Instituto Tecnológico y de Estudios Superiores de Monterrey

MA2006B.601: Uso de Algebras modernas para seguridad y criptografía (Gpo 601)

Casa Monarca

Firmas solidarias: Tecnología criptográfica para los derechos humanos

Solidarity Signatures: Cryptographic Technology for Human Rights

Integrantes:

Juan Marco Castro Trinidad A01742821

Fedra Fernanda Mandujano López A00835797

Miranda Isabel Rada Chau A01285243

Eliani González Laguna A00836712

Alfredo André Durán Treviño A01286222

Profesores:

Luis Miguel Méndez Díaz

Daniel Otero Fadul

Raúl Gómez Muñoz

16 de marzo de 2025

Índice

Resumen 3

Abstract 3

Introducción 4

Marco Referencial 5

Marco Legal 6

Resumen

Casa Monarca, una organización sin fines de lucro en Monterrey, brinda apoyo humanitario a migrantes, facilitando su integración social, legal y cultural en México. Las firmas tradicionales a papel pueden ser fácilmente falsificadas, sin mencionar los trucos de impresión a computadora. Para mejorar la seguridad y eficiencia de sus procesos administrativos, la organización busca implementar un sistema de firma digital que garantice la autenticidad e integridad de los documentos. Este reporte explora el estado del arte de las firmas digitales, estándares criptográficos, soluciones existentes y consideraciones legales y éticas en México. El objetivo es proponer una solución adaptada a las necesidades de Casa Monarca, asegurando la protección de datos sensibles y el seguimiento de las normas legales.

Abstract

Casa Monarca, a non-profit organization in Monterrey, provides humanitarian support to migrants, facilitating their social, legal and cultural integration in Mexico. Traditional paper signatures can be easily forged, not to mention computer printing tricks. To improve the security and efficiency of its administrative processes, the organization seeks to implement a digital signature system that guarantees the authenticity and integrity of documents. This report explores the state of the art of digital signatures, cryptographic standards, existing solutions and legal and ethical considerations in Mexico. The objective is to propose a solution adapted to Casa Monarca's needs, ensuring the protection of sensitive data and compliance with legal regulations.

Introducción

Casa monarca es una organización sin fines de lucro donde cuentan con la filosofía de brindar ayuda humanitaria a los migrantes que transitan o buscan instalarse en la ciudad, proporcionándoles alojamiento, con la finalidad de que logren integrarse legalmente, social y culturalmente a México. Abogan por sus derechos humanos por una mejor calidad de vida, tomando en cuenta sus necesidades como la alimentación, ropa, calzado, asistencia médica, orientación y acompañamiento jurídico. (Casa Monarca, s.f.)

Con esto, esta organización tiene una necesidad en mejorar sus procesos de firmas electrónicas de documentos para mejorar su seguridad, ya que se trata de documentos sensibles de las personas migrantes y de documentación interna dentro de la organización. Una firma digital como dice el nombre, reemplaza a una forma física de identificar a una persona a través de métodos criptográficos que garantizan seguridad en los documentos. Es importante que estos documentos tengan esta seguridad para no ser corrompidos por un atacante queriendo modificar estos documentos. El propósito de este proyecto es generar métodos de seguridad por medio de criptografía para documentos internos, asegurando la protección de datos sensibles. A continuación se muestra una investigación respecto a la necesidad de estos métodos de seguridad y la importancia de este proyecto para una organización. (Casa Monarca, s.f.)

Con este proyecto el socio formador obtendrá grandes beneficios acorde a la seguridad y el buen manejo de sus datos al aplicar las firmas digitales en ellos, puesto que, contará con una mejor protección e integridad de estos, añadiendo una reducción a posibles fraudes cibernéticos.

Marco Referencial

Las transacciones electrónicas son ahora algo indispensables, por lo que es necesario usar un mecanismo cuyo objetivo sea asegurarse de que la integridad de los datos no esté alterada, autenticar el origen, y evitar que el usuario niegue su uso, la firma digital, que es el fruto de una transformación criptográfica de datos (of Standards y NIST, 2023). Dicho de mejor manera, un algoritmo usado para vincular criptográficamente un documento digital a la identidad de algo, sea máquina, persona o compañía. (Entrust, s.f.).

Esta herramienta es importante porque, al contrario que las firmas tradicionales, las de papel, es posible detectar inmediatamente las alteraciones de los documentos, y la autenticidad de la identidad del firmante sin necesidad de recurrir a testigos, permitiendo además de todo lo anterior llevar un registro electrónico de cualquier cambio lo que facilita enormemente la auditoría en caso de desacuerdos (Entrust, s.f.).

Algo importante a tener en cuenta es que casi todos los países y regiones tienen normas y reglamentos diferentes en cuanto a la creación de firmas electrónicas para que sean reconocidas legalmente, por lo que es necesario asesorarse jurídicamente para asegurarse de que se están cumpliendo con las normas requeridas en la región (Entrust, s.f.).

En Perú, Cachay (2024) realizó una investigación con la intención de analizar la situación actual de la manera en que se están procesando los documentos importantes que necesitan firmas digitales. Se consideró necesaria la creación y el uso de este tipo de firmas para mejorar el manejo administrativo de documentos en las universidades públicas de Perú. A través de este estudio se identificaron varios beneficios relacionados con el uso de firmas digitales, pero esto no ha aportado al avance y la agilización de los procesos administrativos de la universidad. Por lo tanto, la implementación y el uso de estas firmas no han aumentado.(Cachay Reyes et al., 2024) Las firmas digitales también se han usado en otros tipos de procesos como las compras electrónicas, el voto electrónico, entre otros. Para que se considere que

las firmas digitales y los procesos en los que se utilizan son exitosos es cuando son seguros y tienen factores que aseguran la autenticidad y la integridad de las firmas. Estos aspectos son importantes, ya que son los que verifican la identidad de la persona que firma.(Roy y Karforma, 2012)

Marco Legal

Como se ha mencionado en la sección anterior, el socio formador está buscando comenzar a implementar firmas digitales. Este proceso tiene el principal objetivo de eficientar el proceso de firmado y que este mismo sea más seguro. El aspecto legal que se relaciona con estas firmas varía dependiendo del país y la región. En el caso de México, se comenzaron a aceptar las firmas digitales a partir del 2003, cuando se actualizó el Código de Comercio Mexicano. Este mismo estableció que tanto individuos como compañías pueden usar firmas tanto físicas como digitales para firmar cualquier tipo de contrato o documento comercial. México ha establecido que para que una firma digital sea reconocida legalmente debe ser única para el firmante, se debería de poder identificar independientemente y cambios deben de ser fácilmente detectables. (SSL, 2024)

Referencias

Cachay Reyes, L., Chang Saldaña, J., Pastor Segura, J., Salirrosas Navarro, L., & Castagne Vasquez, J. (2024). Document processing system with digital signatures and administrative management in public universities. A review of the literature. Data and Metadata, 3-292. https://doi.org/10.56294/dm2024292

Casa Monarca, A. h. a. m. A. (s.f.). Inicio. https://casamonarca.org.mx/ Recuperado 10/03/2025.

Entrust. (s.f.). Firmas digitales. https://www.entrust.com/es/resources/learn/digital-signatures Recuperado 10/03/2025.

of Standards, N. I., & NIST, T. (2023). FIPS 186-5: Digital Signature Standard (DSS). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.186-5

Roy, D. A., & Karforma, S. (2012). A survey on digital signatures and its applications. JCIT, 3, 45-69. https://www.researchgate.net/publication/233391380_A_survey_on_digital_signatures_and_its_applications

SSL, S. T. (2024, marzo). The Legality of Digital Signatures: A Comprehensive Global Guide. https://www.ssl.com/article/the-legality-of-digital-signatures-a-comprehensive-global-guide/#ftoc-heading-14