Sistema Seguro de Identificación y Autenticación Digital

Andrés Alvear, Adrián Gómez, Edgar Beltrán, Sebastián Naranjo
Estudiantes Maestría en Seguridad de la Información
Departamento de Ingeniería de Sistemas y Computación
Universidad de Los Andes. Bogotá, Colombia
Junio 2019

1. Introducción

En Colombia, los ciudadanos adelantan múltiples procesos con el gobierno, entidades financieras y comerciales para obtener servicios de acuerdo con sus necesidades. Las entidades, tanto públicas como privadas, que ofrecen los servicios generalmente usan la cédula y la huella dactilar para identificar y autenticar a quien pide un servicio. La huella dactilar es el factor biométrico mas común en diferentes entornos y el mas reconocido por diferentes tecnologías.

Sin embargo, los procedimientos actuales de validación de la identidad de un ciudadano presentan vulnerabilidades. Es posible encontrar diferentes casos reportados de suplantación de identidad gracias al uso indebido de los datos personales que se encuentran visibles en la cédula de ciudadanía, casos facilitados por la ausencia de trazabilidad y mecanismos de autorización de uso en tiempo real. Entre los casos reportados encontramos: Jefe de frente urbano del Eln le robó identidad a pensionado[1], Con fotocopia de la cédula les basta a los falsificadores[2], Suplantan a un patrullero de la Policía en Barranquilla[3].

Teniendo en cuenta el número de transacciones y servicios que en Colombia requieren usar un mecanismo de identificación y el monto de dinero asociado con la prestación de estos servicios es necesario evaluar si es posible usar un esquema de identificación que sea mas robusto y que contribuya a minimizar la probabilidad de materialización de riesgos relacionados con pérdidas de reputación y fraudes o pérdidas económicas para las entidades que ofrecen los diferentes servicios y para los ciudadanos que los requieren. Es necesario cuestionarnos con respecto a la seguridad; confidencialidad, integridad, disponibilidad y no repudio; que puede ser ofrecida por los métodos que usan la huella dactilar como mecanismo de identificación.

Actualmente, se puede afirmar que no contamos con el procedimiento más seguro para garantizar la identidad de los ciudadanos. Por razones económicas se usan dispositivos de captura de huellas dactilares que solo toman ciertos patrones de las huellas (porciones de la imagen dactilar) lo que puede llevar a que una porción de huella sea similar a otras huella de diferentes ciudadanos, incrementando la posibilidad de suplantaciones o robos de identidad. [1] Este mecanismo tiene otras debilidades. La información de la huella puede ser tomada de las fotocopias de una cédula que son entregadas por un ciudadano para adelantar diferentes tramites. Las huellas digitales

[1] Fuente: https://m.eltiempo.com/justicia/investigacion/pensionado-denuncia-que-jefe-del-eln-le-robo-su-identidad-321596
[2] Fuente: https://www.elheraldo.co/judicial/con-fotocopia-de-la-c-dula-les-basta-los-falsificadores-28870
[3] Fuente: https://www.eltiempo.com/justicia/investigacion/pensionado-denuncia-que-jefe-del-eln-le-robo-su-identidad-321596

también pueden ser tomadas de las bases de datos de huellas gestionadas por establecimientos a los cuales un ciudadano accede normalmente; hoy día es una practica común en diferentes entidades y establecimientos. Es muy fácil crear un molde de las huellas, las cuales pueden ser obtenidas de cada objeto que tocamos o manipulamos cotidianamente. Además, la huella dactilar no es universalmente inclusiva, algunas personas tienen limitaciones físicas que dificultan la captura de manera adecuada de las huellas de estos ciudadanos.

Teniendo en cuenta las debilidades mencionadas, es recomendable que el país considere otros métodos de identificación y autenticación. Por ejemplo, mecanismos seguros de identificación digital, que permitan autenticar de forma segura a los ciudadanos mayores de edad, garanticen no repudio e integridad de los trámites digitales y permitan que las personas tengan control total sobre sus datos. En el mundo es posible encontrar gobiernos que ya implementaron esquemas de identificación digital como Suecia[4], Nigeria[5], Estonia[6] y Uruguay[7]. Las tecnologías usadas varían, pero los usos son prácticamente los mismos: adelantar trámites gubernamentales, operaciones tributarias, gestión de salud electrónica, trámites de pensiones, voto electrónico, licencias de conducción y firmar digitalmente.

2. Propuesta

Con el objetivo de identificar una solución más apropiada este proyecto evaluó diferentes tecnologías con base en un conjunto de componentes mínimos esperados y un conjunto definido de criterios de evaluación. A continuación se presentan brevemente los componentes y los criterios.

2.1 Componentes

- Factor Biométrico utilizado por el sistema propuesto de identificación y autenticación digital.
- Tarjetas. Que tecnología usan las tarjetas para comunicarse con los agentes externos a ellas.
- Punto de comparación del factor. Identifica el esquema de interacción del factor biométrico con la tarjeta, teniendo en cuenta almacenamiento y comparación.
- Sistema operativo de los chips de las tarjetas (*Card Operating System - COS*) es el sistema operativo de los chips de las tarjetas. Se debe tener en cuenta cuál es el que mejor se acomoda a los requerimientos presentes y proyecciones futuras de lo que debería tener el proyecto.
- Tecnologías de apoyo para proveer información soportada por el sistema.
- Marcos de Autenticación para soportar la validación de la identidad de la tarjeta contra el sistema de autenticación.

2.2 Criterios de evaluación

La tabla siguiente presenta la lista de criterios seleccionados para evaluar las tecnologías disponibles. Cada criterio tiene un conjunto de subcriterios para hacer más preciso el esquema de evaluación. Por cada subcriterio adicionamos una pregunta para aclarar el significado del mismo.

[4] https://polisen.se/Aktuellt/Nyheter/2015/Juni/Mojligt-att-resa-i-hela-EU-med-nationellt-ID-kort/
[5] https://www.nimc.gov.ng/
[6] https://e-estonia.com/solutions/e-identity/id-card/
[7] https://mi.iduruguay.gub.uy/

Criterio	Subcriterio
1.Madurez	1.1. Longevidad: ¿Cuánto tiempo lleva la tecnología en operación?
	1.2. Interoperabilidad: ¿La tecnología está basada en algún estándar? ¿de preferencia abierto?
2.Rendimiento	2.1. Tiempos de respuesta: ¿Qué tan rápido responde el sistema a una solicitud individual?
	2.2. Indice de efectividad: ¿Qué tan libre de fallas es la tecnología durante su operación? False Acceptance Rate y False Rejection Rate.
	2.3. Tasa de transferencia: Tasa de volumen por unidad de tiempo.
	2.4. Estabilidad: ¿En qué medida la tecnología es resistente ante factores externos como el paso del tiempo, nuevos desarrollos, u otros?
3.Escalabilidad	3.1. Adaptación a volumetría de datos o de usuarios: ¿Qué tan bien se adapta la tecnología ante el incremento o reducción en el volumen de datos o usuarios en el sistema?
	3.2. Simplicidad para adquirir e instalar HW y SW: ¿Qué tan fácil es para el diseñador adquirir e implementar la solución incluyendo software y hardware?
4.Facilidad de implementación	4.1. Integración con otras tecnologías. ¿Qué tan fácil resulta integrar la tecnología evaluada con otras heredadas y futuras?
	4.2. Facilidad de aprendizaje: ¿Qué tan fácil es para un operador aprender a usar la tecnología?
	4.3. Aceptación cultural: ¿Que tan acogida resulta la tecnología en el entorno?
	4.4. Interfaz de usuario amigable: ¿Qué tan sencillo es para un operador interactuar con el software y hardware de la solución?
5.Seguridad	5.1. Confidencialidad: ¿Qué tan difícil es acceder de manera no consentida al factor a evaluar?
	5.2. Disponibilidad: ¿Porcentaje que cuentan con el factor a evaluar?
	5.3. Elusión: ¿Qué tal fácil es suplantar el factor evaluado? ¿Qué tan difícil es de engañar al lector?
	5.4. Resiliencia: Capacidad para superar incidentes. ¿Qué tan óptimo es su proceso de recuperación frente a situaciones adversas?
	5.5. Privacidad: ¿Cómo está reconocido dentro la normativa el factor?; contribuye o soporta los lineamientos que en materia de protección de das personales han sido definidos por la reglamentación nacional.
6.Adquisición y Mantenimiento	6.1. Facilidad de compra de HW y SW: ¿Qué tan barato es el factor?
	6.2. Mantenimiento: ¿Qué tan costoso es el mantenimiento de la tecnología? ¿Qué tanto tiempo toma realizarlo?

Además de determinar la lista de criterios, es necesario establecer su importancia; no todos los criterios son igual de importantes. Para asignar pesos que representen la importancia usamos el método de análisis jerárquico. Este método evalúa la importancia de cada criterio frente a los demás y permite establecer una matriz de correlacionamiento de pesos. La evaluación se realizó utilizando la escala Saaty (1: igual importancia, 3: importancia moderada, 5: importancia fuerte de un elemento sobre otro, 7: extrema importancia de un elemento sobre otro. 2,4,6,8: valores intermedios entre juicios adyacentes). Después de consultar con diferentes usuarios expertos sobre la importancia (/peso) de cada criterio las calificaciones se consolidaron y normalizaron generando la asignación de peso que la Ilustración 1 presenta.

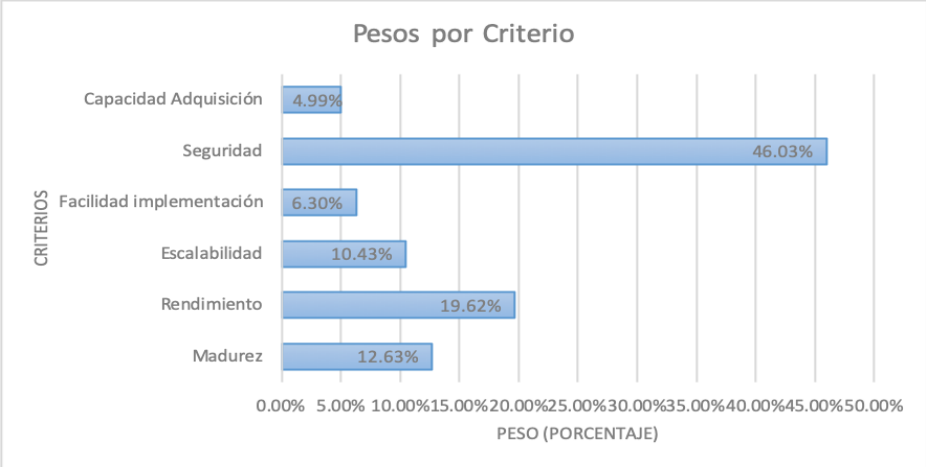


Ilustración 1. Distribución de pesos por criterio después de consolidar asignaciones de expertos y normalizar.

3. Evaluación

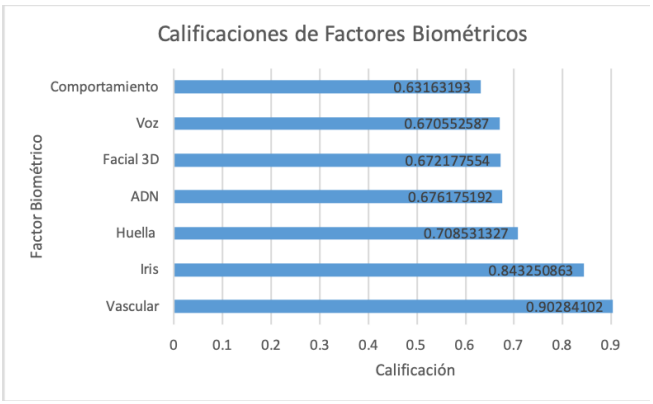
Esta sección presenta los componentes que evaluamos, sus principales características y ventajas.

- Identificadores biométricos: huella dactilar, iris, reconocimiento facial, reconocimiento de voz, análisis de conducta, reconocimiento vascular y ADN. En todos los casos consideramos los requerimientos de privacidad. Además, evaluamos FRR y FAR como medida de efectividad.
    - Privacidad. La ley de protección de datos personales indica que los factores biométricos son considerados como datos personales y por esto es necesario contar con mecanismos que permitan que los datos recogidos solo sean accesibles por personas autorizadas. Considerando los requerimientos mencionados, es preferible un proceso de autenticación con un dispositivo descentralizado porque implica menos riesgos. El dispositivo descentralizado queda en posesión del usuario y sus datos no tienen que almacenarse en una base de datos. Por el contrario, si se utiliza un proceso de identificación que requiere una base de datos externa, el usuario pierde control de sus datos, con todos los riesgos que ello implica.
    - Índice de efectividad. Se calculó con base en dos factores FRR (*False Rejection Rate*) y FAR (*False Acceptance Rate*). La primera mide la probabilidad de rechazar a un usuario debidamente registrado, mientras la segunda mide la probabilidad de aceptar a un usuario que no está debidamente registrado. Los factores con los niveles FRR y FAR más bajos (es decir, los mejores factores) son huella dactilar, iris y reconocimiento vascular. [2,3]
- Tarjetas. Las tarjetas de memoria solo permiten almacenar información y no cuentan con capacidad de cómputo. Por ello nos concentramos en tarjetas con microprocesador con interfaces por contacto, sin contacto y dual (ambos tipos de interfaz).
- Punto de comparación del factor. La tarea de comparación puede darse en un servidor o en la tarjeta. En la primera la comparación de los datos de un individuo con la información almacenada se ejecuta en un servidor central, en la segunda la comparación se da en la tarjeta. Una mejora, actualmente en desarrollo, de la comparación en tarjeta es la tecnología BSoC (*Biometric System on Card*) que además de comparar la información, incorpora el lector. Es decir, no es necesario tener un lector externo. [4]

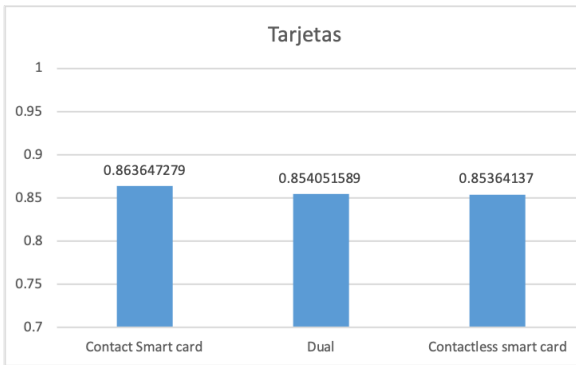
- Sistema Operativo. Las tarjetas cuentan con un sistema operativo que facilita la interacción con el hardware. Los sistemas más usados son JavaCard y MultOS. JavaCard se basa en Java un lenguaje muy conocido, además era de código abierto no requería licenciamiento, lo que ayudó a acelerar la cantidad de aplicaciones disponibles y reducir el costo de las mismas. MultOS permite interoperar distintas aplicaciones en una misma tarjeta sin que estas tengan el mismo lenguaje (Soporta C, MEL y Java). Su estándar es abierto a desarrollo y es administrado por el consorcio MultOS.
- Marcos de autenticación. El marco de autenticación define en gran parte el protocolo usado para autenticar a un usuario: FIDO UAF, FIDO U2F, OpenID Connect y SAML.
    - FIDO UAF (Universal Authentication Framework)[8]: Provee un marco de autenticación donde una vez registrado, el usuario no tiene necesidad de volver a ingresar la contraseña. La autenticación pasa a enfocarse contra el dispositivo local desde el cual se haya realizado la autenticación. La llave privada es retenida por el usuario.
    - FIDO U2F **(**Universal Second Factor)[9]: Esquema donde el servidor al que se está tratando de conectar el usuario genera un reto. El usuario genera su par de llaves pública y privada. Responde al reto firmando con su llave privada utilizando el dispositivo puesto como segundo factor.
    - OpenID Connect[10]: es un protocolo construido sobre las especificaciones de OAuth 2.0, con un token ID adicional que provee información sobre el usuario sobre como el cómo y cuando el usuario se autenticó. El usuario se autentica contra el OpenID Provider. Este genera un token que le sirve al usuario para autenticarse contra la app a la que quiere acceder.
    - SAML[11]: Define un esquema XML para describir e intercambiar información de seguridad entre entidades en línea.
- Tecnologías de apoyo. Corresponden a mecanismos adicionales de las tarjetas que pueden mejorar la velocidad de lectura de las tarjetas físicas, proporcionar medios alternativos para leer la información contenida en las tarjetas o hacer que estas tarjetas sean más seguras. Las tecnologías evaluadas son código de barras, banda magnética y *machine-readable text*. El código de barras y la banda magnética son ampliamente conocidos. La última tecnología, texto legible por máquina, utiliza algoritmos para optimizar y reconocer los caracteres dentro de las imágenes y convertirlos en texto que sea legible por los seres humanos.

Resultado. Teniendo en cuenta la información recopilada de diversas fuentes se asignó una calificación entre 1 y 4 a cada tecnología bajo cada uno de los criterios. 1 significa que no satisface las expectativas, 2 por debajo de las expectativas, 3 satisface parcialmente las expectativas y 4 satisface completamente las expectativas. La Ilustración 2 resume los resultados obtenidos con la asignación de pesos presentada en la Ilustración 1. Asignando la prioridad al ítem de seguridad, el reconocimiento vascular sobresale como el mejor factor biométrico (Ilustración 2-(a)).

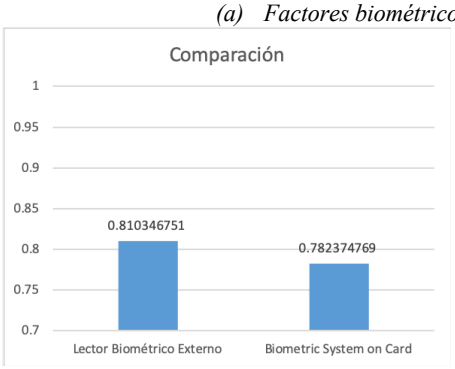
[8] https://fidoalliance.org/specifications/
[9] 94 https://developers.yubico.com/U2F/Libraries/Using_a_library.html
[10] 95 https://openid.net/connect/
[11] https://www.ibm.com/support/knowledgecenter/es/SSQL82_9.5.0/com.ibm.bigfix.doc/Platform/Config/c_what_is_saml_2_0.html



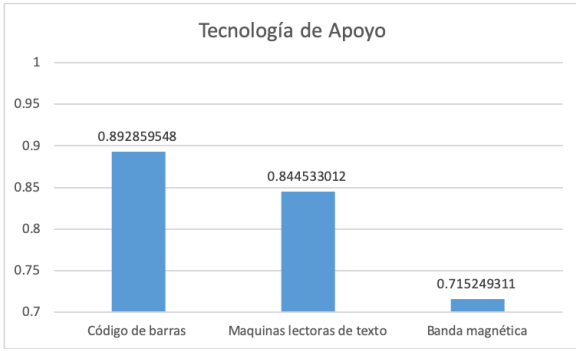
(a) Factores biométricos



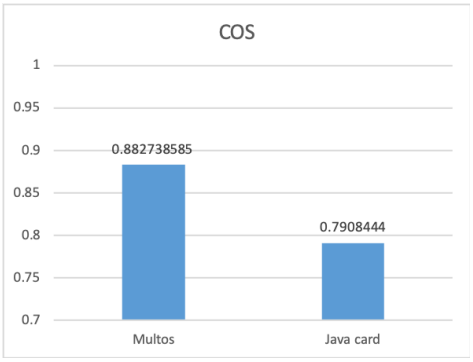
(b) Tarjetas



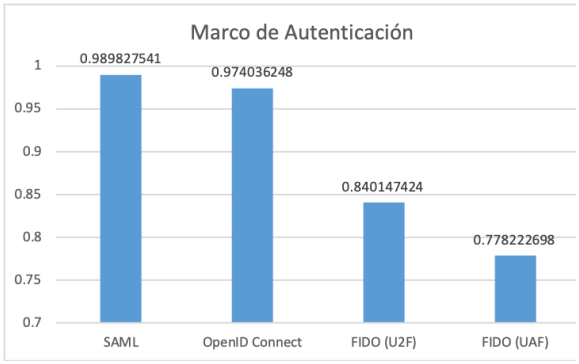
(c) Tecnología de comparación



(d) Tecnologías de apoyo



(e) COS



(f) Marcos de autenticación

Ilustración 2. Calificaciones resultantes para las tecnologías evaluadas.

Hoy día el uso del reconocimiento cardiovascular no es un mecanismo usado de manera común, no encontramos información de países que usen este método para manejar identificación y autenticación de ciudadanos. Sin embargo, es una opción interesante dado que hay sistemas robustos que hacen uso de este método de identificación [5], pero no de forma masiva sino para atender un grupo seleccionado de la población, específicamente el "NYU Langone Medical Center", hospital especializado que usa un sistema de cotejo de venas para identificar y llevar el registro médico de pacientes. Otro ejemplo de un sistema de este tipo es el software *Finger Vein ATM* diseñado por la empresa HITACHI para ser usado por empresas financieras como método de identificación de sus usuarios, eliminado así la necesidad de tarjetas o claves para acceder a los servicios ofrecidos, sin embargo, su adopción no es tan alta como se esperaba, lo cual limita nuestra capacidad evaluar los resultados de este dispositivo. En el entorno colombiano, encontramos el

reporte de Palm Secure de Fujistu Colombia, un sistema diseñado como mecanismo de control de acceso a espacios físicos, métodos de login para el acceso a servidores o estaciones críticas, acceso a terminales de venta y cajeros automáticos, entre otros. [6]

Con respecto al esquema de comparación el externo supera al sistema biométrico integrado en la tarjeta (Ilustración 2c). Para el sistema operativo MultOS sobresale por encima de JavaCard (Ilustración 2e). La mejor tecnología de apoyo es el código de barras (Ilustración 2d). Y sobre los marcos de autenticación Open ID Connect y SAML tienen resultados muy cercanos (Ilustración 2f).

Como un cambio en la asignación de pesos de los criterios de evaluación puede afectar los resultados, adelantamos un análisis de sensibilidad creando otros escenarios al asignar (i) mayor peso a la capacidad de adquisición y mantenimiento, (ii) a rendimiento y escalabilidad y (iii) a escalabilidad e implementación. En los resultados encontramos:

- Con respecto al factor biométrico. La huella se ve ligeramente beneficiada cuando se aumenta el peso a adquisición y mantenimiento. En los demás escenarios el reconocimiento vascular se presenta como la mejor alternativa.
- Con respecto al punto de comparación. El lector biométrico externo aumenta su ventaja con respecto al lector biométrico interno en la tarjeta en los escenarios adicionales.
- Con respecto a la tarjeta. La tarjeta dual se presenta como la mejor opción en los demás escenarios.
- Con respecto al sistema operativo de las tarjetas. Cuando se da mayor peso a costo y facilidad de implementación, JavaCard se muestra mejor que MultOS. Este último tiene mejores resultados cuando se aumenta el peso de rendimiento, escalabilidad y seguridad.
- En todos los escenarios se observan resultados muy cercanos entre Open ID Connect y SAML, lo cual sugiere que a la luz de los criterios seleccionados los dos marcos de autenticación son razonables.
- La tecnología de código de barras se muestra como la mejor bajo los distintos escenarios para la tecnología de apoyo.

3. Recomendaciones

Después de un análisis cuidadoso, recomendamos el uso de tarjetas inteligentes que cuenten con algoritmos que permitan la comparación de un factor biométrico diferente a la huella dactilar. El uso de tarjetas inteligentes hace posible implementar procedimientos de identificación que no requieran conexión a una base de datos centralizada, sino que se pueden realizar de manera local en cada una de las tarjetas, lo que contribuye a garantizar la confidencialidad y privacidad de los datos personales de los ciudadanos. Además, es posible establecer procedimientos que permitan contar con doble factor de autenticación, de tal forma que la tarjeta sólo se activará cuando el usuario presente su factor biométrico al lector de la tarjeta, lo que evitaría fraudes derivados de la pérdida de la tarjeta contribuyendo a la integridad y no repudio de las transacciones asociadas.

Para que este tipo de iniciativas sean viables es fundamental contar con el apoyo del gobierno nacional a nivel económico, normativo y social, de tal manera que se cuente con los recursos necesarios para definir un servicio seguro y de calidad. Este apoyo también contribuiría a minimizar la resistencia al cambio que se pueda presentar por parte de los ciudadanos.

Referencias

[1] Eset, ‘Demuestran que Es Posible Vulnerar Lectores de Huella Digital Mediante Huellas Maestras | WeLiveSecurity’, 2018 <https://www.welivesecurity.com/la-es/2018/11/16/demuestran-que-es-posible-vulnerar-lectores-de-huella-digital-mediante-huellas-maestras/>.
[2] Bayometric, ‘Top Five Biometrics: Face, Fingerprint, Iris, Palm and Voice’ <https://www.bayometric.com/biometrics-face-finger-iris-palm-voice/>.
[3] Biocatch, ‘Behavioral Biometrics: A Primer on the Future of Cybersecurity’, 2018 <https://www.biocatch.com/blog/behavioral-biometrics-primer-future-cybersecurity>.
[4] Chen Tai Pang and others, ‘Biometric System-on-Card’, in Encyclopedia of Biometrics (Boston, MA: Springer US, 2014), pp. 1–6 <https://doi.org/10.1007/978-3-642-27733-7_9136-1>.
[5] Ferrerosa Luisa ; Ceron Felipe, ‘Diseño De Un Sistema De Reconocimiento Biométrico Vascular’, The Effects of Brief Mindfulness Intervention on Acute Pain Experience: An Examination of Individual Difference, 1 (2014)
[6] Fujitsu, ‘PalmSecure® - Fujitsu Colombia’ <https://www.fujitsu.com/co/solutions/business-technology/security-solutions/biometrics/> .