

Actualidad y futuro de la Identidad Digital

Author : a.h.

Categories : [Auditoría, Certificación y Calidad de Sistemas Informáticos](#)

Date : 27 noviembre, 2018



Tras semanas escribiendo en este blog sobre la identidad digital, sus riesgos, los controles que implantar y hasta noticias de actualidad, ha llegado el día en el que escribo este, mi último post. Para la ocasión he elegido varios temas con los que me gustaría terminar que iré desglosando poco a poco.

En el mundo físico cuando nos comunicamos con un interlocutor tenemos evidencias de quién es la persona como puede ser la voz o el aspecto físico del individuo. Cuando la comunicación es escrita se usa el concepto de “firma” para reconocer al emisor del mensaje. ¿Pero qué pasa cuando el medio es el más abierto y menos confiado del Mundo? Sí, estoy hablando de Internet. Sorprendentemente la solución es usar el concepto que acabo de mencionar pero en la era digital, es decir, “firma digital”. Esta tecnología se lleva usando décadas con la finalidad de proteger mensajes de carácter sensible como en la Guerra Fría. Pero la noción de la tecnología de clave pública permite una identificación y autenticación económica de mensajes y personas en la red. Las firmas digitales usan una infraestructura de clave pública (PKI) en la que las autoridades de certificación actúan como terceros de confianza para tanto identificarte como autenticarte [1].

Puede que gracias a la tecnología de “firma digital” podamos verificar quién es el emisor de un mensaje, ¿pero y si lo que queremos es demostrar nuestra identidad a las administraciones

públicas o a otras personas en general en Internet? Para dar respuesta a este reto nace el concepto de “identidad universal digital” también conocido como “identidad nacional”. Las mayores barreras para este desafío son la tecnología y la política en sí mismas ya que son pocos los países que han conseguido llevar a cabo de manera eficaz la identidad nacional [2]. Veamos los casos más significativos de países que han logrado un sistema eficaz de identificación.

- El primer caso es el de Estonia, cuyo sistema está siendo usado por el 98% de la población del país y donde el 88% usa el sistema en Internet de forma regular. En este país cada ciudadano cuenta con una ID card (nuestro DNI) que les permite identificarse en toda Europa, acceder al sistema público de salud, identificarse en sus bancos, televoto, firma digital, ver las prescripciones médicas,... Pero además, este producto físico puede usarse de forma digital con la Smart-ID o Mobile-ID, que son dos formas diferentes de autenticarse online usando nuestro dispositivo móvil [3].

- El segundo caso que me gustaría analizar es el de India. En este estado tienen implantado un sistema llamado Asdhaar. Este no es más que un número de 12 dígitos únicos que identifica a cada ciudadano (de la misma forma que nuestro número de DNI) pero que usa técnicas biométricas (huella dactilar y el iris) y demográficas. Este sistema está denominado como “el sistema más sofisticado de identificación del Mundo”. Como en el caso de Estonia, el método permite tener asignados datos personales como número de teléfono o domicilio pero también incluye los servicios públicos o cuentas bancarias. Cabe destacar que numerosos grupos de activistas se oponen a este sistema por considerar que perjudica a la privacidad de las personas [4].

La última tecnología de que quería hablar es la poco conocida ViDChain, basada como su propio nombre indica en Blockchain. Esta propuesta permite agregar diferentes fuentes de identidad en una cartera de atributos de identidad. Las fuentes de identidad pueden ir desde RRSS a sistemas biométricos u oficiales como el DNle [5]. A pesar de lo prometedor que parecía esta propuesta por unificar todos nuestros perfiles, parece que no se ha terminado de hacer una realidad. Posiblemente debido a los riesgos que conlleva dicho sistema y el estado actual de la tecnología.

Para terminar me gustaría dar mi opinión personal al respecto de este tema y decir que me ha resultado muy interesante la investigación previa a la realización de esta serie de 5 posts. Considero un avance necesario e importante el uso de la biometría como forma de identificación pero creo que debe estar ligada a otros métodos. Lo que quiero decir es que la forma que veo más idónea para la identificación en Internet es la utilización de más de un sistema, combinando factores físicos (por ejemplo aceptar usando el móvil que eres tú), demográficos (parametrizar lugar de residencia y zonas habituales de acceso), contraseñas y variables biométricas. Estos sistemas se podrían usar de forma combinada para garantizar la identidad de la persona. Además, en cuanto a la identidad digital personal me gustaría recalcar que hoy en día el “yo” físico y el digital están cada vez más conectados y que debemos comprender cómo funcionan para gestionarlos correctamente.

[1] “Digital signatures - Security & Controls”, acceso el 27 de noviembre de 2018. <https://www.isaca.org/bookstore/extras/Pages/Digital-Signatures-Security-andamp-Controls-Executive-Summary.aspx>

[2] “In search of a national identity”, acceso el 27 de noviembre de 2018. <https://www2.deloitte.com/uk/en/pages/financial-services/articles/in-search-of-a-national-identity.html#>

[3] “e-identity”, acceso el 27 de noviembre de 2018. <https://e-estonia.com/solutions/e-identity/id-card/>

[4] “Aadhaar”, acceso el 27 de noviembre de 2018. <https://en.wikipedia.org/wiki/Aadhaar>

[5] “ViDChain, el futuro de la identidad digital”, acceso el 27 de noviembre de 2018. <https://www.validatedid.com/es/vidchain-el-futuro-de-la-identidad-digital/>