente un documento, utilizando el certificado digital. El video del manual de usuario se encuentra disponible en el siguiente enlace:

https://youtu.be/r_KgaXaGbvM.

Operación y pruebas del servicio.

El servicio se encuentra operando en el laboratorio H402 del ESPE CERT en Sangolquí, con la disponibilidad para ser usado por la comunidad universitaria de la misma sede y la sede Latacunga, a través de la intranet de la ESPE.

En una primera fase de pruebas, realizado con tres cursos de estudiantes pertenecientes al DCCO de la Sede Sangolquí, siendo un total de 40 estudiantes, se logró

emitir certificados digitales para esta pequeña muestra sin problemas de saturación del servicio o relacionados. Sin embargo, se tuvo problemas para enviar notificaciones del proceso de emisión del certificado digital, a través del correo electrónico, puesto que se está usando el servicio de correo electrónico Outlook. Al enlazar este servicio, con el sistema de la firma electrónica, se obtuvo bloqueos de la cuenta de email, provocando que las notificaciones no se entregasen a los estudiantes. Por ello, para continuar con la fase de pruebas, se solicitó un correo electrónico institucional a la Unidad de Tecnologías, que permita el envío de correos masivos sin limitaciones o bloqueos.

Análisis de certificación

Objetivos

- Determinar los requisitos técnico-legales para la certificación del Servicio de firma digital con las características diseñadas e implantado en el ESPE-CERT para la comunidad de la ESPE sede Latacunga.

Alcance

Realizar un análisis de certificación del servicio de firma electrónica, implantado en el ESPE CERT, en un plazo de 7 días desde el inicio del análisis, de manera que se pueda determinar los requisitos técnicos y legales en concordancia con lo establecido por los organismos de control gubernamental, para obtener la certificación.

Indicadores de cumplimiento

- Determinación de los requisitos legales
- Determinación de los requisitos técnicos
- Tiempo de entrega

Recursos

- Humanos: Se dispone de un estudiante a cargo del proyecto de titulación y del docente tutor del mismo.

- Financieros: No se requiere de recursos financieros.
- Hardware: Computadora personal.
- Software: Zoom
- Conocimientos: Investigación de campo.

Actividades a realizar

El siguiente cronograma indica todas las actividades a realizar, necesarias para realizar el análisis de certificación.

Tabla 5

Actividades para el análisis de certificación del servicio de firma electrónica

Tarea	Responsable	Duración	Comienzo	Fin
Visita al organismo de control gubernamental de certificación (ARCOTEL).	Estudiante	1 días	5 jun	5 jun
Investigar de los requisitos técnicos y legales de certificación.	Estudiante	2 días	6 jun	7 jun
Análisis de certificación.	Estudiante	4 días	8 jun	11 jun

Ejecución de actividades

Visita al organismo de control gubernamental de certificación (ARCOTEL).

Como primer paso para realizar el análisis de la certificación, se realizó una visita a las oficinas de ARCOTEL, que es el organismo de control gubernamental, que se encarga de otorgar la acreditación a entidades de certificación de la información, por lo que se acudió a ella, para obtener información acerca del proceso y los requisitos de certificación.

Dentro de las oficinas de la ARCOTEL, se acudió al centro de atención al cliente, donde una persona encargada, atendió a la solicitud de información requerida. Durante esta charla se dio a conocer, que los requisitos técnicos y legales se encuentran disponibles en el portal web de la ARCOTEL. Además, se puso a disposición otros medios para obtener más información al respecto, tales como, una solicitud de información al Director Ejecutivo de la ARCOTEL y reuniones a través de Zoom con personal administrativo de la institución.

Investigar los requisitos técnicos y legales de certificación.

Luego de la visita a las oficinas de la ARCOTEL, se procedió a investigar los requisitos técnicos y legales dentro del portal web de la ARCOTEL, el mismo que se encuentra en el siguiente enlace: <https://www.arcotel.gob.ec/>. Dentro de este portal, se encontró la sección “Requisitos: ENTIDADES DE CERTIFICACIÓN”. Esta sección describe los requisitos necesarios que se debe presentar para obtener la certificación, siendo un total de 12 literales, entre requisitos técnicos y legales (ver anexo 2).

Luego de realizar una revisión preliminar de los requisitos técnicos y legales, se logró tener una visión general acerca del proceso de certificación, sin embargo, los requisitos técnicos no son lo suficientemente claros o abarca muchas cosas y no hay mayor especificación disponible, por lo que se determinó que es necesario mayor información acerca de los mismos. Para ello, se solicitó una reunión por medio de Zoom, con personal administrativo de la ARCOTEL, para obtener mayor información acerca de los requisitos técnicos. Como resultado de esta reunión, se pudo obtener una mejor explicación cada uno de los requisitos técnicos presentados.

Especificación requisitos técnicos.

Se pudo obtener un mejor detalle acerca de la documentación técnica necesaria para la certificación. La información que se presentará a continuación, es la documentación mínima que la institución debe presentar para poder obtener la certificación, según se esclareció en la reunión mencionada (ver anexo 2).

Análisis de certificación.

Después de realizar la investigación acerca de los requisitos de certificación, se presenta el siguiente análisis, en el que se presenta un resumen general y conclusiones acerca de los mismos.

Análisis requisitos legales.

En cuanto a la documentación legal que se debe presentar, no existe mayor complejidad para generarla, sin embargo, en ciertos requisitos se especifica que no se deben presentar en el caso de instituciones públicas, como lo es esta institución; esto también se explicó en la reunión que se realizó por medio de Zoom, estos requisitos son:

- Copia certificada e inscrita en el Registro Mercantil (excepto las instituciones públicas) del nombramiento del representante legal: No aplica para la ESPE.
- Copia certificada debidamente registrada en el Registro Mercantil, de la escritura de constitución de la empresa unipersonal o compañía y reformas en caso de haberlas (excepto las instituciones públicas): No aplica para la ESPE, pero se debe presentar un decreto oficial de creación o algún documento emitido por el estado, donde se constituya a la ESPE como Universidad.
- Original del certificado de cumplimiento de obligaciones emitido por la Superintendencia de Compañías o Bancos y Seguros según corresponda, a excepción de las instituciones del Estado: No aplica para la ESPE.
- Información que demuestre la capacidad económica y financiera para la prestación de servicios de certificación de información y servicios relacionados: En el caso de este requisito, la ESPE, al ser una institución pública que depende de los fondos del estado, para demostrar la solvencia económica, debe presentar certificados emitidos por el Ministerio de Finanzas, en el que se demuestre que se cuenta con los recursos asignados o presupuestados para la institución, para cubrir todos los

gastos necesarios que pueda incurrir el proyecto de acreditación, como pueden ser, el costo de la acreditación, la garantía de acreditación, recursos humanos y la adquisición de la infraestructura de TI para la implementación del servicio de firma electrónica.

Análisis requisitos técnicos.

Como bien se menciona en la presentación de los requisitos técnicos, esta documentación es lo mínimo que se debería presentar para el proceso de acreditación. Por lo que se intuye, que el servicio de firma electrónica actualmente implantado, como se muestra en **Figura 5**, requiere de una arquitectura del servicio más robusta, con procedimientos de seguridad más rigurosos y una alta disponibilidad del servicio.

Para garantizar una alta disponibilidad del servicio, se requiere que algunos de los servicios internos de la PKI, como el RA y VA, se encuentren distribuidos en múltiples servidores. Este tipo de arquitectura con estas características, se encuentran disponibles en la versión empresarial del software EJBCA. El servicio implantado actualmente, como se ve en la **Figura 5**, permite implementar estos servicios en un único servidor, lo que podría ocasionar problemas en el servicio cuando se disponga el mismo para toda la comunidad universitaria. Por lo cual se plantea la posibilidad de adquirir la versión empresarial del software usado para el servicio de firma electrónica.

Análisis de presupuesto para la certificación.

Luego de realizar una investigación de los requisitos y del proceso de certificación, se realiza este análisis de presupuesto, en el que se determina un costo total estimado de inversión, que se necesita para que este servicio se encuentre legalmente constituido y acreditado.

En primer lugar, se tiene el costo de la acreditación, es decir el valor que se tiene que pagar para obtener el título de Entidad de Certificación de la Información, este valor es de \$ 22,000. Luego se tiene que disponer de un valor de garantía, que, como su nombre lo indica,

sirve como garantía para cubrir daños o perjuicios que se pudiesen presentar a los clientes del servicio de firma electrónica, este valor es de \$ 400,000.

En vista de que se plantea la posibilidad de adquirir la versión empresarial del software para la PKI, se realizó una reunión una persona que trabaja en la empresa que desarrolla este software, para obtener un costo estimado del software EJBCA empresarial. En esta reunión se determinó dos valores correspondientes al paquete completo del software EJBCA, y la licencia o soporte empresarial. El paquete completo del software EJBCA, tiene un valor de \$ 20,000, esto incluye, además, un HSM. La licencia o soporte empresarial, tiene un valor de \$ 24,000, esta licencia tiene un tiempo de validez de un año, lo que significa que se debe renovar anualmente y el costo de la renovación equivale al costo de adquisición, es decir, \$ 24,000.

Tabla 6

Resumen de presupuesto de certificación

Detalle	Costo	Renovación
Acreditación	\$ 22,000	No
Garantía de acreditación	\$ 400,000	No
Paquete software completo EJBCA y un HSM (opcional)	\$ 20,000	No
Licencia EJBCA (opcional)	\$ 24,000	Si (Anual)
Total	\$ 466,000	

El costo total de inversión, en el primer año de operación del servicio, tiene un estimado de \$466,000, como se resume en la **Tabla 6**. Este costo es estimado, puesto que no se considera la adquisición adicional de infraestructura de TI ni recursos humanos.

Capítulo IV

Análisis técnico de pre certificación

Objetivos

- Evaluación técnico informática de pre certificación del servicio de firma digital para la ESPE sede Latacunga.

Alcance

Realizar una evaluación técnico informática del servicio de firma electrónica, implantado y operando en el ESPE CERT, acorde a los requisitos técnicos de certificación, de manera que se pueda determinar si el servicio cumple con el nivel técnico requerido. La evaluación se considerará terminada cuando se presenten los resultados de la evaluación y se presente un informe con las no conformidades y recomendaciones de mejora.

Indicadores de cumplimiento

- Resultados de la evaluación
- Informe de no conformidades
- Recomendaciones de mejora
- Tiempo de entrega

Recursos

- Humanos: Se dispone de un estudiante a cargo del proyecto de titulación y del docente tutor del mismo.
- Hardware: Computadora personal.

Actividades a realizar

El siguiente cronograma indica las actividades a realizar, necesarias para realizar la evaluación técnico informático del servicio.

Tabla 7

Actividades para la evaluación técnico informático del servicio de firma electrónica

Actividad	Responsable	Duración	Comienzo	Fin
Elaboración del plan de investigación de campo.	Estudiante	2 días	12 jul	13 jul
Ejecución del plan de investigación de campo.	Estudiante	3 días	14 jul	16 jul
Informe de las no conformidades y las recomendaciones de mejora.	Estudiante	1 día	17 jul	18 jul

Ejecución de actividades

Elaboración del plan de investigación de campo.

Objetivo.

Evaluar técnica e informáticamente el servicio de firma electrónica implementado en el ESPE CERT, con el fin de determinar si cumple con los requisitos técnicos de certificación establecidos y garantizar su nivel de cumplimiento.

Marco teórico.

El proceso de implementación del servicio de firma electrónica, presentado en Implantación del servicio de firma electrónica, será parte fundamental de la literatura de esta investigación, así como los requisitos técnicos de certificación que se determinaron en Análisis de certificación. Revisar la literatura de estos dos aspectos en conjunto, proporcionarán el conocimiento necesario para llevar a cabo esta investigación.

Diseño de la investigación.

El diseño de esta investigación se compone de la siguiente manera:

- Enfoque metodológico: Estudio de evaluación técnico informática.
- Tipo de estudio: Descriptivo y comparativo.

- Muestra: Esta investigación no tiene por objeto realizar un estudio social, por lo que no se define una muestra de usuarios.

Procedimiento de recolección de datos.

La metodología para recolectar datos en esta investigación, se realizará a través:

- Observación directa: Un método que consiste en realizar observaciones directas de la implantación del servicio, así como su funcionamiento, analizando su rendimiento, funcionalidades, arquitectura, entre otros.

Análisis de datos.

Una vez recolectados los datos, el análisis de los mismos se realizará a través de una comparación entre, las observaciones realizadas, y, los requisitos técnicos de certificación definidos. Para ello se realizará una matriz de evaluación, donde se estime el nivel de cumplimiento de cada uno de los requisitos técnicos.

Consideraciones éticas.

- Garantizar la confidencialidad y privacidad de información sensible, que se pueda recopilar durante la investigación.

Limitaciones y delimitaciones.

- Realizar la investigación dentro del plazo establecido.
- Realizar la evaluación técnico informática del servicio.
- No abordar aspectos administrativos o financieros.

Presupuesto.

No se requiere de recursos económicos para realizar esta investigación.

Ejecución del plan de investigación de campo.

Definición de variables de evaluación.

En primer lugar, se realizó una revisión de la literatura planteada, haciendo más énfasis en los requisitos técnicos de certificación, con el objetivo de determinar variables o aspectos

técnicos que se puedan evaluar de manera técnica e informática, y posteriormente, realizar la investigación de campo.

Tabla 8

Variables de evaluación del servicio de firma electrónica

Requisito técnico de certificación	Variables	Descripción
Jerarquía entidad de certificación de información	Jerarquía PKI	Diseño e implementación de una Jerarquía PKI para el servicio de firma electrónica
Administración de la autoridad de certificación	Rol de administrador Rol de auditor	Definición de roles de administración
Roles y responsabilidades para generación y migración de llaves privadas	Roles de administración de llaves privadas	Asignación de roles y responsabilidades para la administración de las llaves privadas
Procesos de auditoría de seguridad	Auditoría de seguridad	Auditoría de seguridad del servicio de firma electrónica
Mecanismos de validación: CRL, OCSP, LDAP	CRL OCSP LDAP	Servicios de autoridad de validación
Certificados de servidor seguro (SSL)	Certificados SSL	Certificados para navegación segura para protocolo HTTPS
Servicios de emisión, renovación y revocación de certificados digitales	Servicio de emisión de certificados digitales Servicio de renovación de	Servicios para administrar el ciclo de vida de los certificados digitales

Requisito técnico de certificación	Variables	Descripción
Autoridades de Registro	certificados digitales Servicio de revocación de certificados digitales Rol de Autoridad de Registro	Roles y reglas de acceso para la administración del ciclo de vida de los certificados digitales
Contenedores criptográficos HSM	HSM	Dispositivo de almacenamiento de tokens criptográficos
Mecanismos de seguridad	Autenticación con certificados digitales	Método de autenticación para administrar el servicio de firma electrónica
Componentes de seguridad perimetral	Sistema de prevención de intrusos Firewall Balanceadores	Controles de seguridad y protección del servicio de firma electrónica
Plan de contingencia	Plan de contingencia	Estrategias y medidas para garantizar la continuidad del servicio en caso de un siniestro
Sistema de control de acceso al centro de cómputo	Control de acceso al centro de cómputo	Controles de seguridad de ingreso de usuarios al centro

Requisito técnico de certificación	Variables	Descripción
Registro de ingreso al centro de cómputo	Registro de acceso al centro de cómputo	de cómputo donde se encuentra implantado el servicio de firma electrónica Registros sobre los usuarios que ingresa al centro de cómputo donde se encuentra implantado el servicio de firma electrónica.
Respaldo de información	Respaldo de información	Respaldo de base de datos

Evaluación del servicio de firma electrónica.

Luego de realizar el análisis técnico informático y realizar las observaciones necesarias del servicio de firma electrónica, implantado en el ESPE CERT, se presenta la siguiente matriz de evaluación del servicio.

Tabla 9

Matriz de evaluación del servicio de firma electrónica

Variable	Cumple	Observación
Jerarquía PKI	Si	Actualmente se ha diseñado una Jerarquía PKI, pero esta no contempla todos los tipos de usuarios finales que pudiesen existir dentro del contexto de la universidad ni todos los tipos de usuarios administradores.
Rol de administrador	Si	Se ha creado un rol y reglas de acceso para la administración del servicio

Variable	Cumple	Observación
Rol de auditor	No	No se ha creado un rol y reglas de acceso para la administración del servicio
Roles de administración de llaves privadas	No	No se ha creado ni asignado roles para la administración de llaves privadas
Auditoría de seguridad	No	
CRL	Si	
OCSP	Si	
LDAP	No	
Certificados SSL	Si	El software crea e implementa estos certificados para la navegación segura (HTTPS), pero estos certificados no son reconocidos a nivel de internet.
Servicio de emisión de certificados digitales	Si	Este servicio se ha configurado para que el usuario final, llene un formulario y solicite la emisión de un certificado digital.
Servicio de renovación de certificados digitales	Si	
Servicio de revocación de certificados digitales	Si	Este servicio puede ser usado únicamente por la Autoridad de Registro
Rol de Autoridad de Registro	Si	

Variable	Cumple	Observación
HSM	No	No se cuenta con este tipo dispositivo.
Autenticación con certificados digitales	Si	El ingreso de los usuarios administradores y Autoridades de Registro, se realiza a través de certificados digitales.
Sistema de prevención de intrusos	No	
Firewall	No	
Balanceadores	No	Toda la implementación de la PKI y del servicio de firma electrónica se encuentra realizada en un único servidor, debido a que la versión libre del software usado, no permite realizar una arquitectura distribuida.
Plan de contingencia	No	
Control de acceso al centro de cómputo	Si	El laboratorio donde se encuentra implantado el servicio, cuenta con un sistema de control de ingreso de usuarios, a través de tarjetas electrónicas. Sin embargo, en este laboratorio se encuentra también, la dirección de carrera de TI, por lo que se permite el ingreso de usuarios comunes.
Registro de acceso al centro de cómputo	No	
Respaldo de información	No	

Conclusión de evaluación del servicio de firma electrónica.

De acuerdo a los requisitos técnicos de certificación, se establecieron un total de 22 variables para la evaluación del servicio, de los cuales el 50 %, se cumple a cabalidad con algunas observaciones; mientras que el otro 50 % aún no se ha implementado. De esto se puede concluir que el servicio aún no se encuentra listo para ser certificado.

Informe de las no conformidades y las recomendaciones de mejora.

Presentación de no conformidades.

Con la evaluación técnico informático del servicio de firma electrónica, se encontraron algunas no conformidades relacionadas a las limitaciones que presenta el uso de la versión libre del software en cuestión. Principalmente, se tiene la limitación de la distribución de los servicios para garantizar una alta disponibilidad del servicio de firma electrónica, como por ejemplo la distribución de los servicios exclusivos de VA o RA. Con la versión libre no se puede realizar una instalación exclusiva de estos, pero si permite realizar varias instalaciones completas de toda la arquitectura de PKI, lo que sería suficiente para cumplir con este aspecto.

Algunos de los aspectos evaluados, se cumplen de manera parcial en relación con el requisito técnico, como es el caso de la Jerarquía PKI, donde no se ha definido por completo todas las entidades finales que se requieren. De igual forma sucede con los servicios de la Autoridad de Validación, donde no se ha configurado el servicio de validación LDAP. Por otro lado, de los servicios para manejar el ciclo de vida de los certificados digitales, solo se ha puesto a disposición el servicio para solicitar nuevos certificados por parte de los estudiantes, los otros servicios para la renovación y revocación, únicamente son manejados por las Autoridades de Registro.

En cuanto a la seguridad del centro de cómputo o del laboratorio donde se encuentra implantado el servicio de firma electrónica, los procedimientos y mecanismos de seguridad, para garantizar la integridad del servicio, no son suficientes. Además, los servidores utilizados no se encuentran debidamente instalados, ya que estos se encuentran en el piso; por otra

parte, no cuentan con un sistema de redundancia de energía eléctrica, que permita la continuidad ininterrumpida del servicio de firma electrónica, en caso de fallos eléctricos o cortes de energía. El servicio debería trasladarse a un Data Center, ya que estas estructuras cuentan con las especificaciones mencionadas y la administración del servicio debería estar en un centro de cómputo, en este caso puede considerarse utilizar el laboratorio H402.

Recomendaciones de mejora.

A continuación, se describen recomendaciones que permitirían mejorar el servicio de firma electrónica en conformidad con los requisitos técnicos de certificación.

- Jerarquía PKI: Complementar la jerarquía PKI diseñada con todos los roles de administración y entidades finales.
- Servicios de validación: Configurar el servicio de validación LDAP.
- Respaldos de información: Crear un plan de respaldo de información de la base de datos de forma periódica.
- Balanceador de carga: Disponer de una mayor infraestructura de TI para la creación de un servicio de alta disponibilidad. La instalación del servicio se realizó en 2 servidores; para garantizar un servicio de alta disponibilidad se debería considerar una asignación mínima de 6 servidores.
- Firewall
- Centro de cómputo
- Registro y control de acceso al centro de cómputo
- Seguridad del centro de cómputo
- Data Center
- Plan de contingencia y Auditoría de seguridad
- Sistema de prevención de intrusos
- HSM

Capítulo V

Mejora del servicio y resolución de las no conformidades

Objetivo

- Elaborar un plan de mejora del servicio de firma electrónica para su certificación, en base de las recomendaciones del informe de evaluación técnico informático.

Alcance

Elaborar y recomendar acciones de mejora para el servicio de firma electrónica implementado en el ESPE CERT del DCCO, con la finalidad de proponer soluciones a las no conformidades encontradas en su instalación y arquitectura, en relación con los requisitos técnicos de certificación. Presentar alternativas para la recaudación del presupuesto necesario para certificar el servicio de firma electrónica.

Indicadores de cumplimiento

- Recomendaciones de mejora para la instalación del servicio
- Recomendaciones de mejora para la arquitectura del servicio
- Alternativas de recaudación de presupuesto

Recursos

- Humanos: Se dispone de un estudiante a cargo del proyecto de titulación y del docente tutor del mismo.
- Materiales: Computadora personal.

Actividades a realizar

El siguiente cronograma indica las actividades a realizar para crear el plan de mejora del servicio de firma electrónica.

Tabla 10

Actividades del plan de mejora

Actividad	Responsable	Duración	Comienzo	Fin
Elaboración de las recomendaciones de mejora para la instalación del servicio.	Estudiante	2 días	25 jul	26 jul
Elaboración de las recomendaciones de mejora para la arquitectura del servicio.	Estudiante	2 días	27 jul	28 jul
Evaluación del plan de mejora.	Estudiante	1 día	29 jul	29 jul
Elaboración de alternativas de recaudación de presupuesto	Estudiante	1 día	01 ago	01 ago

Elaboración de las recomendaciones de mejora para la instalación del servicio

En esta etapa se contempla recomendar un conjunto de acciones para mejorar la instalación del servicio de firma electrónica. Al hablar de la “instalación” se refiere a las instalaciones o el espacio físico donde se encuentra instalado el servicio. Estas recomendaciones están enfocadas a la seguridad de las instalaciones, entre otros aspectos, y que son necesarias puesto que son parte de los requisitos técnicos de certificación.

Centro de computo principal.

Actualmente los servidores en los que se encuentra instalada la firma electrónica, están ubicados en el laboratorio H402 del DCCO. En este mismo lugar se encuentra la dirección de carrera de TI, por lo que cualquier estudiante puede ingresar a este laboratorio. Como primer paso, se debería designar un espacio aislado donde solo personal autorizado pueda ingresar a las instalaciones de la firma electrónica.

Además, en este laboratorio H402, los servidores utilizados se encuentran en el piso, lo cual no sería apropiado si se busca certificar este servicio.

Este espacio debe tener un control de acceso mediante llaves, tarjetas electrónicas u otros dispositivos de seguridad de borde, de manera que solo personal autorizado pueda ingresar a él.

Se debe tener un registro de todas las personas que ingresen a este centro de cómputo, especificando la hora de entrada, salida y la actividad a realizar.

Este centro de cómputo debe estar adecuado para un correcto funcionamiento de los servidores. Debe tener un sistema de ventilación que permita evitar el sobre calentamiento de los servidores. Sistema de respaldo de energía eléctrica en caso de apagones, algo que es muy constante en el espacio geográfico donde se encuentra la Universidad. Básicamente, este centro de cómputo debe seguir los mismos estándares que se utilizan para la implementación de Data Centers. En tal caso, este servicio debería trasladarse hacia un Data Center, y el centro cómputo, que sería el laboratorio H402, podría usarse para la administración del servicio.

Centro de cómputo secundario.

Este centro de cómputo secundario no requiere de las mismas especificaciones que el principal, puesto que funcionaría como un sitio alternativo, en caso de que el principal sufriese de algún inconveniente. Pero se requiere de un sitio secundario para garantizar la continuidad del servicio en caso de incidentes con el principal.

Este sitio secundario debe ser un espacio aislado, que solo pueda ingresar personal autorizado. Con los mismos controles de acceso que el principal y registro de accesos.

Servidores de respaldo de información.

Para garantizar la pérdida de información en caso de desastres, se debe contar con servidores de respaldo de base de datos ya sea en la nube o de manera local, o en el mejor de los casos, ambos. Estos respaldos deberían realizarse de manera diaria, a partir de la media noche, para no afectar la funcionalidad del servicio.

Plan de contingencia.

Se debe crear un plan de contingencia ante posibles desastres o fallos que interrumpan parcial o totalmente la funcionalidad servicio, estableciendo procedimientos para evitar interrupciones en la continuidad del mismo.

Elaboración de las recomendaciones de mejora para la arquitectura del servicio

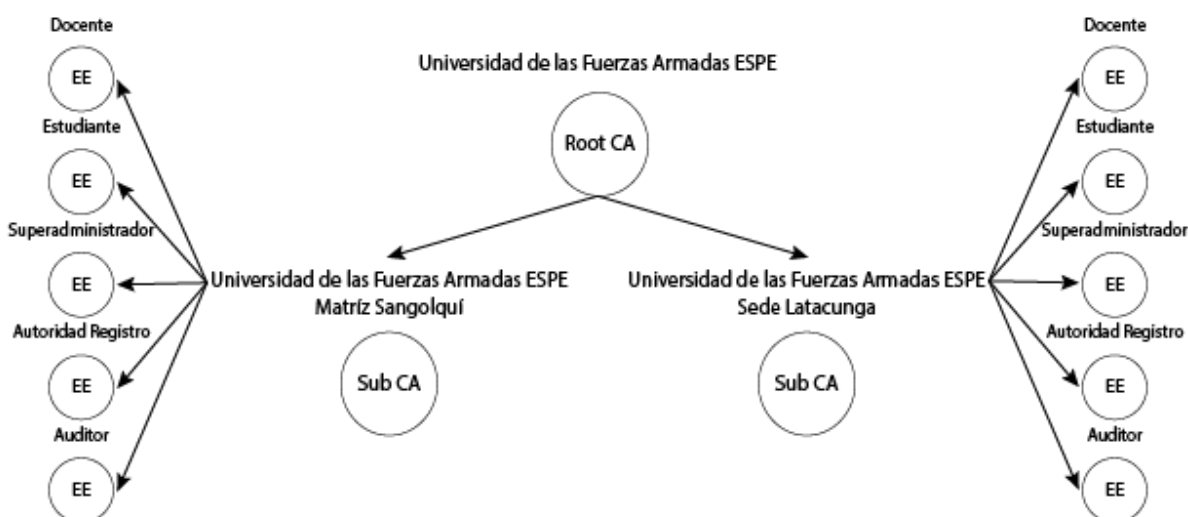
En esta etapa se contempla recomendar un conjunto de acciones para mejorar la arquitectura del servicio de firma electrónica. Al hablar de la “arquitectura” se refiere a como se encuentra instalado y funcionando el servicio. Para ello se propone un diseño mejorado, considerando los requisitos técnicos de certificación.

Jerarquía PKI.

Se propone la siguiente jerarquía PKI mejorada, considerando todas las entidades o usuarios a los que se emitirán certificados digitales, usuarios de administración y la sede Latacunga como Autoridad Certificadora Subdelegada.

Figura 60

Jerarquía PKI mejorada



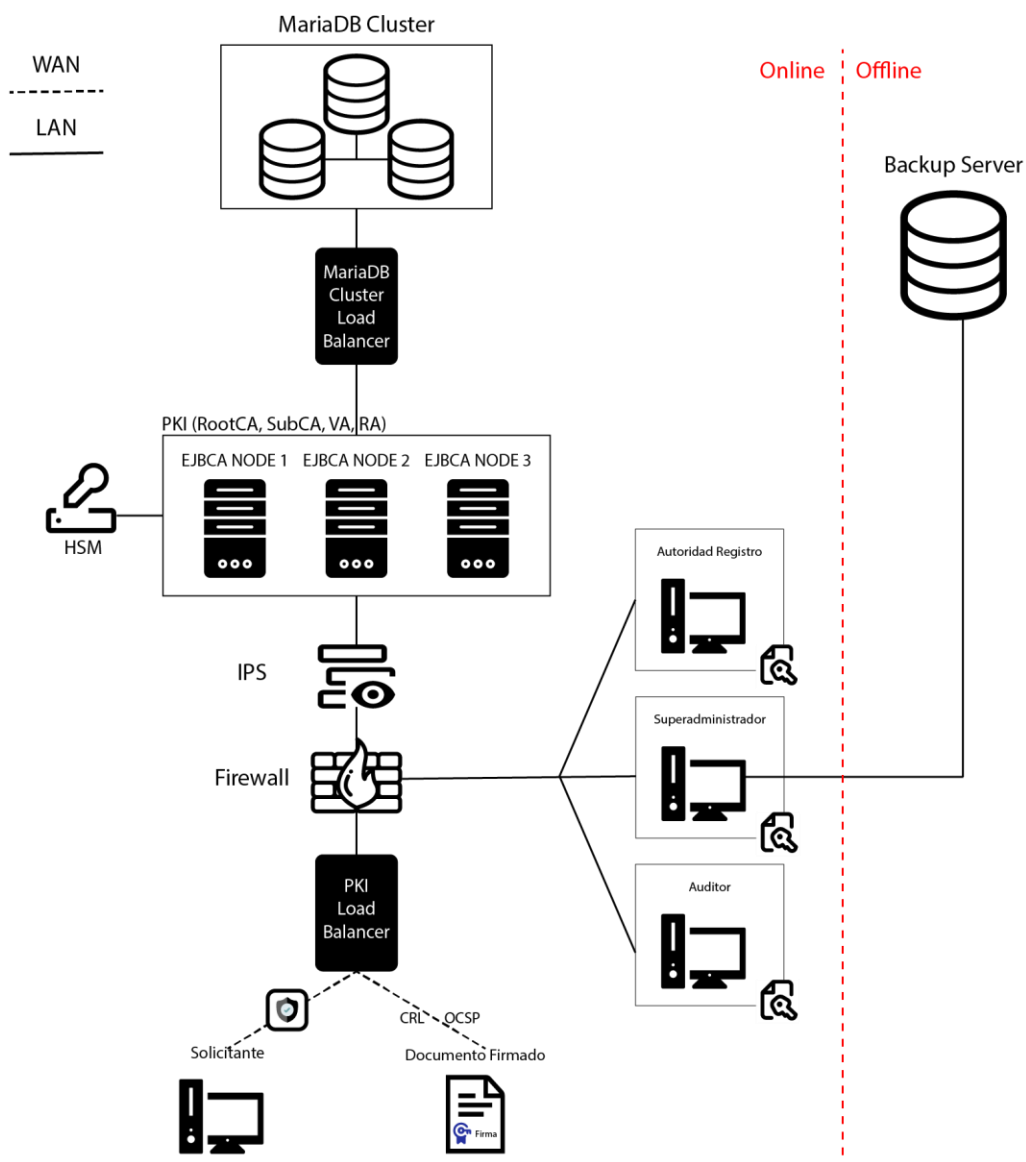
Esta jerarquía tiene una mejor organización en la distribución o emisión de certificados digitales para entidades o usuarios finales. Cada sede maneja y emite certificados por separado, para los diferentes tipos de usuarios identificados.

Arquitectura del servicio.

En el siguiente diseño se presenta una arquitectura mejorada, contemplando aquellos aspectos técnicos de certificación requeridos, como lo son la implementación de: firewall, HSM, conectividad LAN, WAN, servidores de respaldo, balanceadores de carga, conexiones cifradas o SSL.

Figura 61

Arquitectura del servicio mejorada



Clúster de base de datos.

Garantizar un servicio de alta disponibilidad no solo involucra tener redundancia en los servicios o aplicaciones web, en este caso de la PKI. Múltiples servidores web que se conectan a un solo servidor de base de datos, podría ocasionar fallos en el mismo. Por ello se recomienda también tener un sistema redundante de base de datos.

En este aspecto aparece el concepto de “clúster”, que es una agrupación de servicios que trabajan en conjunto para crear un servicio más robusto. Un clúster de base de datos,

permite conectar múltiples servidores de base de datos de manera sincronizada, es decir, que, si se realiza acción de escritura en un nodo del clúster, este cambio se ve automáticamente reflejado en los otros nodos.

MariaDB Galera es un software gratuito y de código abierto, que permite la creación de un clúster de base de datos con el motor de base de datos MariaDB. Este software recomienda usar un número impar de servidores para usar el clúster, siendo el mínimo 3 servidores. De igual forma, el software de la PKI, EJBCA, recomienda usar mínimo 3 servidores de base de datos MariaDB para crear un servicio de alta disponibilidad.

Alta disponibilidad de PKI.

Luego de crear un clúster de base de datos, se puede crear la redundancia para los servicios de la PKI. Esto consiste en instalar el software EJBCA en múltiples servidores o nodos, conectados al clúster de base de datos a través de un balanceador de carga entre el clúster y la PKI. Cada nodo contiene todas las componentes o servicios de la PKI, es decir, la Autoridad de Validación, Autoridad de Registro y Autoridad de Certificación, entre otros, por lo que, implementando 3 nodos, se estarían creando 3 servicios de cada uno de ellos.

Balanceador de carga.

Un balanceador de carga permite distribuir las solicitudes que recibe un servidor a varios de ellos, permitiendo que un servicio se pueda distribuir en varios servidores y aligerar la carga de cada uno de ellos de forma automática.

Existen varios tipos de balanceadores de carga, ya sea físico o lógicos, dependiendo de la capa de red donde se implemente. Para esta implementación se puede recomendar un balanceador de carga lógico o de software como HA Proxy. Este software es gratuito y de código abierto que proporciona un equilibrador de carga de alta disponibilidad y un proxy inverso para aplicaciones basadas en TCP y HTTP.

Este software serviría tanto para el clúster de base de datos, que usa el protocolo TCP y para los servicios web de la PKI, que usan el protocolo HTTP.

Firewall.

Un firewall es una herramienta que monitorea el tráfico de la red, permitiendo bloquear y controlar los accesos a través de la red a los servidores.

Uno de los aspectos más importantes para certificar el servicio de firma electrónica, es la seguridad del mismo, por ello la implementación de un firewall es muy importante y necesario.

Este tipo de herramienta se puede implementar tanto en hardware o software o una combinación de ambos. En este caso se recomienda un firewall de hardware, puesto que hay muchos dispositivos en custodia o que deben protegerse detrás de él.

Respaldo de base de datos.

Como parte de la seguridad del servicio de la firma electrónica, es importante contar con un respaldo de la base de datos constante, de manera diaria, de manera que, en caso de un fallo en el clúster de base de datos o pérdida del mismo, se pueda restablecer el servicio sin pérdida de información. Este servidor de respaldo debe estar fuera de línea del servicio de firma electrónica, para evitar accesos innecesarios u otros procesos ajenos al mismo. Adicional, se puede considerar tener un servidor de respaldo en la nube.

IPS.

Un IPS es una herramienta que permite identificar el tráfico malicioso en la red y tomar acciones contra el mismo. Esta herramienta controla de mejor manera los accesos al servicio de firma electrónica y mejora aún más su seguridad.

HSM.

Un HSM es un dispositivo que sirve para almacenar los tokens criptográficos de las Autoridades Certificadoras. Estos tokens son usados para firmar y otorgar los certificados digitales, por lo que su seguridad es muy importante.

Este dispositivo es un hardware sólido y resistente a manipulaciones, con altos estándares de seguridad, que garantiza la utilización y almacenamiento de tokens

criptográficos. La administración de este proceso debe ser realizado por el usuario superadministrador.

Evaluación del cumplimiento del plan de mejora

Con el fin de evaluar el plan de mejora y las acciones recomendadas para optimizar el servicio de firma electrónica en relación con los requisitos técnicos de certificación, se procede a realizar una nueva evaluación técnico informático del servicio.

Tabla 11

Matriz de evaluación del plan de mejora para el servicio de firma electrónica

Variable	Cumple
Jerarquía PKI	Si
Rol de administrador	Si
Rol de auditor	Si
Roles de administración de llaves privadas	Si
Auditoría de seguridad	No
CRL	Si
OCSP	Si
LDAP	No
Certificados SSL	Si
Servicio de emisión de certificados digitales	Si
Servicio de renovación de certificados digitales	Si
Servicio de revocación de certificados digitales	Si
Rol de Autoridad de Registro	Si
HSM	Si

Autenticación con certificados digitales	Si
Sistema de prevención de intrusos	Si
Firewall	Si
Balanceadores	Si
Plan de contingencia	Si
Control de acceso al centro de cómputo	Si
Registro de acceso al centro de cómputo	Si
Respaldo de información	Si

Con las propuestas presentadas, el resultado de la evaluación tiene un 90.9 % de cumplimiento, en donde se cubre casi en su totalidad los requisitos técnicos de certificación.

Elaboración de alternativas de recaudación de presupuesto

Ejecución del servicio de firma electrónica dentro de la ESPE.

Se plantea la propuesta de poner en ejecución el servicio de firma electrónica para la realización de trámites internos en la ESPE. La Universidad actualmente cuenta con aproximadamente 20,000 estudiantes, entre todas sus distintas sedes. Teniendo en cuenta el número de estudiantes a los que se prestaría el servicio, se considera aplicar una tarifa por la emisión y renovación de certificados digitales. El certificado digital tendría un costo de \$ 10 por un periodo de validez de un año o de \$ 5 por semestre. Considerando el número de estudiantes y el costo del servicio, por cada año de operación se recaudarían aproximadamente \$ 200,000. De esta forma al cabo de 3 años de operación del servicio se estaría recaudando el presupuesto necesario para obtener la certificación.

Capítulo VI

Conclusiones

Se realizó una nueva implementación mejorada del servicio de firma electrónica en el ESPE CERT del DCCO de la matriz Sangolquí, contemplando una arquitectura y jerarquía de PKI similar a como funcionaría una Entidad de Certificación, con la disponibilidad para prestar el servicio a la comunidad universitaria de esta misma sede y la sede Latacunga. Esta implementación se realizó utilizando únicamente software libre, por lo que adquirir la versión empresarial del software usado, sería opcional en el caso de que se quisiese implementar un servicio mucho más robusto.

Se realizó un análisis de certificación en el que se determinó los requisitos económicos, legales y técnicos para certificar el servicio de firma electrónica, obteniendo como resultado una pausa en el proceso de certificación, puesto que se necesita una inversión económica grande y una mayor asignación de recursos e infraestructura de TI.

Se evaluó el servicio de firma electrónica en relación a los requisitos técnicos de certificación, determinando que este no se encuentra listo para obtener la certificación, ya que se requiere que el servicio cuente con altos niveles de seguridad y una mejor distribución de los servicios, para lo cual se necesita una mayor asignación de recursos e infraestructura de TI.

En base a la evaluación realizada, se elaboró un plan de mejora del servicio de firma electrónica, en el que se propuso recomendaciones para mejorar el servicio y cumplir con los requisitos técnicos de certificación.

Recomendaciones

Se pretende extender el servicio de firma electrónica para toda la comunidad universitaria en cada una de las sedes de la ESPE, por lo que se recomienda asignar más recursos e infraestructura de TI para crear un servicio seguro y de alta disponibilidad como se plantea en el plan de mejora.

En vista de que se debe realizar una inversión económica grande para certificar el servicio de firma electrónica y no se ha podido determinar si se asignarán los recursos económicos en un futuro, se recomienda crear un conjunto de políticas internas y que formen parte del reglamento de la ESPE, en el que se autorice al servicio de firma electrónica implantado en el ESPE CERT, como un medio de legalización y certificación de documentos para tramites dentro de la Universidad.

El uso de software libre se adapta perfectamente a las necesidades para crear un servicio de firma electrónica para la ESPE, sin embargo, en el caso de requerir características adicionales que se encuentran en la versión empresarial del software, se recomienda realizar un análisis del código fuente del software y determinar si es posible ajustarlo a las necesidades requeridas, puesto que es software libre y se puede modificarlo según se necesite.

Referencias

About EJBCA®. (s. f.). EJBCA. Recuperado 14 de junio de 2023, de

https://www.ejbca.org/?page_id=775

ARCOTEL. (2016, agosto 18). Requisitos: ENTIDADES DE CERTIFICACIÓN - Agencia de

Regulación y Control de las Telecomunicaciones. *Agencia de Regulación y Control de*

las Telecomunicaciones - Promovemos el desarrollo armónico del sector de las

telecomunicaciones, radio, televisión y las TIC , mediante la administración y regulación eficiente del espectro radioeléctrico y los servicios.

<https://www.arcotel.gob.ec/requisitos-entidades-de-certificacion/>

Carrera López, A. F., & Celi Jiménez, J. F. (2022). *Implementación de una PKI no acreditada*

utilizando estándares internacionales para garantizar la integridad de los documentos

firmados digitalmente. Caso de estudio: Departamento de Ciencias de la Computación

DCC-ESPE [BachelorThesis, Universidad de las Fuerzas Armadas ESPE. Carrera de Ingeniería de Sistemas e Informática].

<http://repositorio.espe.edu.ec/jspui/handle/21000/29387>

Congreso, N. (2002). *Ley de comercio electrónico, firmas electrónicas y mensaje de datos.*

<https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf>

Firma_electronica.pdf. (s. f.). Recuperado 9 de junio de 2023, de

http://www.eco.uva.es/firmaelectronica/res/firma_electronica.pdf

Montesinos Flores, N. I. J., & Jhonatan Rober, T. J. (2022). Propuesta de una implementación

de un sistema de gestión de proyectos e incidencias con enfoque ITIL v4.0 para mejorar los servicios de TI del centro comercial MegaPlaza en la ciudad de Lima—2021.

Repositorio Institucional - UTP. <http://repositorio.utp.edu.pe/handle/20.500.12867/6273>

- Olsina, L., Rivera, M. B., Papa, M. F., & Becker, P. (2020). PROCESO DE DESIGN SCIENCE RESEARCH APLICADO A LA CONSTRUCCIÓN DE UNA ONTOLOGÍA DE TESTING DE SOFTWARE COMO ARTEFACTO. *Revista Digital del Departamento de Ingeniería e Investigaciones Tecnológicas*, 5(1), Article 1.
[//reddi.unlam.edu.ar/index.php/ReDDi/article/view/116](http://reddi.unlam.edu.ar/index.php/ReDDi/article/view/116)
- Orozco Cajilema, F. F. (2017). *Desarrollo del sistema informático para la web integrando a JSP y MariaDB como DBMS para la gestión de fichas médicas del Hospital básico "San Marcos" utilizando tecnología móvil*. [BachelorThesis, Escuela Superior Politécnica de Chimborazo]. <http://dspace.esPOCH.edu.ec/handle/123456789/9091>
- Peffer, K., Tuunanen, T., Gengler, C. E., Rossi, M., & Hui, W. (s. f.). THE DESIGN SCIENCE RESEARCH PROCESS: A MODEL FOR PRODUCING AND PRESENTING INFORMATION SYSTEMS RESEARCH. *SYSTEMS RESEARCH*.
- Pilicita Garrido, A., Borja López, Y., & Gutiérrez Constante, G. (2021). *Rendimiento de MariaDB y PostgreSQL*. <https://repositorio.upse.edu.ec/handle/46000/7315>
- Remache Típan, M. L. (2022). *Marcos de gestión de tecnologías de información: Análisis del marco de gestión ITIL v4*. [BachelorThesis, Quito : EPN, 2022.].
<http://bibdigital.epn.edu.ec/handle/15000/22414>