

Resumen

La falsificación, duplicado y comercio ilegal de comprobantes curriculares se ha convertido en una problemática que alcanza niveles internacionales. Motivado por tal situación, se presenta en este trabajo el diseño de un sistema basado en tarjetas inteligentes que permite almacenar y recuperar de manera segura y eficiente, expedientes curriculares electrónicos para brindar una alternativa en la verificación de la autenticidad de los documentos probatorios de todas las personas que cuentan con estudios de nivel profesional o superior en el país. El sistema consiste de una red de servidores de bases de datos y servidores de aplicaciones distribuidos de acuerdo a entidades establecidas a las que se les nombró “Entidades de Certificación”. Se implementa una arquitectura que permite brindar alta disponibilidad y concurrencia por medio del uso de servidores de réplicas y enlaces seguros a través de la red Internet, haciendo el uso de Redes Privadas Virtuales (VPN). El trabajo incluye una investigación a profundidad sobre la tecnología de tarjetas inteligentes, las cuales se incorporan a este sistema para utilizarse como mecanismo de acceso seguro para visualizar la información de los expedientes curriculares electrónicos. El mecanismo de autenticación mutua basado en el algoritmo criptográfico 3-DES que las tarjetas inteligentes seleccionadas para este trabajo implementan, permitió contar con un mecanismo seguro para el acceso e identificación de los usuarios con el sistema. Se diseñó un modelo para representar y almacenar la información de los expedientes curriculares utilizando el Lenguaje de Marcado Extensible (XML), el cual pretende que se estandarice para ser utilizado por las diversas instituciones educativas y empresas del país.

Abstract

The illegal creation, reproduction and sale of fake diplomas has become an international issue. Motivated by this problem, this work presents the design of a smart card based system that stores and retrieves electronic academic files in an efficient and secure way to provide an alternative process of academic document authenticity verification of all professionals in this country. The system consists of a database server network and application servers distributed among designated locations called “Certification Entities”. An architecture that provides high availability and concurrency is implemented using replica servers and secure communication links across the Internet via Virtual Private Networks (VPN). This work includes an extensive research on smart cards which are integrated to the system for being used as a secure access mechanism for visualizing the electronic curricular files. The mutual authentication mechanism based on the 3-DES cryptographic algorithm that the smart cards chosen for this system employ, allow the system to have a secure mechanism for user access and identification. A model for representing and storing information about electronic curricular files was designed using the eXtended Modeling Language (XML) which is intended to be standardized and used by the diversity of educational institutions and companies in this country.