UAB
Universitat Autònoma de Barcelona

La incidencia de la protección de datos personales en el nuevo modelo europeo de identidad digital

El régimen jurídico de las pruebas de conocimiento cero en la identidad digital europea

RAÜL RAMOS FERNÁNDEZ
Doctorando en Derecho

Índice

1. El estatus de las ZKP en el modelo europeo de identidad digital

Se trata de una técnica criptográfica que permite demostrar la veracidad de una afirmación sin tener que exponer más información personal que la estrictamente necesaria (Goldwasser, Micali y Rackoff,1985). Es siempre relativa desde el punto de vista del solicitante.

Se están llevando a cabo debates sobre las pruebas de conocimiento cero. No se ha seleccionado ninguna ZKP específica para ser compatible con los componentes del ecosistema EUDI Wallet. (Documento ARF)

Considerando 14

Los Estados miembros deben integrar en la cartera europea de identidad digital distintas tecnologías de protección de la privacidad, como la prueba de conocimiento cero. Estos métodos criptográficos ***deben permitir que una parte usuaria valide si una declaración dada basada en los datos de identificación y la declaración de atributos de la persona es verdadera sin revelar ningún dato en que se base dicha declaración, preservando así la privacidad del usuario.***

Considerando 21

Los Estados miembros deben tener la posibilidad de establecer medidas jurídicas y organizativas que mejoren la flexibilidad para los proveedores de carteras europeas de identidad digital y que hagan posibles ***otras funcionalidades de las carteras europeas de identidad digital aparte de las establecidas en el presente Reglamento****.*

Reglamento (UE)2024/1183 de 11 de abril

2. Fricciones del RGPD y el eIDAS 2

1. Enlazabilidad (linkability)	Las declaraciones electrónicas de atributos (DEA) incluyen **información auxiliar** para garantizar su verificabilidad. Esta información auxiliar contiene datos únicos que pueden utilizarse como identificadores personales (Podda et al. 2025).	**Minimización de datos (Art. 5.1.c)**: tratamiento y correlación de más información que la estrictamente necesaria.
2. Evaluación de riesgos	La EUDIW utiliza mecanismos (como los salted hashes) que **no eliminan completamente** la capacidad de rastreo por parte de los proveedores de DEA. La solución técnicamente más avanzada (ZKP) no es obligatoria ni está plenamente implementada. (ARF 2.6.0)	**Privacidad desde el diseño y por defecto (Art. 25)**: a) Las organizaciones deben tener en cuenta los últimos avances tecnológicos y evaluar los costes y beneficios de la implementación de estas tecnologías. b) Se deben evaluar la naturaleza, el alcance, el contexto y los fines de las actividades de tratamiento de datos. c) Se debe llevar a cabo una evaluación exhaustiva de los riesgos y gravedad para determinar el impacto potencial sobre los derechos y libertades de las personas.
3. Estado de la técnica	ZKP como **índice de referencia** (benchmark) para demostrar el cumplimiento del artículo 25 RGPD. Valoración de otras técnicas contra ZKP (Ramos Fernández 2024)	

3. Propiedades de las pruebas de conocimiento cero

Minimización de datos	Minimización de la divulgación	El usuario puede probar la posesión de un dato sin revelar el dato subyacente. El verificador solo aprende la validez de la afirmación.
	Prevención de rastreo (unlinkability)	Se evita la divulgación de **datos auxiliares criptográficos enlazables** (firmas, claves públicas, etc.) que permiten el seguimiento y perfilado en sistemas convencionales.
	Acreditar existencia de datos (predicados)	Permiten presentar **afirmaciones derivadas de atributos** (ej., "es mayor de 18") en lugar del dato crudo, liberando solo la información estrictamente necesaria.
Verificabilidad de la identidad	Alto grado de garantía (completitud y solidez)	El protocolo satisface propiedades criptográficas clave (completitud y solidez), asegurando un nivel de seguridad y confianza equivalente al de los métodos de presentación no-ZKP.
	Delegación de la verificación y **prueba de ejecución**	Los chequeos complejos (verificar firma, validez, etc.) se realizan **localmente en el dispositivo** del usuario. La wallet (en sistemas así diseñados) genera un **certificado de ejecución correcta (la ZKP)**, que convence al receptor de que los pasos de verificación locales cumplieron los estándares.
	Autenticación del titular (holder binding)	La wallet (en sistemas así diseñados) demuestra que conoce la clave secreta asociada al documento para confirmar la posesión, **sin revelar la clave pública** (que es un identificador enlazable).

4. Consecuencias del vacío legal

Ausencia de seguridad jurídica	El receptor de la prueba (Relying Party) asume un **riesgo legal significativo** al aceptar una ZKP. No hay un marco legal que garantice su validez ante autoridades supervisoras (ej., reguladores AML/KYC), lo que desincentiva su adopción.
Fragmentación del mercado único	La implementación de ZKP queda a la **discreción de cada Estado Miembro.** Esto conduce a la existencia de múltiples regímenes regulatorios incompatibles, socavando el objetivo de la **interoperabilidad transfronteriza.**
Freno a la innovación	La ausencia de un régimen legal claro y armonizado desincentiva al sector privado a invertir en soluciones ZKP.

5. Propuestas

Regla de equivalencia sustantiva	Modificar eIDAS 2.0 para estipular que una presentación basada en ZKP tiene el **mismo efecto jurídico** que la presentación directa de los datos de la EUDI wallet o la (Q)EAA original.
Regulación de producto (SaaP) y certificación previa (**modelo híbrido sector público/privado**)	Tratar las ZKP como un producto de software generado localmente y crear un sistema de **certificación ex-ante del software ZKP que se quiera enlazar con la EUDI wallet**, alineado con organismos como ENISA y los esquemas EUCC.
Aceptación obligatoria	Permitir la **vinculación** de software ZKP certificado de terceros **a la EUDI wallet**. Extender la obligación de aceptar la EUDI wallet a la aceptación obligatoria de presentaciones ZKP generadas por software certificado. (**Seguridad jurídica usuarios/terceros**).
Clarificación del régimen de responsabilidad	Modificar el Artículo 11 de eIDAS 2.0 para **excluir la responsabilidad de los Estados Miembros** por daños causados por componentes de software de terceros certificados; la responsabilidad recaería en los desarrolladores del software.

6. Perspectivas de futuro

Revisión del Reglamento eIDAS 2 (2026)	El Reglamento eIDAS 2 prevé en su Art. 49 una **revisión de su aplicación a más tardar el 21 de mayo de 2026.** Se presenta como una oportunidad para abordar el estado de la técnica sobre las ZKP.
Evolución Técnica del ARF	El Marco de Arquitectura y Referencia (EUDI wallet ARF) es un documento evolutivo, en el que se pueden seguir discusiones públicas del uso de ZKP. No tiene valor legal, sin perjuicio de los actos de ejecución que lo adopten.
Desarrollo del ecosistema	A modo de ejemplo: ETSI TR 119 476 Electronic Signatures and Trust Infrastructures (ESI); Analysis of selective disclosure and zero-knowledge proofs applied to Electronic Attestation of Attributes. ISO/IEC DIS 27565 Information security, cybersecurity and privacy protection - Guidelines on privacy preservation based on zero-knowledge proofs (en desarrollo a fecha 01/11/2025).

7. Conclusiones

El Reglamento eIDAS 2 permite el desarrollo de un régimen flexible para modular privacidad, seguridad pública y cohesión el mercado.

La dificultad en la implementación de las pruebas de conocimiento cero se debe a la ausencia de seguridad jurídica, no a la inmadurez técnica.

Mientras que las pruebas de conocimiento cero se tratan de un concepto técnico, es necesario recepcionarlas jurídicamente para otorgarle efectos claros y seguridad jurídica.

8. Bibliografia

European Digital Identity Wallet -Architecture and Reference Framework. Accessed November 1, 2025. https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/2.6.0/architecture-and-reference-framework-main/.

Goldwasser, Shafi, Silvio Micali, and Charles Rackoff. 1985. “Knowledge Complexity of Interactive Proof-Systems.” *Conference Proceedings of the Annual ACM Symposium on Theory of Computing*, 291–304. https://doi.org/10.1145/22145.22178.

Podda, Emanuela, Pol Hölzmer, Alexandre Amard, Johannes Sedlmeir, and Gilbert Fridgen. 2025. “The Impact of Zero-Knowledge Proofs on Data Minimisation Compliance of Digital Identity Wallets.” *Internet Policy Review* 14 (3). https://doi.org/10.14763/2025.3.2019.

Ramos Fernández, Raül. 2024. “Regulatory Options for Integrating Zero-Knowledge Proofs into the European Digital Identity Wallet.” *International Review of Law, Computers and Technology*, September. https://doi.org/10.1080/13600869.2024.2398915.

¡GRACIAS!

Más información: raulramos@icasbd.org

UAB
Universitat Autònoma
de Barcelona