Verificación de edad en línea basada en extensión de navegador y pruebas de conocimiento cero

Alejandro Manuel López Gómez[1,2], Alonso Alfredo Rodríguez Rodríguez[2,4], Ofelia Tejerina Rodríguez[3], Julián Inza Aldaz[3,5], Gregorio López López[1,2]
[1]Instituto de Investigación Tecnológica (IIT), Universidad Pontificia Comillas
[2]Escuela Técnica Superior de Ingeniería (ICAI), Universidad Pontificia Comillas
[3]Observatorio LegalTech Garrigues – ICADE, Universidad Pontificia Comillas
[4]Polygon Labs
[5]EADTrust
amanlopezgomez@alu.icai.comillas.edu, alonso@polygon.technology, otejerina@comillas.edu, jinza@ext.comillas.edu, gllopez@icai.comillas.edu

Resumen- **La verificación de edad en línea se ha convertido en un desafío clave en la protección de menores y el cumplimiento normativo, a menudo entrando en conflicto con la privacidad del usuario. En este artículo, presentamos una solución basada en una extensión de navegador, tecnología *blockchain* y pruebas de conocimiento cero (ZKP, por sus siglas en inglés), que permite verificar la mayoría de edad sin revelar información personal sensible. Esta propuesta ofrece un equilibrio entre anonimato y usabilidad, beneficiando tanto a los usuarios, que pueden navegar con mayor privacidad, como a los proveedores de contenido adulto, permitiéndoles verificar la mayoría de edad sin almacenar datos innecesarios.**

***Index Terms*- blockchain, plug-in, verificación de edad, zero knowledge proofs**

Tipo de contribución: *Investigación original*

I. Introducción

En la era digital, la identidad en línea se ha convertido en un activo valioso, pero también en una vulnerabilidad. La recopilación masiva de datos por parte de gobiernos, empresas y ciberdelincuentes ha generado una creciente preocupación por la privacidad y la seguridad personal. Proteger la identidad digital no solo implica evitar fraudes o robos de datos, sino también preservar la libertad de expresión y el derecho al anonimato. Este anonimato es especialmente relevante en situaciones donde el estigma social o la discriminación pueden afectar la vida personal y profesional de un individuo. Por lo tanto, hay determinadas situaciones en las que sólo es necesario comprobar que el usuario cumple con un determinado requisito, sin necesidad de desvelar su identidad.

Un ejemplo claro es el acceso a contenido para adultos en línea, un sector que, a pesar de su legalidad en muchos países, sigue rodeado de tabúes y riesgos de exposición. La filtración de datos personales relacionados con este tipo de contenido puede dar lugar a situaciones de acoso o incluso represalias en entornos laborales y familiares. Por ello, el uso de herramientas de privacidad, como redes privadas virtuales (VPN), navegación anónima y métodos de pago discretos, se ha vuelto fundamental para quienes desean ejercer su derecho a la intimidad sin temor a consecuencias no deseadas.

En este contexto, el acceso a contenido para adultos en línea plantea un desafío importante tanto a nivel técnico como regulatorio: garantizar que solamente aquellos usuarios mayores de edad puedan consumirlo sin comprometer su privacidad. En muchos países, las regulaciones exigen mecanismos de verificación de edad, pero las soluciones actuales suelen ser invasivas, exigiendo el uso de documentos de identidad, tarjetas de crédito o registros en plataformas centralizadas. Esto no solo pone en riesgo la información personal de los usuarios, sino que también genera fricciones en la experiencia de navegación.

La raíz del problema radica en encontrar una solución que encuentre un equilibrio entre el cumplimiento normativo y garantizar la privacidad del usuario. Exigir datos personales para demostrar la mayoría de edad introduce riesgos como filtraciones de información, rastreo de actividad en línea y la pérdida de anonimato en un ámbito que, por su naturaleza, muchos usuarios prefieren mantener en privado. En este contexto, a nivel nacional ha surgido una solución técnica para la verificación de edad, la “Cartera Digital Beta”, que permite a los usuarios demostrar su mayoría de edad mediante credenciales digitales verificables.

En este artículo, se presenta una alternativa a esta solución basada en una extensión de navegador que emplea pruebas de conocimiento cero (*Zero Knowledge Proofs* - ZKP) para permitir la verificación de edad de manera anónima y eficiente. Posterior a la descripción de dicha solución se realizará una comparación con la “Cartera Digital Beta”, analizando las características de ambas soluciones en términos de privacidad, seguridad y usabilidad.

II. Contexto Legal

Los sistemas de verificación de edad (SVE) para limitar el acceso en línea a contenidos para adultos siguen siendo, desde hace años, un desafío recurrente en la protección de la infancia y la juventud. La solución no parece sencilla, ni siquiera única. Aunque en los últimos tiempos los esfuerzos por encontrar una propuesta suficientemente eficaz se han intensificado, la realidad es que las soluciones - técnicas y normativas - conocidas hasta la fecha, no acaban de establecer un marco sólido de confianza.

El legislador se debate entre la protección de los menores y la protección, al mismo tiempo, de los derechos y libertades de los consumidores adultos [1]. Por una parte, hay quien considera que los SVE pueden afectar a derechos y libertades de los propios menores, si los criterios que etiquetan contenidos "para adultos" son demasiado restrictivos o conservadores [2], también en las redes sociales que frecuentan, como sería el caso de Instragram, Tik Tok e incluso Onlyfans. Por otra parte, es altamente probable que los adultos renuncien a acceder determinados servicios o contenidos, como la pornografía o las apuestas en línea, si no confían suficientemente en la seguridad del sistema responsable del tratamiento, o en la correcta custodia de los datos identificativos que les solicitarían.

En Estados Unidos, Texas fue uno de los primeros Estados en promover legislación específica al respecto, la *Texas House Bill 896*, relativa a la "Prohibición del uso de plataformas de medios sociales por menores", de 2022, que siguieron Louisiana y Arkansas con medidas equivalentes. Para verificar la edad se exigía una fotografía del usuario y la licencia de conducir o similar, junto con la obligación del proveedor de contenidos de almacenarlo exclusivamente mientras procedía a la verificación y, una vez hecho, eliminarlo totalmente. La actual *Texas House Bill 1181*, relativa a la "Publicación o distribución de material sexual perjudicial para menores en un sitio web de Internet; sanción civil", de 2023, exime de responsabilidad en la verificación a los motores de búsqueda y a las plataformas de redes sociales, imponiéndosela a las empresas prestadoras del servicio para adultos si no verifican correctamente la edad del usuario, y esto causa daños a algún menor. Hoy son 19 los Estados que tienen leyes de verificación de edad parecidas y, por ejemplo, el sitio web Pornhub está bloqueado en 17 Estados [3]. Pero, "¿qué nivel de carga puede imponerse al acceso a la libertad de expresión en nombre de la protección de los niños frente al visionado de pornografía?". Esta cuestión ha sido llevada ante la Corte Suprema, *Free Speech Coalition et al. v. Paxton* [4], y se espera que sea resuelta en verano de 2025.

En Europa, la regulación de los SVE es un tema complejo que continúa avanzando sin una respuesta definitiva. Estos servicios están siendo desarrollados bajo varios marcos regulatorios, entre los que se incluyen el Reglamento (UE) 910/2014 (eIDAS), que establece las bases para la identificación electrónica y los servicios de confianza en transacciones electrónicas, y su revisión más reciente, el Reglamento (UE) 2024/1183 (eIDAS2). Este último introduce el Marco Europeo de Identidad Digital y la "Cartera de Identidad Digital" como método para la identificación en línea. Además, el Reglamento (UE) 2022/2065 (DSA) regula el mercado único de servicios digitales, modificando la Directiva 2000/31/CE.

Con el objetivo de mejorar la fiabilidad de los SVE, en enero de 2024 la Comisión Europea, a través de su Dirección General de Redes de Comunicación, Contenido y Tecnologías (Connect), creó un "Grupo de Trabajo sobre Verificación de la Edad". Este grupo tiene la misión de fomentar la cooperación con las autoridades nacionales de los Estados miembros que tienen experiencia en la verificación de la edad, para desarrollar prácticas más seguras y efectivas.

Por otro lado, en febrero de 2025, el Comité Europeo de Protección de Datos (CEPD), en colaboración con la Agencia Española de Protección de Datos (AEPD), adoptó un "Dictamen sobre la determinación de la edad para el uso de servicios en línea que requieren una edad mínima para acceder a ellos", basado en el Reglamento General de Protección de Datos (RGPD). Este dictamen establece principios clave para la implementación de los SVE, con el fin de garantizar que se respeten los derechos fundamentales de los usuarios.

Algunos Estados europeos han publicado sus propios criterios para el desarrollo de cualquier sistema de verificación, como Alemania (*Punktepapier einer gemeinsamen deutschen Position zum Thema Altersverifikation unter Inbezugnahme auf den DSA.* 31 de octubre de 2024, BfDI) o Reino Unido (*Age assurance for the Children's code*. 2024, ICO). Francia incluso ha aprobado legislación específica (*LOI n° 2023-566 du 7 juillet, 2023, visant à instaurer une majorité numérique et à lutter contre la haine en ligne*) y un detallado informe de especificaciones técnicas (*Référentiel déterminant les exigences techniques minimales applicables aux systèmes de vérification de l'âge mis en place pour l'accès à certains services de communication au public en ligne et aux plateformes de partage de vidéos qui mettent à disposition du public des contenus pornographiques*, 2024). En España, la *Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual* obliga a las "plataformas de intercambio de vídeos a establecer sistemas de verificación de edad respecto a contenidos que puedan perjudicar a los menores" y es la Comisión Nacional de los Mercados y la Competencia (CNMC) la que evaluará la idoneidad de estos sistemas.

Entre otros, el Ministerio del Interior, el Ministerio de Juventud e Infancia, la CNMC, la Fábrica Nacional de Moneda y Timbre (FNMT) como entidad certificadora, y la AEPD, forman parte del Grupo de Trabajo interministerial que ha creado el Consejo de Ministros del Gobierno. Concretamente, la autoridad de control de protección de datos es la que ha venido liderando los trabajos de esta iniciativa pública, que se desarrollará e implementará, bajo el mandato del Ministerio para la Transformación Digital y de la Función Pública (MTDFP). En 2023 la AEPD publicó en su sitio web el "Decálogo de principios Verificación de edad y protección de personas menores de edad ante contenidos inadecuados" acompañado de una solución técnica que incorporaría en una aplicación móvil denominada "Cartera Digital Beta", y que promete cumplir su objetivo de verificar la edad del usuario sin afectar su privacidad. Este proyecto está además encuadrado en el marco legal que propone el "Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales" en el que trabaja en este momento el Gobierno español [5].

Si bien esta propuesta podría formar parte de la solución, porque plantea independizar la verificación de edad de los proveedores de identidad (no es preciso crear nuevos sistemas de identidad digital), fomentando así la neutralidad tecnológica y el libre mercado de opciones, con un sistema de claves públicas y privadas implementadas en una aplicación móvil y terceros de confianza intermediarios para la

verificación, no ha logrado todavía generar suficiente confianza en los usuarios. Lo cierto es que hasta la fecha ningún SVE se ha posicionado con fuerza en el mercado, ni se ha proclamado como "fiable" ni ha sido implementado en el sector público o privado [6].

III. Requisitos de los SVE

Una solución de verificación de edad en línea debe cumplir una serie de requisitos que garanticen el anonimato del usuario, así como la usabilidad del sistema tanto para éste como para el proveedor de contenido adulto. Estos requisitos han sido recopilados desde diferentes fuentes como el "Statement 1/2025 on Age Assurance" europeo [7] y Decálogo de Principios para la Verificación de Edad y Protección de Menores ante Contenidos Inadecuados publicado por la AEPD [8]. También se incluyen conclusiones propias fruto del desarrollo realizado.

El documento redactado por la AEPD establece diez principios fundamentales que todo sistema de verificación de edad debe cumplir desde un nivel de gestión, es decir, no se comentan posibles implementaciones o prácticas técnicas recomendadas. En primer lugar, el sistema debe evitar que se pueda realizar la identificación y rastreo de menores por parte de alguno de los actores involucrados en el proceso u otros terceros potencialmente maliciosos, previniendo así riesgos adicionales como la explotación o el abuso. La verificación de edad debe enfocarse en confirmar quién está autorizado a acceder a contenidos restringidos, sin exponer la identidad de los menores y sin ofrecer más información.

Otro principio clave es que la obligación de verificar la edad solo debe aplicarse a contenidos específicamente restringidos para adultos, evitando barreras innecesarias para el acceso a información general. Además, la verificación debe realizarse con métodos confiables y sin revelar datos sensibles, como la fecha de nacimiento del usuario. También se establece que todo sistema debe evitar el perfilado de usuarios basado en su navegación, así como la restricción de cualquier mecanismo que vincule la actividad de un usuario entre distintas plataformas para evitar su posible rastreo y posterior identificación

El decálogo de la AEPD también resalta la importancia de garantizar el derecho de los padres a decidir sobre los contenidos a los que acceden sus hijos, respetando la diversidad cultural y educativa de cada familia. Además, los sistemas de verificación de edad deben diseñarse de manera que respeten los derechos fundamentales, como la privacidad, la libertad de expresión y el acceso a la información. Por último, se subraya la necesidad de un marco de gobernanza claro, con mecanismos de supervisión y auditoría que garanticen la eficacia del sistema y la protección de los derechos de todos los usuarios.

Durante el desarrollo de la prueba de concepto, además de los requisitos impuestos por agencias como la AEPD, se han identificado requisitos técnicos que una solución de verificación de edad que busque su implantación a una escala mediana o elevada debe tener en cuenta. Desde el punto de vista de la privacidad del usuario, la solución debe garantizar la minimización de datos, es decir, se debe verificar la edad sin recopilar ni procesar información personal innecesaria. El único dato que debe validarse es la mayoría de edad, sin revelar otros detalles personales.

Además de otras regulaciones, es crucial que la solución cumpla con las normativas de privacidad, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea, que exige el consentimiento explícito del usuario y la garantía y capacidad de destrucción los datos recopilados [9]. A nivel técnico esto quiere decir que ninguna solución podrá almacenar información acerca de sus usuarios, y aquella que fuese necesaria para su verificación debe ser destruida apropiadamente una vez se haya hecho uso de ésta.

En cuanto a la usabilidad de cara al usuario final, la solución debe ser fácil de instalar y utilizar. El proceso de verificación de edad debe ser lo más sencillo posible, sin requerir conocimientos técnicos. Debe poder completarse rápidamente, garantizando una experiencia de usuario fluida y sin fricciones. La verificación debe ser compatible con los principales navegadores y dispositivos, garantizando que cualquier usuario, independientemente de la plataforma que utilice, pueda acceder al contenido adulto sin dificultades.

Desde el punto de vista del proveedor de contenido, la solución debe facilitar el cumplimiento normativo. El proveedor debe poder verificar que los usuarios cumplen con el requisito de mayoría de edad sin necesidad de almacenar información personal sensible. La usabilidad para el proveedor de contenido es también esencial. La integración debe ser sencilla en las plataformas existentes, sin requerir cambios significativos en la infraestructura.

Respecto a su desarrollo, toda solución debe presentar un carácter modular y dinámico, ofreciendo la capacidad de incluir o retirar servicios sin afectar al funcionamiento del sistema. Por último, se debe ofrecer transparencia y auditoría, permitiendo que el proceso de verificación sea fácilmente auditado, aumentando la confianza en el sistema de las partes involucradas.

IV. Solución técnica propuesta

La solución ideada consta de tres componentes fundamentales (ver Fig. 1): el proveedor de contenido adulto, una extensión de navegador responsable de la interacción con el sistema y la generación de la prueba de conocimiento cero, y el propio sistema de verificación de edad y otorgamiento de credenciales. En primer lugar, el proveedor de contenido es responsable de bloquear el acceso al contenido adulto al usuario si no proporciona la prueba criptográfica pertinente, esto se ve ilustrado en los pasos 1 y 2 de la Fig. 1, donde el usuario trata de acceder al contenido y el servidor web realiza una petición para obtener su ZKP. En el paso 3, el usuario inicia el proceso para obtener su credencial y por tanto su prueba criptográfica. La verificación de la edad del usuario es realizada en el paso 4 (en la prueba de concepto desarrollada se ofrece verificación por certificado digital y/o teléfono móvil mediante una consulta al operador).

Habiendo sido exitosa esta verificación se prosigue al paso 5 donde se da la generación de credencial en el entorno de Privado ID, siendo enviada la credencial en el paso 6. La prueba es generada y almacenada por la extensión de navegador.

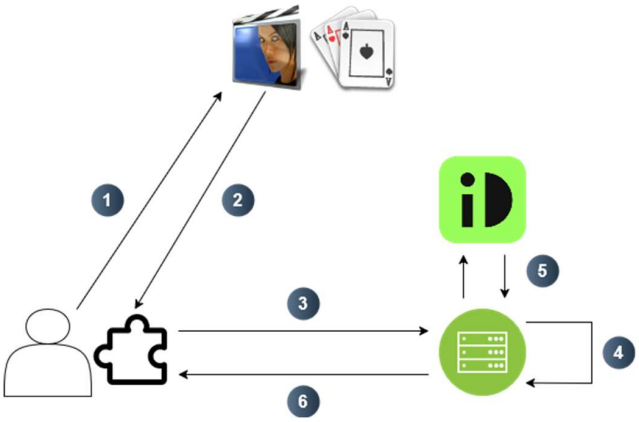

Fig. 1 Explicación a alto nivel del proceso de obtención de credencial

Se ofrece la opción de verificación de teléfono móvil debido a las siguientes razones. En España, algunos operadores como Movistar o Vodafone están empezando a implementar servicios de verificación de edad mediante el número de teléfono para garantizar que solo los usuarios mayores de edad accedan a ciertos contenidos o servicios.

Telefónica, a través de su iniciativa Open Gateway, ofrece la API estandarizada de Verificación de Número (Number Verification) [10].). Además, Telefónica ha colaborado recientemente con TikTok para desarrollar una solución que permite a los usuarios registrarse en la aplicación utilizando su número de teléfono. Esta iniciativa tiene como objetivo verificar la edad de los usuarios de manera eficiente, garantizando que solo aquellos que cumplen con los requisitos de edad puedan acceder a la plataforma.

Vodafone ofrece servicios de verificación de edad a través de su API *Age Verify*, diseñada para simplificar la autenticación de usuarios en productos restringidos por edad, como alcohol o tabaco [11|]. Esta API permite verificar si un cliente de Vodafone cumple con los requisitos de edad utilizando su número de teléfono móvil. El proceso se realiza de manera silenciosa a nivel de red y ofrece una confirmación binaria (Si o No), respetando la privacidad del usuario y ayudando a las empresas a cumplir con las normativas vigentes.

Cuando el usuario trate de volver a acceder al contenido (paso 7) esta vez se encontrará en posesión de una prueba de conocimiento cero, la cuál será enviada a la web adulta previa reclamación (paso 8). La web adulta le enviará esta prueba al entorno de Privado ID [12] (paso 9), en concreto al nodo de verificación o *"verifier node"*, realizándose una verificación de la prueba criptográfica *on-chain* u *off-chain* (este proceso se detalla más adelante). Tras recibir la confirmación de este nodo, la web adulta podrá emplear sus propios mecanismos de acceso (JWT, cookies…) para permitir al usuario acceder al contenido (ilustrado en el paso 10).

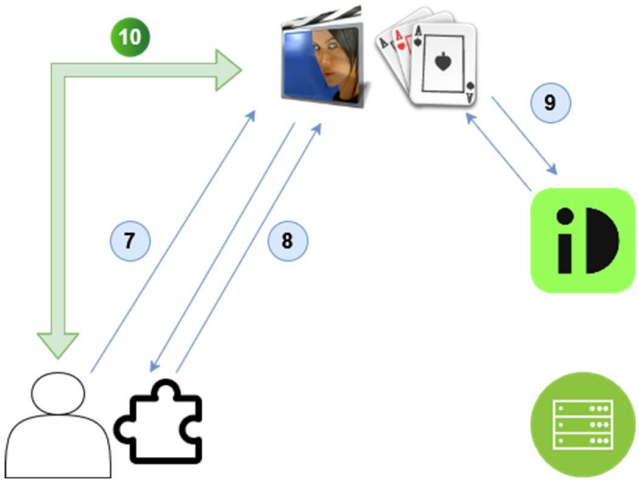

Fig. 2 Explicación a alto nivel del acceso a contenido adulto mediante ZKP

Privado ID es un sistema de identidad descentralizada que permite a los usuarios demostrar ciertos atributos sin revelar información sensible. Utiliza *Zero-Knowledge Proofs* (ZKP) y *blockchain* para garantizar la privacidad. Dentro de este ecosistema, hay dos componentes clave: el *issuer node* y el *verifier node*

El *issuer node* es la entidad encargada de emitir credenciales verificables cuando un usuario necesita demostrar cierta información, generando una credencial firmada digitalmente. El usuario recibe esta credencial y la almacena en su dispositivo. Esto permite que los usuarios tengan control total sobre sus credenciales y decidan cuándo y con quién compartirlas.

Por otro lado, el *verifier node* es el componente que valida las credenciales presentadas por los usuarios sin comprometer su privacidad. Cuando un servicio o aplicación (en este caso el proveedor de contenido adulto) necesita verificar cierta información, solicita una prueba al usuario. En lugar de compartir toda la credencial, el usuario genera una prueba criptográfica con ZKP, que permite al *verifier node* confirmar la autenticidad de la información sin revelar detalles adicionales. Esto garantiza que los servicios puedan verificar atributos específicos (en este caso si alguien es mayor de edad) sin darse a conocer más datos de los necesarios.

La interacción entre el usuario y el sistema se realiza a través de la extensión de navegador, la cual se comunica con el sistema, encargado de verificar la mayoría de edad del usuario. En las pruebas de concepto realizadas, este se ha constituido a partir de API REST *(Application Programming Interface - Representational State Transfer)* construidos en Python, y se han establecido dos posibles mecanismos de identificación, a partir de certificados digitales o mediante el número de teléfono, como ya se ha comentado anteriormente.

Una vez verificada la mayoría de edad por parte del sistema este realizará una serie de peticiones al *issuer node* del entorno de Privado ID. Este genera la credencial que será devuelta al usuario como una URL. La interacción por parte del usuario es necesaria debido a cómo está construido Privado ID (tras hacer *click* en la URL se muestran detalles de la credencial y el usuario debe aceptarla haciendo *click* en un

botón). En futuras versiones se devolverá esta credencial como un código QR, permitiendo al usuario utilizar una cartera móvil.

La extensión descrita anteriormente aparte de la lógica necesaria para la interacción con el resto del sistema presenta una cartera digital capaz de almacenar esta credencial. Esto se hará a partir de un fichero cifrado gestionado y almacenado por la extensión. Tras este proceso de verificación y asignación, en el momento en el que el usuario accede al sitio de contenido adulto, la extensión compartirá la prueba criptográfica al servicio web por medio de una petición que debe ir a través de HTTPS en el cuerpo o cabeceras de esta. El proveedor de contenido adulto contactará entonces al *Verifier node*. La verificación podrá realizarse *off-chain* u *on-chain.*

En el caso de verificación *off-chain* el proceso sería el siguiente. Al acceder al sitio web de contenido adulto, el usuario debe enviar una solicitud a la extensión (en el caso de la verificación web). Ésta envía la ZKPP generada previamente a partir de las credenciales guardadas en la propia cartera del plugin. El usuario entonces envía la ZKPP al *Verifier node* y este la verifica utilizando la API de verificación.

El *verifier node* verifica entonces que el estado del emisor de la credencial (el *issuer node* que otorgó esta credencial) y el estado del usuario sigan siendo válidos y no hayan sido revocados, ambas validaciones se realizan en segundo plano a partir de llamadas a dos contratos alojados en la red (se explica con mayor detalle en el siguiente párrafo). Si la verificación es exitosa, el *verifier node* devuelve un OK al proveedor de contenidos para que este emplee su lógica (cookies, JWT…) para otorgar y mantener por un periodo de tiempo el acceso del usuario al contenido.

Existen dos formas de agregar la lógica de verificación a ZKP a un contrato [13]. Se puede heredar la lógica del contrato *EmbeddedZKPVerifier* ya desplegado o emplear el contrato *UniversalVerifier*. Ambos contratos comparten la misma clase principal e implementan la misma interfaz *IZKPVerifier*, que define métodos para establecer, obtener y enviar respuestas para solicitudes de pruebas.

Mediante *EmbeddedZKPVerifier* se agrega la lógica de verificación al contrato personalizado del cliente, eso significa que todos los resultados de verificación se almacenan en el estado del contrato de este cliente, por tanto, si se quiere usar la verificación *on-chain* para un nuevo contrato, este debe volver a enviarle todas las respuestas a pruebas previamente enviadas.

El proceso para la verificación de una prueba es el siguiente. Previo a este proceso, se debe haber implementado un contrato personalizado de cliente y diseñar una solicitud de prueba con el método de contrato *setRequest*. Cuando un usuario accede al contenido web adulto, este se comunica con la extensión enviando una solicitud de verificación. El plugin de navegador entonces envía la ZKPP generada en la *wallet* al obtenerse la credencial. Esta se envía al proveedor de servicios y este la envía al contrato a través del método *submissionZKPResponse* o *submissionZKPResponseV2*.

El contrato entonces verifica que el estado del emisor de la credencial (el estado del *issuer node*) y el estado del usuario sigan siendo válidos y que no hayan sido revocados. Si la verificación es exitosa, se informa al sitio web para que este aplique su lógica de acceso para el usuario.

Por otro lado, *UniversalVerifier* se implementa como un contrato independiente y actúa como un registro central de verificación. Una vez que se envía una prueba, se puede usar en muchos contratos de cliente diferentes sin necesidad de enviar a estos las pruebas previas.

V. PRUEBAS DE CONOCIMIENTO CERO

Una prueba de conocimiento cero (ZKP) permite a un usuario o parte convencer a un verificador de la veracidad de una declaración sin revelar información adicional. Privado ID utiliza principalmente zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) a través del protocolo Iden3. Las zk-SNARKs generan pruebas de tamaño reducido y permiten una verificación rápida. El protocolo Iden3 implementa un esquema llamado Rapid-PLONK para una generación y verificación eficiente de zk-SNARKs [14]. Circom, un compilador de circuitos, utilizado para definir la lógica de las pruebas de conocimiento cero en Iden3. El protocolo Iden3 es de código abierto y se centra en la identidad auto-soberana, la privacidad y la descentralización. Proporciona un marco para crear y gestionar identidades digitales utilizando blockchain y pruebas de conocimiento cero [15].

Las pruebas de conocimiento cero (ZKPs) son esenciales para la privacidad y minimización de datos en Privado ID, permitiendo a los usuarios demostrar atributos sin revelar los datos subyacentes. Esto minimiza la cantidad de datos personales compartidos. Privado ID también implementa la divulgación selectiva, dando a los usuarios control sobre la información compartida.

VI. PRUEBA DE CONCEPTO

Para demostrar el funcionamiento de esta propuesta, se ha desarrollado una prueba de concepto ofreciendo para el proceso de verificación inicial dos alternativas: mediante el número de teléfono del usuario y consultando al operador, o a través de un certificado digital de la FNMT (Fábrica Nacional de Moneda y Timbre).

En el caso del proceso de verificación de edad basado en el número de teléfono, intervienen varios actores clave: el usuario, el plugin de navegador que gestiona la verificación, el proveedor web que almacena y ofrece el contenido adulto, varios módulos API REST construidos en Python encargados del manejo de solicitudes, el operador móvil encargado de verificar la edad del abonado y el *issuer node* de Privado ID responsable de generar la credencial del usuario.

El proceso (ilustrado en la Fig. 3) comienza cuando el usuario solicita acceso al contenido restringido. En este punto, el servidor web realiza una petición al plugin de navegador requiriendo su ZKP. Como en este caso no se ha realizado el proceso de verificación previamente, la extensión de navegador inicia el proceso de verificación, ofreciendo al

usuario dos opciones, verificar su edad mediante su número de teléfono o utilizando un certificado de la FNMT.

Una vez que el usuario elige la verificación con su número de teléfono y procede a su introducción en el formulario, se envía a la API de Python. Esta genera una contraseña de un solo uso (One Time Password - OTP) realizando una petición HTTPS incluyendo el número de teléfono al servicio *Twilio* [16]. El usuario debe introducir este código en el formulario pertinente para proceder a recibir su credencial.

Tras confirmarse que el OTP enviado por el usuario y el generado por *Twilio* coinciden, se realiza una petición a otra API de Python que simula la interacción con el operador. El operador procede a comprobar si el número de teléfono pertenece a una persona mayor de 18 años, devolviendo una confirmación binaria sin más información. Si el número cumple con este requisito, se genera una petición de credencial que es enviada al nodo emisor.

Finalmente, el nodo emisor responde con una URL de credencial que el usuario puede utilizar para demostrar que ha superado la verificación de edad sin necesidad de revelar más información personal.

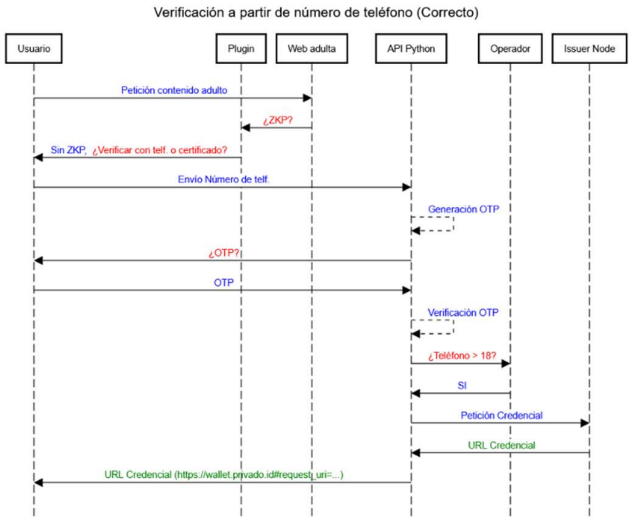

Fig. 3 Verificación a partir de número de teléfono

La Fig. 4 muestra el proceso de verificación de edad basado en un certificado digital, específicamente el certificado FNMT (Fábrica Nacional de Moneda y Timbre), aunque podría utilizarse otro. En este flujo participan varios actores clave: el usuario, el plugin que gestiona la verificación, la web que aloja el contenido para adultos, un servidor Nginx [17] que maneja el tráfico, una API en Python que procesa la verificación y un nodo emisor de credenciales.

El proceso de verificación a partir del certificado de usuario de la FNMT comienza de manera similar. En este caso el usuario elige la opción de certificado FNMT y hace clic en una URL que redirige al usuario hacia un servidor web nginx con el objetivo de enviar su certificado al sistema.

El servidor recibe el certificado del usuario y verifica su firma a partir de certificados raíz de la propia FNMT [18]. En caso de que se valide correctamente esta firma, el servidor envía el certificado a la API de Python, la cual verifica de nuevo la propia firma (evitando posible *bypass* del servidor), el estado del certificado en la CRL (Lista de Revocación de Certificados) y fecha de expiración.

Si el certificado es válido, automáticamente se demuestra que el usuario es mayor de edad, ya que la FNMT solamente otorga certificados de usuario a personas mayores de 18 años. La API entonces envía una petición de credencial al nodo emisor, este genera una URL de credencial que es enviada al usuario.

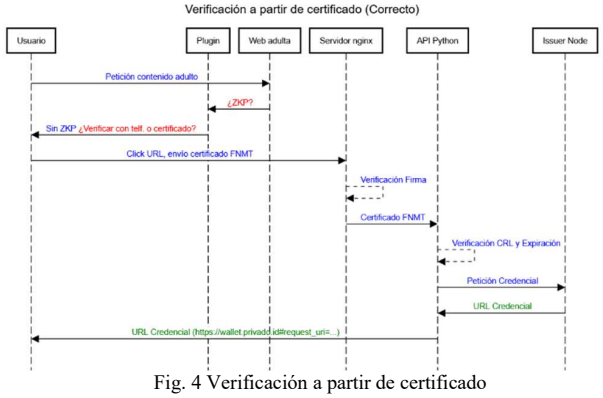

Fig. 4 Verificación a partir de certificado

El proceso de verificación de la edad del usuario finaliza cuando se envía a este la URL de su credencial. Cuando el usuario hace *click* en el *link*, se le redirige al entorno de Privado ID, donde entonces acepta la credencial y se produce la conexión con la cartera de identidad alojada en la extensión de navegador, como se muestra en la Fig. 5. La credencial es entonces almacenada y la cartera genera la ZKPP que será utilizada para la verificación con el proveedor de contenido adulto.

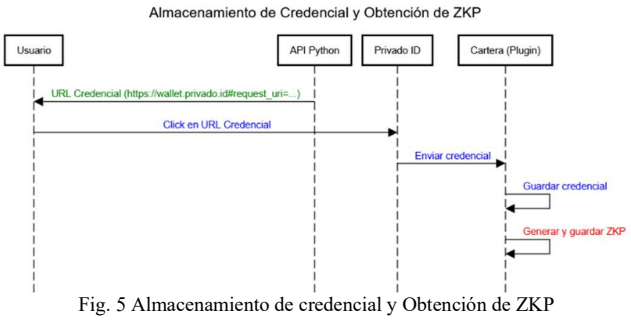

Fig. 5 Almacenamiento de credencial y Obtención de ZKP

Una vez obtenida la ZKP, cuando el usuario visite el sitio de contenido adulto, comienza la fase de verificación de la prueba. El flujo comienza cuando el usuario solicita acceso a dicho contenido. La web adulta, antes de conceder el acceso, envía una petición de verificación al *verifier node* para que este se comunique con la cartera del usuario.

El *verifier node*, al recibir la solicitud, pregunta a la cartera del usuario si dispone de una ZKP válida. En este punto el usuario ya ha realizado el proceso de verificación de edad, por tanto, ya posee dicha prueba, y esta se envía para su verificación. El *verifier node* reenvía la ZKP recibida al contrato de verificación ZKP, que se encarga de validar la prueba de manera descentralizada. Una vez verificada, el contrato responde confirmando que la prueba es correcta.

Después de validar la ZKP, el *verifier node* realiza una consulta adicional al contrato de estado para comprobar si el usuario o el *issuer node* han sido revocados. Si ninguno ha sido revocado, el contrato de estado responde con una confirmación de que todo sigue siendo válido. Con estas verificaciones completadas, el *verifier node* informa a la web adulta que el usuario cumple con los requisitos y que puede acceder al contenido. Finalmente, la web adulta concede el acceso mediante su propio mecanismo de acceso, completando así el proceso de verificación preservando en todo momento la privacidad del usuario.

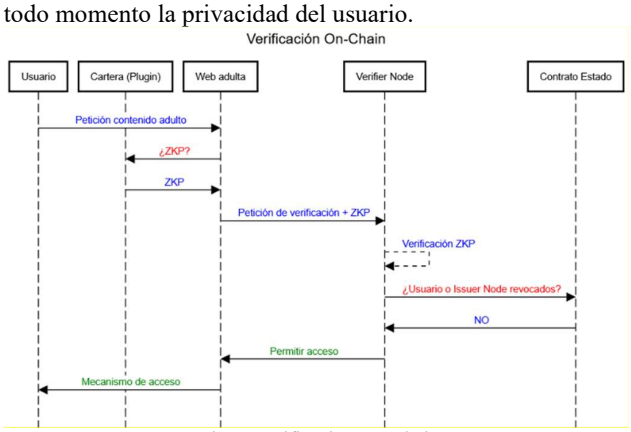

Fig. 6 Verificación On-Chain

Cabe destacar que durante el diseño de este último proceso (Fig. 6), se puso el foco en la facilidad de integración en la infraestructura del proveedor de contenidos adultos de esta solución, siempre considerando la dimensión de la seguridad. Debido a que la ZKP no contiene información alguna sobre la identidad del usuario, es seguro que el proveedor de contenido actúe como "proxy" entre la cartera del usuario y el nodo de verificación, evitando la comunicación directa entre este nodo y los usuarios del servicio, reduciendo la superficie de ataque.

Otra posible opción, de mayor facilidad para el proveedor de contenidos, pero aumentando la exposición a posibles vulnerabilidades es hacer que este redirigiese al usuario al nodo de verificación, realizase la verificación con este y el nodo devolviese al servicio web adulto un simple "apto/no apto". Finalmente se descartó esta opción en favor de la discutida en el párrafo anterior, ya que la complejidad técnica no aumenta en gran medida y se considera que se "compensa" esto con una mayor seguridad.

VII. Comparativa Entre Soluciones

La solución propuesta en este artículo se presenta como una alternativa a la opción propuesta por el Ministerio de Transformación Digital conocida como "Cartera Digital Beta". En este último apartado del documento se ofrece una comparación respecto a la seguridad de cada una. Es preciso destacar que ambas soluciones buscan resolver el mismo problema: permitir la verificación de mayoría de edad sin comprometer la privacidad del usuario.

La información mostrada en este artículo acerca de la solución propuesta por la administración pública ha sido obtenida de los documentos que esta misma ha puesto a disposición del público (véase [19]).

En términos de privacidad, la Cartera Digital Beta incorpora mecanismos de anonimización posteriores a la autenticación, se generan 30 pares de claves (clave pública y privada), junto con los DID respectivos, que le serán facilitados al emisor de las credenciales, de forma que cada credencial de mayoría de edad esté vinculada a una clave pública diferente. Además de la credencial de mayoría de edad, la solución "Cartera Digital Beta" será capaz de solicitar, almacenar y presentar las siguientes credenciales: padrón, ausencia de antecedentes por delitos sexuales, titulaciones universitarias y titulaciones no universitarias. No obstante, se mantiene un vínculo inicial con la identidad del usuario debido al uso de mecanismos como Cl@ve o DNI electrónico. Por el contrario, la solución propuesta refuerza la protección de la información personal mediante la aplicación de pruebas de conocimiento cero, que permiten validar atributos sin exponer los datos subyacentes, lo cual representa una mejora significativa en la preservación de la privacidad.

Respecto a la experiencia de usuario, la Cartera Digital Beta requiere el uso de una aplicación móvil y procesos de autenticación basados en credenciales gubernamentales, incluyendo la interacción mediante escaneo de códigos QR. La solución descentralizada, por su parte, plantea un flujo de uso más simplificado al operar desde una extensión de navegador y aprovechar métodos ya existentes, como los servicios ofrecidos por algunos operadores telefónicos y/o el hecho de que la FNMT emita certificados de usuario exclusivamente a usuarios mayores de edad, simplificando el proceso de verificación y ofreciendo una experiencia más fluida al usuario, lo que podría reducir la fricción tecnológica para el usuario final y el proveedor de contenido adulto.

Desde la perspectiva de seguridad, Cartera Digital Beta se beneficia de métodos consolidados y del respaldo institucional, aunque su centralización representa una vulnerabilidad estructural. En cambio, el enfoque descentralizado de la solución propuesta en este artículo mejora la resiliencia del sistema, disminuye la exposición de datos personales mediante pruebas de conocimiento cero, pero introduce riesgos emergentes vinculados al uso de contratos inteligentes, cuya seguridad depende en gran medida de una implementación rigurosa.

En lo que respecta a la escalabilidad, la propuesta centralizada se ve limitada por la infraestructura gubernamental disponible. La alternativa descentralizada enfrenta desafíos técnicos derivados de la eficiencia computacional de las pruebas criptográficas y de la capacidad operativa de la red, lo que puede afectar su viabilidad a gran escala.

Se destaca que ambas propuestas deben atender al cumplimiento normativo. La Cartera Digital Beta ha sido concebida en alineación con el marco regulador europeo eIDAS 2.0, mientras que la solución alternativa, aunque potencialmente compatible, deberá demostrar su conformidad con dicho reglamento, así como con la normativa de

protección de datos (GDPR), lo cual representa un reto significativo debido a la naturaleza distribuida del sistema.

En cuanto al potencial de integración, la propuesta gubernamental depende de mecanismos de control institucional como listas blancas y su implementación puede estar impulsada por mandatos legales. Por el contrario, la solución descentralizada presenta un modelo de integración más abierto, lo que facilita su adopción por parte de los proveedores de contenido adulto, incluidos proveedores independientes y plataformas emergentes.

Finalmente, los retos de adopción difieren sustancialmente. La Cartera Digital Beta requiere que los usuarios se familiaricen con herramientas gubernamentales y descarguen una aplicación específica, mientras que la alternativa basada en blockchain debe superar barreras de aceptación asociadas al uso generalizado de tecnologías de identidad digital descentralizada, aún incipientes en muchos contextos.

VIII. Conclusiones

Los sistemas de verificación de edad es solo una parte de un sistema de protección más amplio. Es una herramienta, así como la concienciación y formación acerca de los peligros del acceso no supervisado a las redes por parte de menores de edad. Para que esta sea efectiva, debe incluir un mecanismo confiable que no comprometa la privacidad de los usuarios y garantice su anonimato. La responsabilidad de aplicar estas medidas no solamente recae en los padres o tutores, es un deber social del que todos debemos ser conscientes. Se debe involucrar a todos los actores del ecosistema digital, incluyendo proveedores de contenido, motores de búsqueda, redes sociales y otros intermediarios digitales, con el objetivo de proteger a futuras generaciones de contenidos potencialmente dañinos.

Referencias

[1] Bacon, A. (2023). *Children's Safety in the Digital Age: A Look at Identity Verification Legislation in the United States*. American University (Washington, D.C.); Juris Mentem Law Review. https://doi.org/10.57912/23764731.v1.

[2] Stardust, Z., Obeid, A., McKee, A., & Angus, D. (2024). *Mandatory age verification for pornography access: Mandatory age verification for pornography access: Why it can't and won't 'save the children*. Big Data & Society, 11(2). https://doi.org/10.1177/20539517241252129

[3] Lovine, A. (2025, 2nd January). *All the states Pornhub is blocked in as of January 1. Mashable*. https://mashable.com/article/pornhub-shut-off-florida-12-other-states-8764866

[4] Mithani, J. (2025, 7th March). *Can states restrict content in the name of protecting children? The Supreme Court will weigh in*. Tech Policy Press. https://www.techpolicy.press/can-states-restrict--content-in-the-name-of-protecting-children-the-supreme-court-will-weigh-in/

[5] Pastor, J. (2025, 11th March). *Hace unos meses el Gobierno anunció el "pajaporte". Aún no sabemos nada de él pero las plataformas porno españolas sí. Xataca.* https://www.xataka.com/legislacion-y-derechos/gobierno-lleva-meses-retraso-lanzamiento-pajaporte-plataformas-porno-espanolas-estan-notando-su-impacto

[6] Jarvie, C., & Renaud, K.V. (2024). *Age Verification: Government Legislation, Supplier Responsibilization, and Public Perceptions. Children, 11*. https://doi.org/10.3390/children11091068

[7] Comité Europeo de Protección de Datos (2025). *Statement on Age Assurance*. https://www.edpb.europa.eu/system/files/2025-02/edpb_statement_20250211ageassurance_v1-1_en_0.pdf

[8] Agencia Española de Protección de Datos (s.f.). *Decálogo de principios de verificación de edad y protección de menores*. https://www.aepd.es/guias/decalogo-principios-verificacion-edad-proteccion-menores.pdf

[9] Diario Oficial de la Unión Europea (2016). *Reglamento General de Protección de Datos*. https://www.boe.es/doue/2016/119/L00001-00088.pdf

[10] Telefónica Open Gateway (s.f.). *API Number Verification*. https://opengateway.telefonica.com/actualidad/articulo/api-number-verification

[11] Vodafone Developer (s.f.). *Age Verify API Overview*. https://developer.vodafone.com/api-catalogue/age-verify/overview

[12] Privado ID (s.f.). *Privado Identity Verification*. https://www.privado.id/

[13] Privado ID (s.f.). *Verifier Overview*. https://docs.privado.id/docs/verifier/verifier-overview

[14] Protocolo Iden3. https://github.com/iden3

[15] Polygon ID Blog. https://polygon.technology/blog/introducing-polygon-id-zero-knowledge-own-your-identity-for-web3

[16] Twilio (s.f.). *Twilio Official Website*. https://www.twilio.com/en-us

[17] Nginx (s.f.). *Nginx Official Documentation*. https://nginx.org/

[18] Fábrica Nacional de Moneda y Timbre (s.f.). *Certificados raíz de la FNMT*. https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt

[19] Ministerio para la Transformación Digital (s.f.). *Especificaciones técnicas digitales*. https://digital.gob.es/especificaciones_tecnicas.html

.