INVESTIGACIÓN

Plataforma integrada para la firma digital en el contexto de la empresa XETID

Integrated platform for digital signatures in the context of the company XETID

Dr.C. Huber Martínez Rodríguez[*], Ing. Yosvel Dupeirón Porra[2]

Recibido: 11/2025 | Aceptado: 11/2025 | Publicado: 12/2025

Resumen

En el proceso de informatización de la sociedad en los tiempos actuales, es imprescindible tener a disposición una Infraestructura de Clave Pública (PKI) en integración con un servicio seguro de firma digital disponible para su uso por la sociedad y el sector corporativo. La firma digital garantiza la integridad y la asociación del firmante con el documento digital firmado, y asegura así la autenticidad del este con fines legales. El presente trabajo propone una plataforma, que integra diferentes componentes, con el objetivo de brindar un servicio de firma digital seguro desde la Empresa de Tecnologías de Información para la Defensa (XETID) para la sociedad cubana en general. En este sentido intervienen, una infraestructura de llave pública, un servidor de firma digital, un servidor de sellado de tiempo y un servicio seguro para el manejo de claves y operaciones de criptográfica. También, se proponen tipologías de herramientas para el disfrute del servicio de firma digital.

[*] Empresa de Tecnologías de la Información para la Defensa, XETID, La Habana, Cuba. huber@xetid.cu

Universidad Máximo Gómez Báez de Ciego de Ávila, Cuba. huber@unica.cu

[2] Empresa de Tecnologías de la Información para la Defensa, XETID, La Habana, Cuba. ydupeiron@xetid.cu

En el desarrollo del trabajo se describen cada uno de los componentes, sus funciones esenciales y el tratamiento a las claves, con el propósito de lograr un servicio de firma digital robusto y seguro. Así mismo, se describen algunas herramientas esenciales para posteriores desarrollos con el fin de lograr el objetivo deseado.

Palabras clave: infraestructura de clave pública, servicio de sellado de tiempo, servidor de firma digital, protección segura de claves

Abstract

In the current process of digitizing society, it is essential to have a Public Key Infrastructure (PKI) integrated with a secure digital signature service available for use by society and the corporate sector. A digital signature ensures the integrity of and the signer's association with the signed digital document, thereby guaranteeing its authenticity for legal purposes. This paper proposes an integrated platform from the XETID Company that aims to provide Cuban society with a secure digital signature service at large. The solution involves a public key infrastructure, a digital signature server, a timestamp server, and a secure service for managing passwords and performing cryptographic operations. Additionally, tool typologies for utilizing the digital signature service are proposed. The work describes each component, its essential function, and the handling of passwords necessary to achieve a robust and secure digital signature service. Likewise, it outlines essential tools for further development so as to accomplish the desired objective.

Keywords: *public key infrastructure, timestamp service, digital signature server, secure password protection*

Introducción

La firma digital se ha convertido en una herramienta cada vez más demandada por las instituciones y la sociedad cubana en general. En el proceso de informatización de los servicios, la firma digital es indispensable y, con ella, se garantiza la integridad y la asociación con el firmante de un documento digital, asegurando así la autenticidad de este y su validez legal. Pero no se trata solo de validar

documentos, la firma digital es la llave que permite reducir papeles, agilizar procesos y garantizar trazabilidad legal en cada documento.

En 2016, Cuba inició la formalización de las firmas digitales mediante la adopción de la infraestructura de clave pública (PKI), según los lineamientos marcados por la *Resolución 2 del Ministerio del Interior*, luego derogada por el *Decreto-Ley 79/2023*[1] y su reglamento el *Decreto 106/2024*[2]. Esta infraestructura garantiza la emisión de certificados digitales, que son documentos electrónicos que acreditan la identidad de una persona o entidad por lo que podrían tener asociada un par de claves (**clave pública y clave privada**) que les permite asociar su identidad en el mundo digital.

En 2018, el *Decreto-Ley* 370 sobre la informatización de la sociedad en Cuba, reconoció de forma legal la validez de los documentos firmados electrónicamente en el país. En 2022, el Ministerio del Interior (MININT) y el Consejo de Ministros crearon reglas más claras para el uso de firmas digitales en órganos gubernamentales, el Banco Central de Cuba y agencias locales. Ya en la actualidad el Decreto Ley 79/2023 y su reglamento el Decreto 106/2024 sientan las bases jurídicas para las infraestructuras de clave pública en Cuba.

El uso de una PKI como componente individual no garantiza un despliegue adecuado de la firma digital, o sea, solo avala la emisión de certificados digitales que están asociados a la identidad. El manejo de las claves es de suma importancia cuando se diseña una plataforma para la firma digital. En este escenario se trabaja con criptografía asimétrica (Menezes, 1996; Cohen, 2006), así cada persona o entidad contará con un par de claves, es decir, una **clave pública** que como su nombre lo indica, es de conocimiento público y una **clave privada** que debe estar muy bien resguardada. Existen estándares tanto de *software* PKCS#12 (.p12, .pfx, .jks) como de *hardware* (módulos

[1] Decreto Ley 79/2023 "Sobre el desarrollo, la aplicación y uso de los dispositivos de protección criptográfica y servicios en la esfera de la criptografía en la República de Cuba" (GOC-2024-527-O89)

[2] Decreto 106/2024 Reglamento del Decreto Ley 79 "Sobre el desarrollo, la aplicación y uso de los dispositivos de protección criptográfica y servicios en la esfera de la criptografía en la República de Cuba", de 26 de octubre de 2023 (GOC-2024-528-O89)

de seguridad de *hardware*, HSM) que permiten, mediante algoritmos criptográficos, asegurar las claves (Gitlan, 2025). La clave pública es usada en el proceso de **cifrado** y la clave privada en el proceso de **descifrado** de la información. Es esencial garantizar que las claves privadas no viajen por canales inseguros o espacios que faciliten la captura de estas por intrusos, en infraestructuras críticas es importante establecer políticas y procedimientos para el manejo de claves que sean robustos y con altos niveles de seguridad. Kuzminykh (2021) hace un estudio detallado de varias herramientas para el manejo de claves (*KMS, Key Management Service*) donde se definen criterios como *software* libre o de pago, almacenamiento seguro, soporte para HSM, uso de *logs* de auditorías, entre otros.

Además, son necesarias herramientas para llevar a cabo la firma de forma transparente y sencilla. Estas herramientas pueden ser diversas, es decir, una APK para celulares, una app para escritorio u otro tipo de aplicación siempre que tenga garantías de seguridad. Por último es esencial un servidor de firma digital, este debe estar dotado de buenas funcionalidades, debe interactuar con un servicio de sellado de tiempo para alcanzar la validez de un documento firmado aún cuando el certificado haya caducado y en ese caso, los sellos de tiempo son esenciales. En el entorno cubano, diferentes empresas hacen un gran esfuerzo para el desarrollo de la firma digital, tanto para fines comerciales como para su desarrollo empresarial. Algunos ejemplos son: XETID, Softel, Datys, Tecnomática y Segurmática que tienen PKI certificadas por el MININT (Hernández, 2024). Cuando se revisa en cada propuesta de infraestructura de clave pública, la integración de todos los elementos antes mencionados no es alcanzado en su totalidad.

Basado en las razones anteriores, en este trabajo se traza como objetivo: proponer una plataforma integrada y segura para la firma digital, en el entorno de la empresa XETID. Con ese propósito se diseña la interacción general de la plataforma y se plantea para cada uno de sus componentes los diseños y herramientas, así como las funcionalidades deseadas y los estándares de seguridad a alcanzar.

Materiales y métodos

La presente propuesta está basada en la experiencia adquirida en el desarrollo y despliegue de Rinho PKI (desarrollado por: Instituto de Criptografía de la Universidad de la Habana) en la infraestructura de la empresa XETID, basada principalmente en criptografía asimétrica con curvas elípticas (Menezes, 2006) y en armonía con los estándares internacionales en este campo. Se debe mencionar además que el componente principal, la PKI, ya tiene un grado de madurez importante y que se cuenta con todos los recursos e infraestructuras para emprender la propuesta aquí expuesta.

Para potenciar la informatización de la sociedad cubana y optimizar los servicios que la empresa XETID ofrece a terceros, se identifica la necesidad de desarrollar nuevos proyectos que integren el ecosistema de la firma digital. Cabe aclarar, que las funcionalidades propuestas para cada componente son mínimas y pueden ampliarse según las necesidades que surjan durante el desarrollo. No obstante, los requisitos aquí expuestos para el tratamiento de las claves se mantienen estrictos. El presente trabajo se centra en los protocolos que garantizan una interacción segura entre los componentes, sin profundizar en los detalles funcionales internos de cada uno.

La propuesta cuenta con seis componentes fundamentales:

1. **Infraestructura de clave pública**: una PKI incluye las políticas, las funciones, el *hardware*, el *software* y los procedimientos necesarios para crear, administrar, distribuir, usar, almacenar y revocar certificados digitales. Tiene como objetivo facilitar la transferencia electrónica segura de información para una serie de actividades en red. Como, por ejemplo: el comercio electrónico, la banca y el correo electrónico confidencial, entre otros. Intervienen en el proceso:
   - **Certificados digitales**: credenciales electrónicas que vinculan la identidad del titular del certificado a un par de claves que pueden utilizarse para cifrar y firmar información.
   - **Autoridad de certificados (CA)**: una entidad de confianza, autorizada y certificada por el MININT, que emite certificados digi-

tales. La CA gestiona todos los aspectos de los certificados PKI, incluido su ciclo de vida.

- **Autoridad de registro (RA)**: se encarga de aceptar las solicitudes de certificados y autenticar a la persona u organización que las presenta.
- **Autoridad de validación (VA)**: se encarga del proceso de validación de certificados a partir de servicios de OCSP (*Online Certificate Status Protocol*) y CRL (*Certificate Revocation List*).
- **Aplicación web de gestión centralizada**: es una web a partir de la cual los usuarios pueden solicitar y gestionar sus certificados digitales.

2. **XFirma APK**: es una aplicación para celulares que permite, la firma del lado del usuario y avala el manejo privado de sus claves en el entorno de su dispositivo, es decir, este usaría su archivo de claves .p12 para el proceso de firma o podría obtener un certificado desde la CA a partir de una solicitud CSR construida por la misma aplicación XFirma, cuestión más recomendable. Posibilita, además, la validación de certificados y documentos firmados por la APK o por terceros. Este tipo de aplicación tiene potencial para ampliar sus funcionalidades libremente, lo que garantiza el cifrado de documentos, compartir documentos entre usuarios bajo ciertos requerimientos, el envío de documentos cifrados por correo, previo intercambio de claves, entre otras funcionalidades.
3. **Servidor de firma**: se encarga de gestionar la firma digital de documentos en formato .pdf, .xml, códigos, entre otros, y se usan fundamentalmente estándares europeos para la firma digital (eIDAS, Reglamento [9/10/2014]). Es factible su uso en entornos corporativos o para el desarrollo del gobierno electrónico. Debe ser flexible en las interfaces para clientes certificando su uso mediante API Rest, servicios web, Internet, o a través del uso de una herramienta de firma integrada al servidor para el cliente. Para la firma de un documento, el servidor gestiona el aspecto de la firma, el proceso de conformación del documento firmado y además la integración en este del sello de tiempo.

4. **Servidor TSA**: un servidor de sellado de tiempo RFC3161 cumple una función esencial en la protección a largo plazo de los registros de datos. Proporciona la prueba de que los datos existían en un momento determinado y que no han sufrido cambios, ni siquiera un solo bit binario, desde su certificación y sellado de tiempo. El servicio de sellado de tiempo es esencial en una PKI. Es recomendable la renovación por lo menos anual de los certificados de firma usado por el servidor TSA.

5. **Servicio de manejo de claves (SMC) para la firma digital**: en el funcionamiento de un servidor de firma digital es esencial hacer un manejo adecuado de las claves y su resguardo, así en la presente propuesta se habilita este componente donde el usuario o entidad se registra y solicita la generación de sus claves para la firma digital. Este servicio puede tener las siguientes funcionalidades: gestión del ciclo de vida completa, incluyendo su creación, habilitación, deshabilitación, eliminación, rotación, modificación y la asignación de alias; gestión de claves de datos, incluyendo la creación, el cifrado y el descifrado de claves de datos; creación y gestión de claves simétricas; entre otras funciones.

A partir del uso del servicio de solicitud de certificados usando CSR de la CA, se genera localmente la clave privada y pública en el SMC y se protege la llave privada, se crea la solicitud CSR y se solicita el certificado correspondiente firmado por la CA. De esta forma, se garantiza la existencia de claves para el usuario o la entidad en la SMC. Además, las claves están altamente protegidas. Esta protección es recomendada con el uso de un HSM. Es importante señalar que en este entorno se hacen los procesos criptográficos necesarios con las claves aquí almacenadas (firma, cifrado, entre otros) y se utilizan solicitudes con el estándar PKCS#11, así se garantiza que estas claves no salen del entorno seguro.

6. **XFirma Corp.**: es una aplicación web que gestiona la firma digital para todos sus usuarios o entidades registradas, usa una o varias de las interfaces del servidor de firma para gestionar la firma de documentos, XML o código. En este entorno, no es seguro el uso de los .p12 de los usuarios, dado que tendrían que viajar hasta el

servidor de XFirma Corp. además de confiar en una entidad no diseñada para la protección de claves. Si la intención del usuario es firmar con su .p12 entonces lo más seguro es usar XFirma APK. Esta aplicación web también permite incorporar funcionalidades relacionadas con el intercambio de documentos firmados entre usuarios mediante el intercambio previo de claves o el uso de un servicio de correo seguro.

El uso de un servidor de identidad para la integración de los componentes en armonía con sus funcionalidades es de suma importancia. Se lograría así obtener un token de acceso único para los componentes relacionados.

Para los diseños aquí descritos se empleó el aplicativo *draw.io* que permitió de forma libre definir las interacciones en cada uno de los componentes propuestos.

Resultados y discusión

La Figura 1 muestra el diseño sin detalles funcionales de los componentes que intervienen en la propuesta antes comentada y su interrelación.

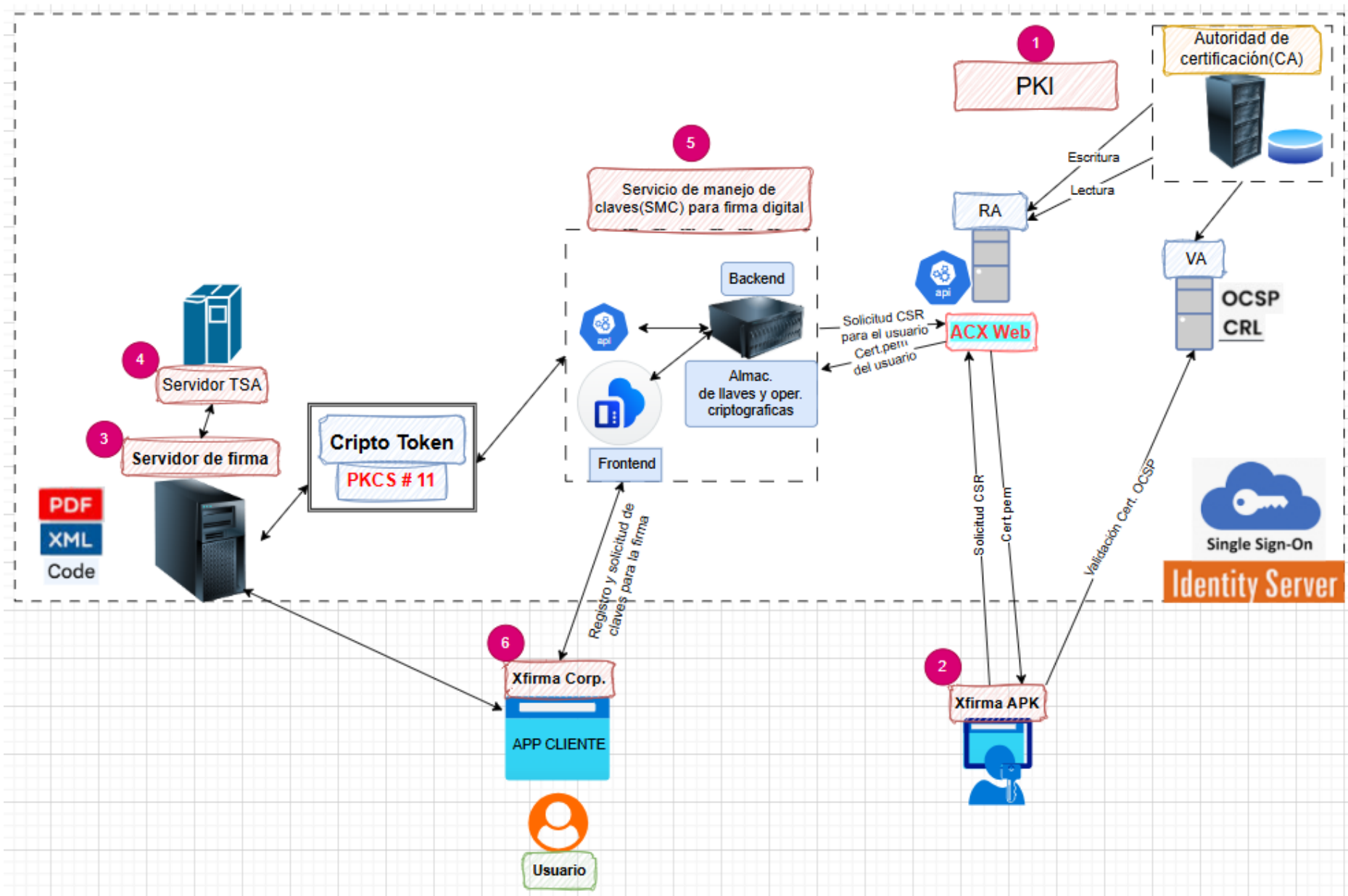

Figura 1. Desglose numerado de los componentes y su interacción dentro del ecosistema de la firma digital

Desglose de interacción seguras entre componentes y funciones relacionadas con la firma digital

1. **Interacción XFirma APK o app con ACX**: al utilizar la librería Bouncy Castle con un generador de número aleatorio propio, se obtienen claves pública y privada en el dispositivo del usuario. Luego debe mantenerse en resguardo la clave privada utilizando archivos cifrados y, después, se genera la solicitud de certificados CSR y se envía a la RA a través de la interfaz de usuario definida. Luego descarga el certificado dado en un archivo .pem y firmado por la CA. A continuación se debe construir el contenedor de claves mediante un archivo .p12 que será guardado en un lugar seguro por la aplicación. Estas claves estarán asociadas al usuario que previamente se registró en la aplicación mediante un formulario de registro adaptado a sus necesidades y requerimientos en su interacción con la PKI. Por último se puede firmar un documento del lado del usuario en su dispositivo, la aplicación valida la firma y además el certificado usado es validado contra el OCSP o usando CRL.
2. **Interacción de XFirma Corp. con el SMC**: el cliente se registra y crea su perfil en el SMC, solicita además su correspondiente par de claves para la firma digital. En este caso, el servidor se encarga, con los datos del usuario, de hacer la solicitud con un CSR de su certificado a la CA. Con el certificado y la clave privada debidamente protegida, se crea y almacena su contenedor .p12 en el SMC. De esta forma ya el usuario tendrá su registro y las claves para la firma digital en el servidor SMC. Es importante hacer notar que el SMC puede tener muchas funcionalidades que no es objetivo discutir en esta propuesta.
3. **Interacción de XFirma Corp. con el Servidor de Firma**: el usuario solicita la firma de un documento en su perfil en XFirma Corp. Esta aplicación web emplea la interfaz de usuario establecida envía al Servidor de Firma, el IDu del usuario, el IDc del certificado y el documento a firmar (doc). Se supone que el usuario ya tiene creado su perfil de firma en el Servidor de Firma con el aspecto para la firma configurado.

4. **Interacción del Servidor de Firma con el SMC**: en este caso, el Servidor de Firma calcula el *hash* del documento (**h=hash(doc)**) enviado por XFirma Corp. y envía para el SMC el IDu, IDc y el **valor *hash* h** del documento usando el estándar PKCS #11 con la orden además de firmar el valor *hash* h. El servidor SMC, por su lado, firma el valor *hash* h del documento con las claves y el usuario especificado, finalmente devuelve ese *hash* firmado al Servidor de Firma.
5. **Interacción del Servidor de Firma con el Servidor TSA**: el Servidor de Firma envía al Servidor TSA el *hash* firmado para el sellado de tiempo, el Servidor TSA agrega el sello de tiempo al *hash* firmado y firma este con sus claves. Es agregado además el certificado del TSA y la cadena de certificación obteniendo así el **Timestamp Token** que es enviado al Servidor de Firma.
6. **Interacción Servidor de Firma con XFirma Corp.**: ahora el Servidor de Firma construye el documento firmado y lo envía de regreso **XFirma Corp**. Así el usuario obtiene el documento firmado sin la necesidad de que sus claves estén viajando por la infraestructura.

Herramientas recomendadas en los servidores

- **Infraestructura de clave pública**: es muy usada en los entornos empresariales EJBCA de la empresa KEYFACTOR con una larga experiencia en desarrollos para la seguridad de la información. Esta herramienta tiene una versión *community* y de código abierto que permite el desarrollo sobre esta versión. Se programa en Java y se sustenta en la librería criptográfica Bouncy Castle. La versión *Enterprise* de EJBCA tiene más funcionalidades, pero es de pago. Para un entorno de producción basado en EJBCA se promueve el uso en el contexto cubano de Rhino PKI, desarrollado y comercializado por el Instituto de Criptografía de la Universidad de La Habana.
- **XFirma APK**: puede desarrollarse una APK para Android usando una librería criptográfica en correspondencia con los tipos de documentos a firmar. Existen varias que son libres y, si se sigue el desarrollo de la PKI hay una forma de utilizar en Android la librería criptográfica Bouncy Castle teniendo así una librería más completa.
- **XFirma Corp.**: Es un desarrollo web que puede integrar diferentes tecnologías y lenguajes, en dependencia de las necesidades.

Bouncy Castle es una librería desarrollada para los lenguajes Java y C#, por tanto, al usar JavaScript o Python para llevar a cabo el desarrollo web cambiarían las librerías criptográficas a usar. También es importante tener en cuenta que se necesitan librerías que hagan tratamiento de la firma digital, validación y manipulación de certificados digitales con el estándar X509. Por ejemplo, si se decide usar el lenguaje JavaScript, en este caso una librería bastante completa es **node-forge** que es similar a Bouncy Castle. Como propuesta completa se tiene:

Backend: Node.js + Express/Fastify, TypeScript (opcional, pero recomendado), Jest para pruebas.

Para criptografía: node-forge / libsodium; bcrypt para passwords; jsonwebtoken para autenticación.

Para base de datos: PostgreSQL con pgcrypto o MongoDB con field-level encryption.

Para frontend: React/Vue/Angular, Web Crypto API para operaciones del cliente.

- **Servidor de Firma**: Se propone el uso de la versión *community* del servidor SignServer[4] de la empresa KEYFACTOR[5] que es de código abierto y sobre esa versión desarrollar un servidor de firma en correspondencia a las necesidades. En la Figura 2 se muestra la interacción del usuario con el servidor y las interfaces disponibles para aplicaciones clientes o para usuario con el fin de disfrutar de los servicios del Servidor de Firma.

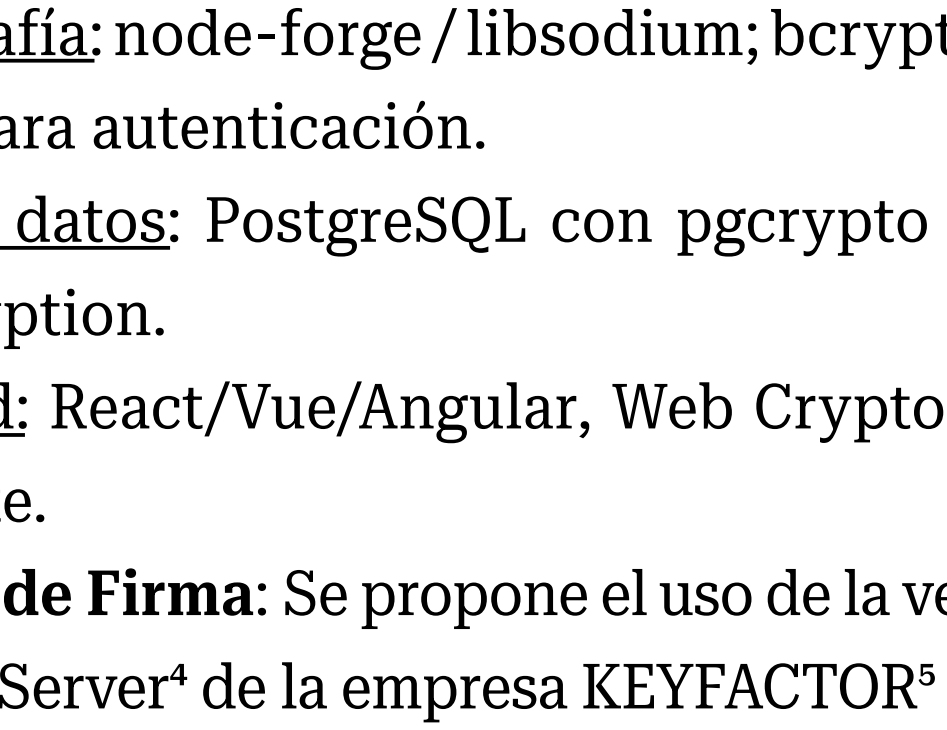

Figura 2. Representación de las funciones del Servidor de Firma

[4] https://www.signserver.org/

[5] https://www.keyfactor.com/

- **Servidor TSA**: Existe un ecosistema de herramientas que se pueden usar como servicio TSA para la firma digital o desarrollar sobre ellas. Por ejemplo: <www.freetsa.org>, <http://timestamp.digicert.com>, OpenTSA, entre otras opciones. No obstante, la instauración de un servidor TSA para producción requiere de desarrollos en correspondencia a la demanda del servicio. En el caso empresarial, para producción puede ser recomendable usar el servidor TSA incluido en la plataforma EJBCA que permite el trabajo con imágenes Docker, balance de carga y adaptación a la demanda (Figura 3).

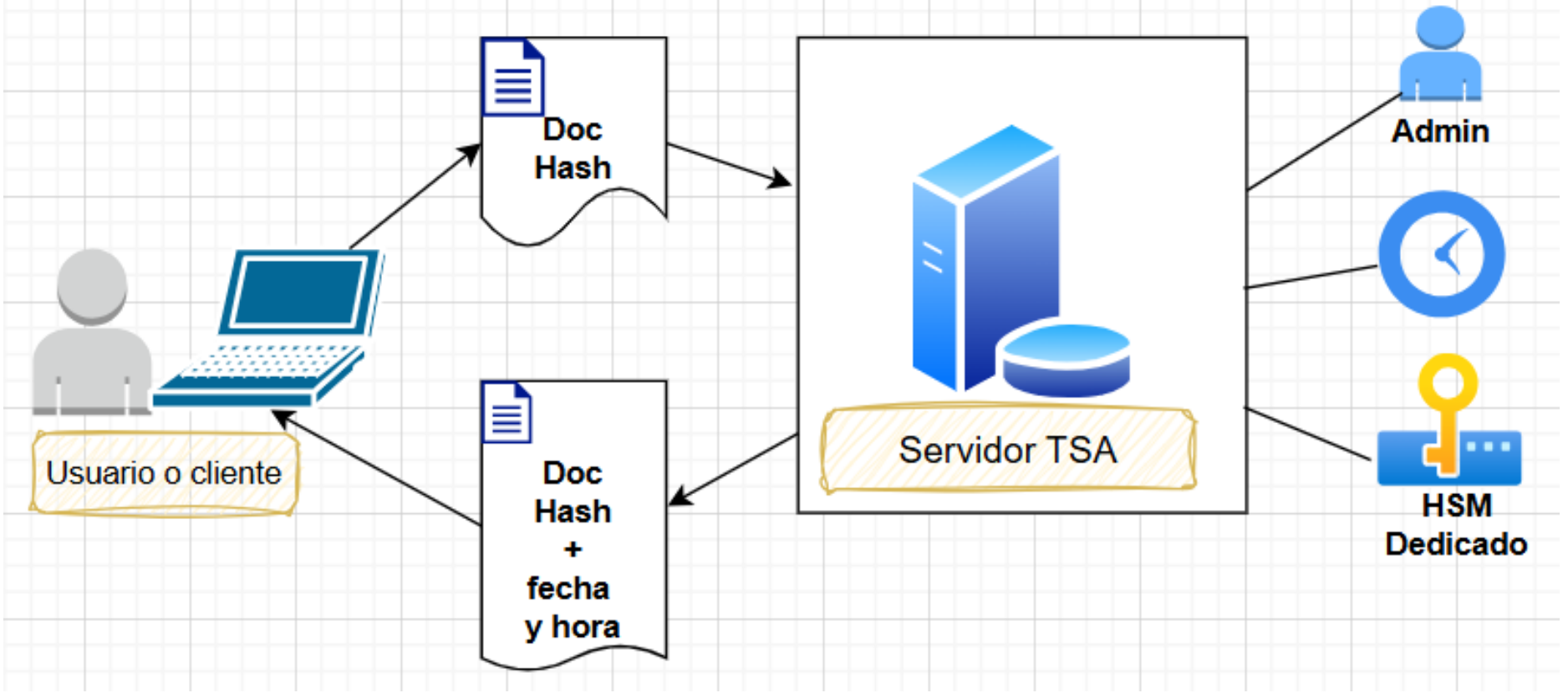

Figura 3. Estructura organizativa recomendada para un Servidor TSA

- **Servicio de Manejo de Claves (SMC) para la firma digital**: para los servicios de manejo de claves existen muchas opciones en la nube con este fin. Kuzminykh (2021) hace un análisis de una amplia gama de herramientas que realizan esta función con criterios bien delimitados y permiten tomar una decisión al momento de elegir una de ellas. En el entorno de la empresa XETID es recomendable llevar a cabo un desarrollo propio usando algunos de los servicios libres con estos fines como SoftHSMV2, que se integra fácilmente con el SignServer de KEYFACTOR y facilita la interacción entre el servidor de firma y el Servidor SMC usando el estándar PKCS#11. Es importante hacer notar que es una salida a la ausencia de una HSM profesional, pero no es la opción recomendada. No obstante, si se extrema la seguridad en la infraestructura y el servicio, podría ser una opción viable.

El desarrollo de una plataforma de esta envergadura requiere dedicación y entrega de todo un equipo de trabajo para el logro adecuado de una integración segura y amigable al usuario final. El trabajo modular de cada componente es esencial con vistas al logro de los avances deseados.

Conclusiones

A través de la investigación, se constata la necesidad de una plataforma con potencial para contribuir a la informatización de la sociedad cubana con el uso de la firma digital. La diversidad de herramientas existente de código abierto para cada uno de los componentes descritos obliga a realizar una revisión profunda para evaluar su factibilidad en el despliegue a nivel de producción. En todos los entornos seguros son recomendables el uso de módulos HSM dedicados, pero dependiendo del contexto podría sustituirse por uno similar a nivel de *software*, lo que garantiza fortalecer la seguridad con medidas adicionales, aunque no es lo recomendable. Es de suma importancia, que el servidor de firma tenga diferentes opciones de interfaz de usuarios con la finalidad de diversificar los tipos de servicios a usuarios o clientes. En los proyectos futuros de la empresa se promueve dar continuidad a los desarrollos actuales integrando los servicios descritos en cada uno de los componentes de la plataforma propuesta.

Referencias bibliográficas

Cohen, H., Frey, G., Avanzi, R., Doche, C., Lange, T., Nguyen, K. y Vercauteren, F. (2006). *Handbook of elliptic and hyperelliptic curve cryptography*. Chapman and Hall/CRC.

Gitlin, D. (2025, 27 de octubre). *Cómo almacenar claves privadas de forma segura*. SSL Dragon. https://www.ssldragon.com/es/blog/mejores-practicas-almacenar-clave-privada/.

Hernández, A. (2024, 21 de febrero). *La firma digital, una herramienta clave para la informatización de la sociedad cubana*. Cubadebate. http://www.cubadebate.cu/especiales/2024/02/21/la-firma-digital-una-herramienta-clave-para-la-informatizacion-de-la-sociedad-cubana/.

Kuzminykh, L., Ghita, B. V. y Shiaeles, S. (2021). *Comparative analysis of cryptographic key management systems*. arXiv. https://doi.org/10.48550/arXiv.2109.09905.

Menezes, A. J., van Oorschot, P. C., y Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC Press.