en Construcción

>> Jorge Dávila

# La Identidad Prometida

**Hace tiempo que la identidad se ha puesto de moda y desata más interés social del que uno debería esperar dada su limitada utilidad real en la sociedad que nos cobija. Identidades de género aparte, la identidad digital es una asignatura pendiente desde hace 34 años y es todavía hoy un foco caliente en el que afloran iniciativas muy publicitadas como lo es la Identidad Auto-Soberana. Está por ver en qué va a quedar esto a la luz de lo que han dejado iniciativas anteriores, pero siempre es bueno prestar atención a las novedades, no vaya a ser que esta vez sí, por fin, lleguemos a la tierra prometida.**

## Érase que se era

Lo que desde hace tiempo se dio en llamar Infraestructuras de Clave Pública, o simplemente PKIs, aparecieron el 3 de julio de 1988 cuando se concibió el estándar X.509 que, inicialmente, formaba parte del estándar X.500, que debería haber sido una especie de Directorio donde buscar a los usuarios del vetusto estándar X.400 de correo electrónico. Ese estándar anfitrión, el X.500, fue iniciado por la International Telecommunications Union (ITU) actuando como asesora de la agencia International Telephony and Telegraphy (CCITT) que, como su nombre indica, se ocupaba de estandarizar teléfonos y telégrafos. Hablamos de una época en la que lo digital era algo realmente incipiente y lo analógico lo ocupaba todo.

Una PKI establece los roles, las políticas, el hardware y el software, así como los procedimientos a seguir para crear, gestionar, distribuir, usar, almacenar y revocar certificados digitales como parte de los sistemas de cifrado asimétrico de clave pública. El formato de esos certificados digitales, alrededor de los cuales todo fue creado, encontramos el famoso estándar X.509. En concreto, el documento RFC 5280[1] establece cómo son los **certificados X.509 v3**, las **Listas de Revocación de Certificados** (CRL) X.509 v2, y establece el procedimiento a seguir en la **validación de los Certificados digitales X.509**, siendo todo ello esencia misma de lo que son las PKIs actuales.

El desarrollo de las PKI es consecuencia directa del descubrimiento previo de la **Criptografía Asimétrica**. Este paradigma se imagina por primera vez a principios de la década de 1970 en la Agencia de Inteligencia británica (GCHQ) donde, principalmente, James Ellis, y Clifford Cocks hicieron importantes descubrimientos[2] sobre estos nuevos algoritmos asimétricos y su potencial y utilidad en **el problema de la distribución de claves**. Como todo lo sustancial que hace la agencia GCHQ está clasificado, estos resultados se mantuvieron en secreto hasta 1997.

Mientras tanto, en abril de 1977, **Ron Rivest**, **Adi Shamir** y **Leonard Adleman** propusieron utilizar la exponenciación modular como función que satisfacía las características de lo que, un año antes, en mayo de 1976, **Whitfield Diffie** y **Martin Hellman** habían ideado[3] y habían dado en llamar Criptografía de Clave Pública cuando realmente eran "*funciones hash con trampa*"[4]. El 20 de septiembre de 1983 el MIT consigue patentar[5] el nuevo algoritmo ya por entonces conocido como **RSA**.

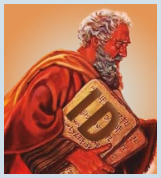
Lo realmente importante del RSA para la sociedad civil resultó ser, no tanto la posibilidad de cifrar o descifrar, sino la de disponer de una **Firma Digital** genuina. La posibilidad de cifrado con RSA, evolucionó de forma independiente y se limitó al cifrado de claves simétricas para la distribución de las mismas dentro del envío de **correos electrónicos confidenciales/secretos**.

Con el nacimiento de Internet y su efervescencia dentro de la sociedad civil, algunas compañías y emprendedores individuales vieron la posibilidad de montar un gran mercado planetario (eCommerce)[6], basado en la posibilidad digital de firmar documentos, contratos, transacciones, etc., y por ello, desde el principio trabajaron para conseguir el reconocimiento legal de esa posibilidad.

## Las PKIs pierden el tren

En 1996, la **American Bar Association** publicó un extenso análisis de algunos aspectos legales que las PKIs podían plantear[7] y poco después algunos estados norteamericanos como el de Utah, que fue el primero en 1995, empezaron a aprobar leyes y regulaciones de Firma Digital. En el resto del mundo se ha producido el mismo fenómeno y ahora existen Leyes de Firma Electrónica o Digital[8] por doquier.

Después de aquellas ensoñaciones iniciales, los vendedores de PKIs realmente encontraron un mercado para sus poco maduros desarrollos (IAM)[9], pero ese resultado no fue el que ellos esperaban a mediados de la década de 1990. Por si fuera poco errar en el tiro, esa evolución ha



***El lastre principal de las PKIs es que no han resuelto muchos problemas que se esperaba resolviesen y el tren del comercio electrónico hace tiempo que lo perdieron, y sólo les queda medrar a la sombra de los estados soberanos que son los que controlan "la identidad", con mayúsculas, que es la única que importa en este escenario.***

[1] Network Working Group. RFC 5280 Mayo 2008 (reemplaza 3280, 4325, 4630). Autores: D. Cooper (NIST), S. Santesson (Microsoft) , S. Farrell (Trinity College Dublin), S. Boeyen (Entrust), R. Housley (Vigil Security), W. Polk (NIST)

[2] https://web.archive.org/web/20141030210530/https://cryptocellar.web.cern.ch/cryptocellar/cesg/possnse.pdf

[3] "We stand today on the brink of a revolution in cryptography..." in W. Diffie; M. Hellman (1976): "New directions in cryptography". IEEE Transactions on Information Theory. 22 (6): pag 644. Ver https://www.cs.jhu.edu/~rubin/courses/sp03/papers/diffie.hellman.pdf

[4] Una función hash con trampa es una función de sentido único para todos menos para el que la fabrica, que si puede calcularla en sentido contrario:"A trap-door cryptosystem can be used to produce a public key distribution system"

[5] US Patent 4,405,829 "Cryptographic communications system and method" Ver https://patents.google.com/patent/US4405829A/en

[6] https://en.wikipedia.org/wiki/E-commerce

[7] https://web.archive.org/web/20170411143006/http://apps.americanbar.org/dch/thedl.cfm?filename=/FST230002/Fotherlinks_files/Fdsg.pdf

[8] https://en.wikipedia.org/wiki/Electronic_signatures_and_law

[9] IAM = Identity and Access Management. https://en.wikipedia.org/wiki/Identity-management_system

sido mucho más lenta de lo que pensaban y ha ido por derroteros que, por aquel entonces, no fueron previstos.

El lastre principal de las PKIs es que no han resuelto muchos problemas que se esperaba resolviesen (jerarquización de su estructura, gestión de los riesgos, aceptación del usuario, usabilidad, comprensión general de su esencia, etc.) por lo que, en realidad, no se han convertido en una realidad planetaria. Al final de cuentas, las PKIs han tenido su único gran éxito en sistemas gubernamentales de identificación y/o autenticación (e-DNIs)[10], y ningún éxito en entornos privados como los del ya muy consolidado "**Comercio Electrónico**" (Amazon, AliExpress, eBay, Apps Bancarias, etc.) que se limitan a utilizar pares Usuario-Contraseña, un ejemplo de "Isolated User Identity Model (SILO)", para la **autenticación/identificación** de sus clientes a través de canales TLS.

Los Certificados Digitales X.509 enlazan una identidad prexistente y esencialmente no digital con una clave pública para ser utilizada dentro de un esquema de firma digital legalmente reconocida. Para ello el sistema X.509 desarrolla dos tipos de certificados, el de las **Autoridades de Certificación** (CA), y los de **Entidad Final**. En la cúspide de una necesaria jerarquía única y planetaria habitaría un certificado auto-firmado denominado certificado de la "Root CA". Debajo de ella están los certificados de las Autoridades de Certificación Intermedias o Subordinadas que, al final, algunas terminan emitiendo los certificados de los usuarios finales que son personas físicas, jurídicas y otros tipos de organizaciones o dispositivos (IoT).

Está por tanto claro que lo importante en este escenario es la **firma digital** y que ésta es útil porque se relaciona legalmente lo que funciona en las redes (**Identidad Digital**)[11] con una **identidad legal** siempre externa (DNI)[12]. Una vez establecido ese vínculo, las PKIs se unen a otros constructos tecnológicos a los que desde hace años quieren acostumbrarnos (PKI[13], FedID[14], SSO[15], OAuth[16], OpenID[17], etc.) para resolver el problema de la autenticación/identificación en sistemas digitales.

El tren del comercio electrónico hace tiempo que lo han perdido las PKIs, y sólo les queda medrar a la sombra de los estados soberanos que son los que controlan "la identidad", con mayúsculas, que es la única identidad que importa en este escenario. En otras palabras, es la **Identidad Legal** que es de la que entienden los Jueces y la que gestionan las Policías.

### La aproximación de las Identidades Auto-Soberanas

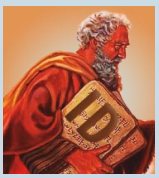
Dentro de las Identidades Digitales, últimamente está muy de moda las denominadas Identidades Auto-Soberanas (*Self-Sovereign Identity*). Estos nuevos planteamientos son una aproximación distinta al problema de la identidad digital y promete utopías como la de otorgar al titular el control total de su identidad[18].

***Dentro de las Identidades Digitales, últimamente está muy de moda las denominadas Identidades Auto-Soberanas, cuyos nuevos planteamientos son una aproximación distinta al problema de la identidad digital y promete utopías como la de otorgar al titular el control total de su identidad.***

En la sociedad, la identidad es algo que intenta establecer y servir de base para construir **la confianza necesaria** para iniciar y mantener una relación social. En aras a que confíen en uno, este uno se presenta a los demás enseñando y entregando **credenciales**, siempre de origen exógeno, que lo colocan, lo ubican dentro de la realidad social conocida por todos, o casi todos. Los demás sólo tiene que validar esas credenciales, determinar si son auténticas y si corresponden realmente al individuo que las presenta para poder empezar a confiar en lo que él/ella afirma ser, tener o poder hacer. En los procesos de autenticación la confianza pasa de las credenciales al presentador de las mismas.

Si se quiere hablar de auto-soberanía, o de soberanía a secas, los usuarios del sistema de identificación deberían poder **controlar en exclusiva** y **durante todo el tiempo** esas credenciales digitales, por lo que deberían contar con su consentimiento para ser verificadas o validadas. La justificación dada para querer algo tan abstracto e ideal siempre es la de combatir la libre (e ilegal) disposición para funciones distintas a las autorizadas de datos personales que en su momento conoció y validó el verificador.

Para ello, los titulares deberían **ser los únicos capaces de generar y controlar** identificadores digitales únicos (*Decentralized Identifiers*) conteniendo cualquier tipo de información referente a ellos mismos. Sin embargo hay que destacar que en los muchísimos artículos y propuestas que se han hecho y hacen de identidades auto-soberanas, nadie dice cómo realmente se puede conseguir tal sueño, tal utopía. La mayoría de las propuestas **1)** son descentralizadas, **2)** utilizan monederos electrónicos para guardar y operar con las credenciales, **3)** se basan en la criptografía asimétrica como concepto y en **4)** en el uso de documentos públicos anclados en registros públicos distribuidos llamados **Cadenas de Bloques** (***Blockchain***).



***¿Qué beneficios reales y qué hay detrás de las iniciativas de Identidades Auto-Soberanas? Pueden verse como experimentos académicos y digitales en el ámbito de la autenticación, o como ataques indirectos a los sistemas centralizados de otorgamiento de identidades por parte de los estados soberanos.***

Sin embargo, en general, en el escenario propio de cualquier identificación/autenticación, la confianza nacería de la verificación de esas credenciales por otros y esa validación, en principio, podría ser pública o privada. Si es privada, el validador contaría con el titular para la verificación de la misma dentro de una transacción que sólo los intervinientes podrían conocer, tanto en el presente como en el futuro. En el caso de que fuese pública, esa verificación podría no necesitar la participación del titular y ser algo que el verificador podría hacer varias veces y podría enseñar a otros. Un control efectivo de la identidad anunciado por las iniciativas auto-soberanas exigiría que todas las validaciones de credenciales fuesen privadas.

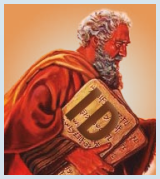
### Las validaciones privadas de credenciales, un sin sentido

El problema de la **identidad digital** es que está unida a la **firma digital** y ésta a la resolución de conflictos ante los tribunales de justicia, por lo que no tiene sentido pensar en validaciones privadas de credenciales; hacerlo sería como esperar la colaboración del denunciado para ser

[10] https://es.wikipedia.org/wiki/DNI_(España), https://en.wikipedia.org/wiki/Electronic_identification
[11] https://en.wikipedia.org/wiki/Digital_identity
[12] https://en.wikipedia.org/wiki/Identity_document
[13] https://en.wikipedia.org/wiki/Public_key_infrastructure
[14] https://en.wikipedia.org/wiki/Federated_identity
[15] https://en.wikipedia.org/wiki/Single_sign-on
[16] https://en.wikipedia.org/wiki/OAuth
[17] https://en.wikipedia.org/wiki/OpenID
[18] https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8776589

condenado. En cualquier sistema que permita dirimir diferencias, en cualquier sistema de justicia, es necesario que las validaciones de credenciales sean públicas y queden en manos exclusivas del verificador para que éste pueda enseñarlas y adjuntarlas a cualquier reclamación posterior. Esto se llama "**no-repudio**" y es una característica esencial e imprescindible de cualquier sistema de firma digital.

Otro aspecto a considerar es la argumentación original de estas iniciativas como mecanismo de protección frente al uso de datos personales sin autorización del titular. El mismo proceso de verificación aporta información sobre el titular al verificador. Si entendemos información como aquello que nos hace saber algo que no sabíamos antes, la verificación de credenciales, como la adquisición de cualquier otra información, equivale a la pérdida efectiva de control de la misma. Cuando alguien cuenta un secreto a alguien, la única manera de revertir el proceso es matar al que lo ha aprendido, y hacerlo suficientemente deprisa ya que éste puede filtrarlo a terceros antes de su "cancelación" física y definitiva.



***La identidad sigue siendo una promesa pendiente del mundo digital y las iniciativas auto-soberanas, un escenario hueco y sin futuro, en el que se está enterrando la necesaria defensa del individuo frente al Matrix digital, y quizás se estén desarrollando escaramuzas de baja intensidad en conflictos entre soberanías competidoras entre sí.***

### El identificador único y el control

El control de nuestros datos se pierde en el mismo momento que los utilizamos. Los que han conocido una información, pueden reunirse y cooperar para ponerla en común y generar bases de datos y de conocimiento para lo que no están autorizados. Es cierto que en los escenarios actuales, esta operación de puesta en común o "cruzado" de bases de datos es mucho más fácil porque en todas ellas aparece un **identificador único** que, en nuestro caso, es el número del DNI.

¿Cuál es la razón por la que siempre nos piden el DNI? Una posible puede ser la costumbre, pero también que ese número sea el identificador que le permite al que nos lo pide, encontrarnos y mentarnos en el sistema bancario y financiero, o referirse a nosotros en el caso de que quieran llevarnos a los tribunales. Una identificación con pseudónimos de origen y uso local tiene una utilidad muy limitada en sistemas sociales algo más complejos que los de un pueblo o aldea con menos de veinte mil habitantes.

### ¿Qué hay detrás?

Otra forma de ver en el escenario actual estas iniciativas de descentralización es imaginar qué puede haber detrás de ellas. Preguntando qué beneficios reales ya están produciendo, quizás podamos encontrar cuáles son sus verdaderas intenciones. Las iniciativas de Identidades Auto-Soberanas pueden verse 1) como **experimentos académicos** y digitales en el ámbito de la autenticación, o 2) como **ataques indirectos a los sistemas centralizados de otorgamiento de identidades** por parte de los estados soberanos.

Si es un experimento académico, habría que presentarlo como tal y ponerlo al mismo nivel que muchos otros experimentos dirigidos a aumentar el conocimiento de la Humanidad, y ver si éstos merecen más o menos financiación que otros. Sin embargo, si se trata de una campaña de ataque a los sistemas centralizados de identidad legal, cualquier ataque debe previamente evaluar sus posibilidades de éxito. En este caso, habría que preguntarse cuáles son las posibilidades reales de que un sistema de identidad descentralizado tenga éxito en el comercio electrónico en general o en las relaciones interpersonales de los ciudadanos del planeta.

El comercio electrónico o digital comparte con el comercio en general las mismas bases económicas y jurídicas. Lo que importa es la firma de contratos que, delante de un juez o autoridad, hagan al comerciante esperar a ser pagado y al cliente a ser servido según un acuerdo previo conocido y/o establecido por ambos. Por tanto, la única identidad que tiene futuro planetario es aquella que reconozcan o utilicen los sistemas legales, y estos siempre acudirán a un sistema único que garantice, al menos en parte, una igualdad operativa para todos los identificados. La componente económica está subordinada a la "seguridad jurídica", por lo que ella no jugará ningún papel en lo que a la identidad de sus agentes se refiere.

Por el contrario, si lo que estamos tratando es la forma de reconocer las empresas a sus clientes y/o trabajadores, el sistema que triunfa desde siempre es el centralizado, en el cual el proveedor y validador de identidad son la misma empresa. Ahí están los pases y tarjetas de identificación de los trabajadores y los programas de fidelización para los clientes.

### Titulares de identidad, control de ésta y cuentos de hadas

En este panorama, la creencia tan cacareada de que se puede entregar a los titulares de la identidad el control de ésta, es simplemente un cuento de hadas que, o bien 1) se está utilizando para dar la sensación de que se hace algo contra la profunda pérdida de intimidad que supone el mundo digital globalizado, o bien 2) se está utilizando como propaganda ofensiva en otras guerras contra el papel preponderante de algún estado o compañía sobre sus ciudadanos o trabajadores. En ambos casos se estaría engañando al público y a todos aquellos que inviertan en esa quimera.

Por si fuera poco, **no está claro** que detrás de esos supuestos sistemas de auto-soberanos haya realmente una tecnología segura que los avale. La **identidad legal** y **la identidad social** son cosas que otros reconocen y otorgan al titular de la misma. El nombre te lo ponen tus padres, te lo reconoce el Registro Civil, y el apodo te lo ponen los del pueblo que vio desarrollar tu infancia o la de tus ancestros.

En el mundo económico, la identidad que importa es tu perfil de gastos y tus capacidades monetarias y financieras, y esas solo se construyen con hechos, con gastos, con inversiones. Para generar cualquier perfil crediticio es necesario disponer de un identificador único que vincule todos los gastos y préstamos relacionados con una misma persona (física/jurídica). Si se hace desaparecer esos identificadores únicos universales, no podrían confeccionarse esos perfiles y el sistema económico que disfrutamos/sufrimos amablemente nos excluiría de él. Nunca la identidad operativa ha sido auto-asignada.

Quede claro que queda fuera de esta discusión la **identidad de género**, la **identidad biológica**, y el **ego**, entre otras, ya que son propiedades que empiezan y terminan en el propio individuo y que, en general, son esencialmente irrelevantes para el funcionamiento de la sociedad. Otra cosa es que las gentes del Big Data estén también muy interesadas en ellas, en conocerlas con detalle, en bucear en sus posibles relaciones causales para luego poder montar sus campañas de márquetin dirigido, de reclutamiento ineludible o de adoctrinamiento operante. Es cierto que por todo ello esas identidades **deben ser protegidas** dentro del gran paraguas que es nuestra **Intimidad** (A.K.A **Privacidad**) que es una parte importante de los Derechos Humanos individuales.

Después de darle muchas vueltas al tema de la identidad y a las iniciativas auto-soberanas veo que la primera sigue siendo una promesa pendiente del mundo digital, y las segundas un escenario hueco y sin futuro, en el que se están enterrando la necesaria defensa del individuo frente al Matrix digital, y quizás se estén desarrollando escaramuzas de baja intensidad en conflictos entre soberanías competidoras entre sí. Además, como las SSIs están de moda, consiguen financiaciones de los que casi nunca saben qué financian realmente (Uniones Europeas, Ministerios, Comunidades Autónomas, Ayuntamientos, Peanías y Empresas e Inversores en general). Además, estos agentes financiadores nunca llegan a pedir cuentas o hacer balances reales de si realmente ha merecido la pena lo financiado para el interés general. ■