Proyecto Casa Monarca: Etapa 1

Casa Monarca Project: Part 1

Juan José de Jesús Hernández Beltrán // A00836747

Julio // A00

Kevin Jesús Martínez Trinidad // A00834493

Mateo Zepeda // A00

Raúl Correa // A01722401

Profesores Asesores
Luis Miguel Méndez Díaz
Daniel Otero Fadul

Grupo: 602

02 de Marzo de 2025

Resumen

Introducción

Con el surgimiento de nuevas herramientas tecnológicas, vienen también nuevos retos en materia de seguridad informática. Los ataques cibernéticos son cada vez más sofisticados y la confianza tanto de las organizaciones como de las personas en la digitalización es cada vez mayor. Reemplazar documentos físicos por electrónicos se está volviendo un estándar en prácticamente cualquier industria, por lo que desarrollar y aplicar herramientas adecuadas para mantener su autenticidad, integridad y confidencialidad es cada vez más relevante, siendo el caso del socio formador Casa Monarca.

La firma digital es un proceso criptográfico que utiliza la infraestructura PKI (Public Key Infrastructure) para comprobar la autenticidad e integridad del archivo recibido. La firma digital emplea la clave privada del remitente para cifrar la información a enviar y el receptor emplea la clave pública del remitente para descifrarla, garantizando de esta forma la originalidad de la información (Ávila, 2015).

Los sistemas transaccionales son comunes en la mayoría de las organizaciones debido a la facilidad que otorgan para operar y gestionarlas, permitiendo la correcta colaboración entre los empleados, así como de agentes externos. Es a través de estos sistemas que se transmite todo tipo de información, tanto direccional como bidireccionalmente, muchas veces conteniendo información sensible o, que de verse modificada, podría afectar seriamente a la entidad (Ávila, 2015).

Casa Monarca lleva a cabo diariamente decenas de transacciones, tanto internas como externas, las cuales muchas veces resultan vitales para la continuación del proyecto. Debido a la naturaleza de la organización, estas transacciones deben de mantener su integridad y confidencialidad durante todo momento. Es por ello que las firmas digitales toman importancia, pues al firmar digitalmente un archivo, se está confirmando su veracidad y autenticidad, permitiendo la no repudiación. Por ejemplo, el correcto registro de donaciones permite tener un control de los ingresos, necesario para evitar tener malos entendidos con el SAT; los cambios efectuados en este registro deben ser aprobados y certificados por quien lo realiza, permitiendo de esta forma llevar un correcto control de las modificaciones.

Marco Referencial

Brainstorm de conceptos relevantes:

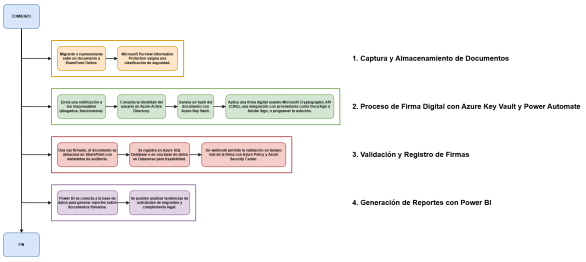
- PDF Advanced Electronic Signatures
- FIPS 140-2 NIST (Protocolo

Esquemas de llave pública según el lenguaje de programación:

- **Java**: Bouncy Castle es una biblioteca que proporciona implementaciones de algoritmos criptográficos y APIs para la generación y verificación de firmas digitales.
- **C++**: La biblioteca OpenSSL ofrece herramientas y funciones para la implementación de protocolos criptográficos, incluyendo firmas digitales.
- **Python**: Cryptography es una biblioteca que proporciona herramientas para la construcción de aplicaciones seguras, incluyendo la generación y verificación de firmas digitales.

Podemos usar Microsoft 365, Azure y Power Platform.

Conexión Docusign con Microsoft:
https://support.docusign.com/s/document-item?language=es&rsc_301=&bundleId=gqy1619537336307&topicId=qno1619537607438.html&_LANG=esxm



Referencias

https://es.wikipedia.org/wiki/PAdES

https://learn.microsoft.com/en-us/power-platform/release-plan/2023wave2/power-automate/use-credentials-azure-key-vault-desktop-connections

https://www.docusign.com/integrations/microsoft

https://learn.microsoft.com/en-us/entra/identity/saas-apps/docusign-tutorial
https://support.docusign.com/s/document-item?language=es&rsc_301=&bundleId=gqy1619537336307&topicId=qno1619537607438.html&_LANG=esxm