# ANALYSIS FOR THE DEVELOPMENT OF A MULTIFACTOR AUTHENTICATION SYSTEM BASED ON ASYMMETRIC KEY ENCRYPTION, FOR E-VOTING

# ANÁLISIS PARA EL DESARROLLO DE UN SISTEMA DE AUTENTICACIÓN MULTIFACTOR BASADO EN CIFRADO DE CLAVE ASIMÉTRICA, PARA VOTO ELECTRÓNICO

**Cristian Camilo Pérez Bohórquez, Gina Maribel Valenzuela Sabogal**

**Universidad de Cundinamarca**
Facatativá, Cundinamarca, Colombia.
Tel.: 57-1-8920706 | 892 0707
E-mail: {ccamiloperez, gvalenzuela}@ucundinamarca.edu.co

**Abstract:** The authentication process constitutes an indispensable factor for the operations carried out through the internet, due to the increasing progress that the development of new e-learning platforms, electronic government and the economy of the current world has represented in the last decade, for what a digital, verifiable and trustworthy identity is of vital importance to avoid fraud, corruption and data loss in an information system. The methods based on multi-factor authentication, widely used in different sectors of the current web industry and public key encryption algorithms are the basis for the study and development of a multi-factor authentication module for an internet voting platform. The current project starts from the generation of asymmetric keys for platform users, a repository of credentials and the implementation of a challenge response protocol linked to the authentication process, being the basis for the establishment of an institutional digital environment and electronic government.

**Keywords:** Authentication, Informatic security, Cryptography, Asymmetric Key.

**Resumen:** El proceso de autenticación constituye un factor indispensable para las operaciones que se realizan a través de internet, debido al creciente avance que ha representado en la última década el desarrollo de nuevas plataformas de e-learning, gobierno electrónico y la economía del mundo actual, por lo que una identidad digital, verificable y de confianza es de vital importancia para evitar el fraude, la corrupción y la perdida de datos en un sistema de información. Los métodos basados en la autenticación multifactor, ampliamente usados en diferentes sectores de la industria web actual y los algoritmos de cifrado de clave pública son la base para el estudio y desarrollo de un módulo de autenticación multifactor a fin de una plataforma de voto por internet. El proyecto en curso parte de la generación de claves asimétricas para los usuarios de la plataforma, un repositorio de credenciales y la implementación de un protocolo de desafío respuesta vinculado al proceso de autenticación, siendo la base para el establecimiento de un entorno digital institucional y gobierno electrónico.

**Palabras Clave:** Autenticación, Seguridad Informática, Criptografía, Clave Asimétrica.

## I. INTRODUCCIÓN

En la actualidad, con el uso masivo de dispositivos electrónicos, sumado al creciente desarrollo y aplicación de nuevas tecnologías de la información, el tratamiento de datos y el pleno auge del internet, se ha generado un aumento en la necesidad de implementar procesos de autenticación que permitan determinar la identidad de los usuarios que interactúan con un sistema, sobre todo en sectores como la industria, la economía y el gobierno electrónico, en los que es indispensable minimizar el riesgo de fraude en las partes involucradas en una transacción web. Para ello existen múltiples estándares y alternativas que ofrecen diferentes niveles de seguridad que van desde métodos de autenticación simple como la implementación de usuario y contraseña, hasta validación de la identidad por medio de análisis biométrico.

Actualmente se destaca el uso de métodos de autenticación multifactor y de identidad basados en criptosistemas y esquemas de firma digital. La infraestructura de clave pública (PKI) se postula como la base para dichos procesos, debido al éxito de su implementación en países como Estonia (Vinkel, 2014) , en donde los avances en materia de gobierno electrónico y voto por internet han demostrado el potencial de dicha tecnología, que se basa en un conjunto de protocolos y estándares de seguridad por los cuales se realiza un proceso de generación y distribución de claves relacionadas a través de un algoritmo o función matemática y almacenadas en un DNI electrónico o el teléfono móvil del titular, además de que permite la administración de certificados digitales, autenticación de identidad y firma digital. Principios en los que el proyecto está basado, tomando algunos de los elementos característicos de dicha infraestructura y que se mencionan en este artículo.

## II. PROBLEMA

La influencia de los sistemas en el mundo actual, ha llevado a la automatización de diferentes procesos que se realizaban de forma presencial, trámites para los que era inevitable tener que desplazarse a una entidad y hacer filas interminables, sin mencionar el desperdicio de papel que supone un impacto sobre el desarrollo sostenible de una sociedad a la que la sobreexplotación de recursos está llevando a un punto sin retorno. Muchos países y sectores de la industria han considerado nuevas alternativas como brindar a sus usuarios la posibilidad de realizar diferentes tipos de transacciones a través de internet, una solución viable, necesaria. Sin embargo, aún tiene muchos retos que enfrentar, sobre todo en materia de seguridad, debido a que dichas transacciones que se realizan a través de un dispositivo electrónico, desde un ambiente no controlado carecen de supervisión, suponiendo un incremento en el riesgo de suplantación de identidad y la necesidad de determinar si una persona que intenta acceder a una información es quien dice ser en realidad, a esto se suma la desconfianza que genera la implementación de dichos sistemas en algunos sectores de la población, adicionalmente la brecha digital existente entre las generaciones más adultas y los más jóvenes. Lo anterior lleva al planteamiento de las siguientes preguntas; ¿Cómo asegurar la identidad de una persona o entidad a través de un entorno web? ¿cuáles son las alternativas que existen actualmente en materia de autenticación e identidad digital?

## III. IDENTIFICACIÓN, AUTENTICACIÓN Y AUTORIZACIÓN EN PLATAFORMAS DIGITALES

Cuando se hace referencia a las medidas de seguridad dentro de una infraestructura digital; la identificación de usuarios, el proceso de autenticación y la autorización son conceptos clave.


*Fig. 1 Identificación, Autenticación y autorización (Andress & Winterfeld, 2014).*

### *3.1. Identificación*

La identificación, es simplemente una afirmación de quiénes somos, como persona o a través de un sistema informático.

### *3.2. Autenticación*

La autenticación es, en un sentido de seguridad de la información, el conjunto de métodos que utilizamos para establecer un reclamo de identidad como verdadero. Es importante tener en cuenta que la autenticación solo establece si el reclamo de identidad realizado es correcto (Andress & Winterfeld, 2014).

La autenticación a través de dispositivos electrónicos constituye la base del futuro de las operaciones transaccionales y los trámites a distancia, por lo que una identidad digital de confianza es el punto de partida para un sistema o

plataforma que requiera ofrecer garantías de seguridad a sus usuarios. Además, se define como un elemento que hace parte de un sistema más amplio de prácticas, procedimientos e implementaciones técnicas, que trabajan juntas para proteger los sistemas de información, las redes y las comunicaciones electrónicas (OECD, 2007).

Es primordial entender que la identidad digital es la representación única de un sujeto involucrado en una transacción en línea, esta siempre es única en el contexto de un servicio digital, pero no necesariamente necesita identificar de forma única al sujeto en todos los contextos. En otras palabras, acceder a un servicio digital puede no significar que se conoce la identidad de la vida real del sujeto (Grassi, Garcia, & Fenton, 2017).

La directriz de autenticación electrónica establecida por el Instituto Nacional de Estándares y Tecnología NIST (Burr et al., 2013), señala tres factores básicos que caracterizan a los sistemas de autenticación estándar:

- El primero de ellos es aquel basado en el conocimiento, más conocido KBA (Knowledge Based Authentication), que hace referencia a cosas que únicamente conoce cada persona, por ejemplo, el uso de usuarios y contraseñas privadas.
- El segundo a partir de la posesión, se caracteriza por la obtención de un documento o elemento único por parte de cada usuario, ya sea un documento de identidad ID-Card, un token o un certificado digital.
- Por último, se encuentra la autenticación basada en todo aquello inherente a cada persona, recurriendo a datos biométricos como la huella dactilar, las facciones del rostro o la voz.

Las buenas prácticas señalan que, para operaciones de riesgo alto, se debe utilizar una combinación de al menos dos de estos elementos (Pareja, Pedak, Gómez, & Barros, 2017) lo que se denomina autenticación multifactor.

*3.2.1. Autenticación Multifactor (MFA)*

La autenticación multifactor, hace referencia a la implementación de las fortalezas de los métodos anteriormente mencionados, para un mayor nivel de seguridad, teniendo en cuenta que la combinación de múltiples fuentes de datos garantiza mayor precisión y confianza a la hora de realizar la identificación de un usuario.

La multiplicación del número de factores de autenticación aumenta el nivel de seguridad general, pero supone algunos retos como la administración del ciclo de vida de cada factor, la usabilidad del sistema, los costes de elementos electrónicos como tarjetas, lectores o sensores biométricos y la carga del servicio de ayuda al usuario (Evidian, 2015) .

Teniendo en cuenta los principios mencionados anteriormente, el objetivo de implementar un MFA es dificultar la intrusión de usuarios no autenticados a un sistema, dispositivo o red; debido a que este constituye un sistema de defensa por niveles.

*Tabla 1: niveles de garantía para autentificación de entidades*

| Nivel | Descripción |
|---|---|
| **1-Bajo** | Poca o ninguna confianza en la identidad declarada. |
| **2-Medio** | Cierta confianza en la identidad declarada. |
| **3-Alto** | Mucha confianza en la identidad declarada. |
| **4-Muy alto** | Muchísima confianza en la identidad declarada. |

*Tomado del marco de garantía de autenticación de entidad (Unión Internacional de Telecomunicaciones, 2012).*

1) Nivel de garantía 1: Existe cierta confianza en la identidad de la persona que se ha autenticado en diferentes eventos. Generalmente se emplea cuando el nivel de riesgo que representa una autenticación errónea es bajo.

2) Nivel de garantía 2: Se emplea cuando el riesgo que representa la autenticación errónea de un usuario es moderado, por lo que se puede recurrir a la autenticación de doble factor.

3) Nivel de garantía 3: En este nivel de garantía se emplean los sistemas de autenticación multifactor, debido al nivel de riesgo considerable que representa la autenticación errónea de una entidad, además de protocolos de encriptación y envió seguro de datos.

4) Nivel de garantía 4: Cuando los riesgos que representa una autenticación errónea son muy altos, se recurre a la utilización de medios físicos inalterables además del uso de certificados

digitales que permitan identificar idóneamente a su portador.

*3.3. Autorización*

La autorización nos permite determinar, una vez que hemos autenticado a la parte en cuestión, exactamente qué se les permite hacer (Andress & Winterfeld, 2014). Uno de los mecanismos de autorización más utilizados es el control de acceso basado en roles.

## IV. CRIPTOGRAFÍA

La palabra criptografía proviene en un sentido etimológico del griego Kriptos, "Ocultar", y Graphos, "escritura", lo que significaría ocultar la escritura, o en un sentido más amplio sería aplicar alguna técnica para hacer ininteligible un mensaje. Es la ciencia encargada de diseñar funciones o dispositivos, capaces de transformar mensajes legibles o en claro a mensajes cifrados de tal manera que esta transformación (cifrar) y su transformación inversa (descifrar) sólo pueden ser factibles con el conocimiento de una o más llaves (Paredes, 2006).

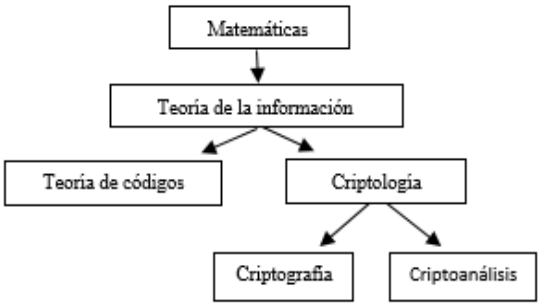


*Fig. 2 Origen de la Criptografía (Paredes, 2006).*

El uso de técnicas criptográficas tiene como propósito prevenir algunas faltas de seguridad en un sistema computarizado. La seguridad, en general, se considera como un aspecto de gran importancia en cualquier corporación que trabaje con sistemas computarizados.

Otros autores plantean que la Criptografía se ocupa del problema de enviar información confidencial por un medio inseguro. Para garantizar la confidencialidad, podría asegurarse el medio de transmisión o bien la información; la Criptografía utiliza este último enfoque, encripta la información de manera que, aun cuando se encuentre disponible para cualquiera, no pueda utilizarla, a menos que alguien autorizado la descifre (Marrero Travieso, 2003).

*4.1. Clasificación de la criptografía moderna*

La criptografía se divide en dos grandes ramas, la Criptografía de clave privada o simétrica y la Criptografía de clave pública o asimétrica (Andress & Winterfeld, 2014).

*Criptografía Simétrica:* La criptografía de clave simétrica, también conocida como criptografía de clave privada, utiliza una sola clave tanto para el cifrado del texto sin formato como para el descifrado del texto cifrado.

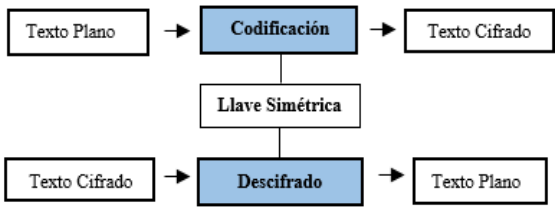


*Fig. 3 Proceso de clave para criptografía simétrica (Medina & Miranda, 2015).*

*Criptografía Asimétrica:* la criptografía de clave asimétrica, también conocida como criptografía de clave pública, utiliza dos claves: una clave pública y una clave privada. La clave pública se usa para cifrar los datos enviados desde el remitente al receptor. la clave privada se utiliza para descifrar los datos que llegan al extremo receptor (Andress & Winterfeld, 2014).

Si encripta datos utilizando la clave pública de alguien, solo su clave privada correspondiente puede descifrarla (Ristić, 2015). Principio empleado en el desarrollo del módulo de autenticación para voto electrónico, por medio de un protocolo de desafío-respuesta.

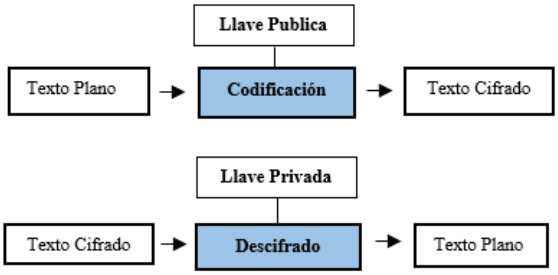


*Fig. 4 Proceso de clave para criptografía asimétrica (Medina & Miranda, 2015).*

*4.2. Algoritmos de clave Asimétrica*

El algoritmo RSA, llamado así por sus creadores Ron Rivest, Adi Shamir y Leonard Adleman, es un algoritmo asimétrico utilizado en todo el mundo, incluso en el protocolo Secure Sockets Layer (SSL), que se utiliza para asegurar muchas transacciones comunes como Web y e- tráfico de correo RSA se creó en 1977 y sigue siendo uno de los algoritmos más utilizados en el mundo hasta el día de hoy (Andress & Winterfeld, 2014).

Se basan en la dificultad de factorizar números enteros de gran tamaño (Franchi, 2012).

- Cifrado de pequeñas cantidades de datos, por ejemplo, claves.
- El sistema RSA permite longitudes variables, siendo aconsejable actualmente el uso de claves de no menos de 1024 bits.
- Algoritmo más sencillo de entender para su aplicación.
- Firmas digitales.

ECC, la criptografía de curva elíptica (ECC) lleva el nombre del tipo de problema matemático en el que se basan sus funciones criptográficas. ECC tiene varias ventajas sobre otros tipos de algoritmos (Andress & Winterfeld, 2014).

- Mayor fuerza criptográfica.
- Claves más cortas que muchos otros tipos de algoritmos.
- Rápido y eficiente.

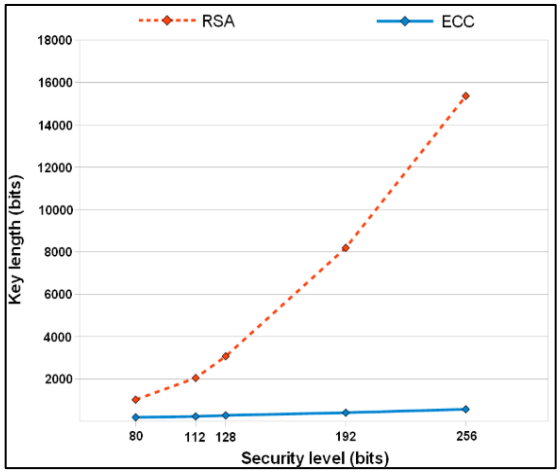


*Figura 5 Comparación de longitud de clave para criptosistemas RSA y ECC (Gayoso, Hernandez, & Sanchez, 2010).*

Por lo anterior se ha elegido la implementación de llaves ECC en el desarrollo del proyecto.

## V. HERRAMIENTAS DE DESARROLLO

El desarrollo del proyecto se basa fundamentalmente en el lenguaje de programación Java. Desde su aparición en la década de 1990, este lenguaje ha experimentado un crecimiento constante con respecto al número de programadores y despliegues comerciales, siendo utilizado de forma masiva en aplicaciones web y corporativas (Martínez, Ávila, García, & Encinas, 2005). En la arquitectura Java, la API de seguridad (construida alrededor el paquete java.security) es una de las principales interfaces del lenguaje.

La implementación de la biblioteca Java Cryptography Architecture (JCA) que es una especificación del lenguaje que precisa interfaces y clases abstractas que sirven de base para las implementaciones concretas (Engines y Providers) de algoritmos criptográficos y es parte del API de seguridad del lenguaje (Maiorano, 2010), en conjunto con Java Cryptography Extension (JCE) que más exactamente proporciona implementaciones para cifrado, algoritmos de encriptación, generación y concordancia de claves de acuerdo a los lineamientos definidos por la JCA.

*5.1. Proveedor Bouncy Castle*

es un kit de herramientas criptográficas de terceros. Las API criptográficas de este proveedor son atendidas por una organización benéfica australiana, la Legión de Bouncy Castle Inc., que se ocupa del mantenimiento de dichas API (Ganesh Adhagale, 2014).

- Bouncy Castle tiene soporte para muchos algoritmos
- Es libre en términos de licencia.
- Ofrece soporte matemático para criptografía de curvas elípticas. Las clases de utilidad se pueden usar para producir y leer cadenas BASE64 y hexadecimales.

## VI. METODOLOGIA

Para el diseño y desarrollo del módulo de autenticación se establece el uso de elementos de la metodología ágil basada en SCRUM, debido a que este es un marco dentro del cual puede emplear diversos procesos y técnicas (Schwaber & Sutherland, 2011) . La forma en que se adapta esta metodología al desarrollo del módulo, se basa en el establecimiento de objetivos claros y alcanzables en un tiempo determinado por el equipo de trabajo, que permitan evidenciar avances en el desarrollo del proyecto además de generar un plan estratégico

basado en dicho progreso, con una respuesta al cambio y a los problemas que se puedan presentar, además de la retroalimentación en cada uno de los procesos presentes en la ejecución e incremento del software.

La organización y jerarquización de las tareas está fundamentado en el modelo en cascada para el proceso de desarrollo del software, como se muestra en el siguiente esquema:

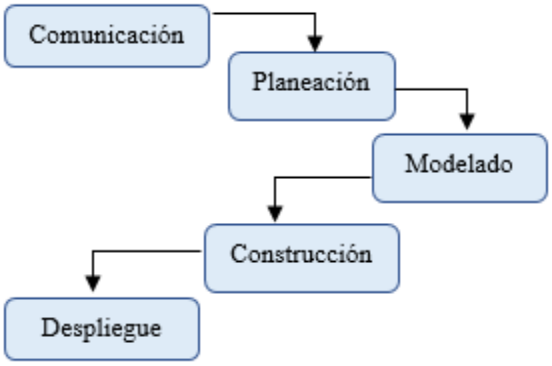


*Fig. 3 Modelo cascada desarrollo de software(Pressman, 2010).*

## VII. RESULTADOS

*Problema de almacenamiento de clave:* Durante el estudio de los requerimientos y el diseño del módulo se estableció que posterior al proceso de registro, cada usuario es el responsable de almacenar la llave privada. Por lo que se concluyó en la necesidad del desarrollo de una aplicación móvil complementaria al sistema de registro y generación de claves, cuya función sería el almacenamiento de dicha llave privada y ser un elemento primordial e indispensable para el proceso de autenticación y acceso a la plataforma de voto por internet.

*Problema de distribución de clave:* Consiste en la problemática que se genera en el momento del envió de la clave privada a cada usuario por un canal "inseguro" de comunicación y constituye un riesgo de seguridad, debido a la posible interceptación de la llave privada. Para implementar una solución se establecieron los siguientes puntos:

1. Para evitar una posible suplantación de identidad, las llaves privadas están asociadas única y exclusivamente a un número de teléfono móvil. Por lo que, si un intento de acceso al sistema se realiza con una clave privada valida, desde un móvil diferente al asociado inicialmente, se denegara la solicitud.

2. Para realizar el envío de la clave privada a cada usuario, se implementará un método de cifrado adicional, por lo que, si alguna clave privada es interceptada durante el envío, no podría ser descifrada y por lo tanto seria invalida.

## VIII. CONCLUSIONES

En la actualidad, el proceso de autenticación en entornos digitales, es uno de los factores fundamentales de la seguridad dentro de un sistema de información y constituye una herramienta para conservar la integridad, confidencialidad y veracidad de los datos allí almacenados, además de minimizar el riesgo de fraude y suplantación de identidad.

Existen diferentes métodos o técnicas de autenticación que se implementan actualmente en plataformas y servicios en la red. Estos se dividen en tres grandes grupos; a) aquellos basados en el conocimiento (usuario y contraseña), b) Por medio de la posesión de un elemento o clave única y C) a través de todo aquello inherente a la persona o datos biométricos.

Con respecto a los niveles de garantía que existen en los sistemas de autenticación, cabe resaltar que dependen de los requisitos y el nivel de confidencialidad de la información que se pretende resguardar, teniendo en cuenta el impacto que genere un acceso malintencionado, en la integridad de los datos y el sistema en sí.

Es recomendable la implementación de más de un factor de autenticación que asegure un nivel de confianza más alto en la identificación de entidades que intentan acceder a un sistema, además del uso de técnicas de cifrado de datos y envió seguro de información.

Las llaves asimétricas son una herramienta de cifrado, que representan un avance para el proceso de autenticación en entornos no controlados y son la base para la implementación de la firma digital en transacciones electrónicas.

## VIII. REFERENCIAS


Andress, J., & Winterfeld, S. (2014). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice: Second Edition. In *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice: Second Edition*. Retrieved from https://www.academia.edu/32643426/Andress_Jason_Basics_of_Information_Security_Second_Edition

Burr, William E, Dodson, Donna F, Newton, Elaine M, … Emad A. (2013). *Archived NIST Technical Series Publication Superseding Publication(s) Electronic Authentication Guideline*. 54. https://doi.org/10.6028/NIST.SP.800-63-2

Evidian. (2015). *Los 7 métodos de Autentificación más utilizados*.

Franchi, M. R. (2012). Algoritmos De Encriptación De Clave Asimétrica. *UNIVERSIDAD NACIONAL DE LA PLATA*.

Ganesh Adhagale, S. S. V. (2014). *A Comparative Study of Various Cryptographic Algorithm Used in Bouncy Castle Toolkit*. Retrieved from www.ijetae.com

Gayoso, V., Hernandez, L., & Sanchez, C. (2010). A survey of the elliptic curve integrated encryption scheme. *Journal of Computer Science and Engineering*, *2*(2), 7–13.

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). *Digital identity guidelines: revision 3*. https://doi.org/10.6028/NIST.SP.800-63-3

Maiorano, A. (2010). *Criptografía para desarrolladores*. 1–14. Retrieved from www.segu-info.com.arhttp://www.cuspide.com/detalle_libro.php/9872311382http://www.amazon.com/CRIPTOGRAFIA-Tecnicas-Desarrollo-Profesionales-Spanish/dp/9872311382

Marrero Travieso, Y. (2003). La Criptografía como elemento de la seguridad informática. *ACIMED*, *11*(6). Retrieved from http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000600012

Martínez, V. G., Ávila, C. S., García, J. E., & Encinas, L. H. (2005). Elliptic Curve Cryptography: Java implementation issues. *Proceedings - International Carnahan Conference on Security Technology*. https://doi.org/10.1109/ccst.2005.1594866

OECD. (2007). *OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication*. Retrieved from www.oecd.org/sti/security-privacy

Paredes, G. (2006). *INTRODUCCIÓN A LA CRIPTOGRAFÍA*. *7*, 1–17. Retrieved from http://www.revista.unam.mx/vol.7/num7/art55/int55.htm

Pareja, A., Pedak, M., Gómez, C., & Barros, A. (2017). *La gestión de la identidad y su impacto en la economía digital*. https://doi.org/10.18235/0000786

Pressman, R. S. (2010). *Ingenieria del Software - Un Enfoque Practico 5b: Edicion (Spanish Edition)*. Retrieved from www.FreeLibros.me

Ristić, I. (2015). *BULLETPROOF SSL AND TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications Free*. Retrieved from www.feistyduck.com

Schwaber, K., & Sutherland, J. (2011). The Scrum Guide - The Definitive Guide to Scrum: The Rules of the Game. *Scrum. Org*, *October*, Vol. 2, p. 17. https://doi.org/10.1053/j.jrn.2009.08.012

Unión Internacional de Telecomunicaciones. (2012). *X.1254 : Marco de garantía de autenticación de entidad. 1254*.

Vinkel, P. (2014). *Voto por Internet en Estonia*. Retrieved from https://www.researchgate.net/publication/281348239