UNIVERSIDAD NACIONAL
JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

FACULTAD DE INGENIERÍA INDUSTRIAL, SISTEMAS E INFORMÁTICA
ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS

INFORME DE TESIS

CERTIFICADOS DIGITALES X.509 DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA DEL ESTADO PERUANO PARA LA FIRMA DIGITAL DE LA INFORMACIÓN

Para optar el título profesional de ingeniero de sistemas

Presentado por:

Bach. Figari Medina, Henry Raúl Oscar

Asesorado por:

Ing. De los Santos García, Juan Carlos
CIP. N° 20326

Huacho, Perú
2014

Resumen

La presente tesis pretende relatar las practicas efectuadas por las prestadoras de servicios de certificación digital para poner en funcionamiento la Infraestructura Oficial de Firma Electrónica, plataforma donde se desarrollara un serie de servicios orientados principalmente a garantizar la autoría, la integridad y confidencialidad de la información trasmitida a través de Internet.

Entre los principales objetivos de este trabajo de investigación se encuentra el de proporcionar información sobre el nivel actual de operatividad en el que se encuentra la infraestructura de estudio necesaria para generar firmas digitales con la misma validez legal que la firma manuscrita. La mayor parte de esta información se provee en forma de descripciones e ilustraciones usando un lenguaje comprensible a fin de permitir un mayor entendimiento a los lectores de la presente, es decir, el nivel matemático aplicado en el capítulo "resultados" es relativamente moderado, casi imperceptible.

Este trabajo se ha estructurado en una serie de capítulos, cada uno de los cuales detalla lo siguiente:

El capítulo I inicia con el planteamiento del problema, que comprende la descripción de la realidad problemática, la formulación del problema y los objetivos de la investigación.

El capítulo II provee el marco teórico, que resume los diferentes antecedentes relacionados a la presente investigación, seguido por la descripción del fundamento teórico que está detrás de una infraestructura de clave pública y que permitirá comprender la importancia de tener operativa una infraestructura de este tipo, en el Estado Peruano. La primera parte de la base teórica define algunas propiedades de la información; la segunda da una explicación compacta y comprensible de la criptografía; la infraestructura y sus elementos básicos se estudian en la tercera parte; y la

última parte introduce conceptos de la firma digital y sus aplicaciones. Este capítulo finaliza con las definiciones conceptuales que tiene relación con la variable de estudio.

El capítulo III se ocupa de la metodología de la investigación, que incluye la definición del diseño metodológico, población y muestra, la operacionalización de variables e indicadores así como las técnicas e instrumentos para la recolección de datos.

El capítulo IV, "resultados", describe los aspectos más relevantes de la infraestructura de estudio incluyendo la forma de cómo está operando y como accederla actualmente. Para ello, analiza la información recopilada a través de fuentes secundarias y entrevistas.

El último capítulo menciona algunas conclusiones y recomendaciones, puntos que ponen en claro los resultados del presente informe, donde se ha enfatizado los temas que deben ponerse atención para mejorar el desempeño de la infraestructura, pues, en base a los mismos, se determinó que los mecanismos que participan dentro de ella, no son los suficientes para que ésta opere de forma efectiva, es decir, por el momento no se podrá gestionar en esta plataforma certificados digitales X.509 para generar firmas digitales.

Finalmente, el anexo B ofrece un ejemplo práctico y muy conveniente para aquellos que deseen saber la manera de solicitar un certificado digital.

Espero que el presente informe sirva como material de estudio e investigación, ya que para el despliegue de esta infraestructura, también es necesario la intervención y ejecución de componentes lógicos, esto es, software para la firma digital, que para su desarrollo deberá tenerse en cuenta la normatividad que rige su operación.