La Independencia Tecnológica de la Firma Digital para un Gobierno Abierto 2.0 en Perú

Bach. Gino Brehan Aguilar Alcarráz, Mg. Percy Edwin de la Cruz Vélez de Villa

gino.aguilara@gmail.com, 08200206@unmsm.edu.pe , pdelacruzv@unmsm.edu.pe

Facultad de Ingeniería de Sistemas e Informática de la Uniiversidad Nacional Mayor de San Marcos
Calle Germán Amézaga N° 375, Ciudad Universitaria - FISI, Lima 1
Lima – Perú

Resumo: *La finalidad de este paper es presentar a la aplicación de la firma digital en un entorno web a través de la tecnología y fundamentos de la PKI con la ayuda de la invocación por protocolos que evita y previene las diferentes incompatibilidades entre las soluciones que deben coexistir dentro de alguna realidad informática ,ya que es un dolor de cabeza lidiar con integraciones complicadas, robustas y realizar pruebas de concepto que se resumen en tiempo, costes y recursos tecnológicos para que se pueda desplegar una nueva tecnología. El duro trabajo de los desarrolladores, los directores de TI o gerentes es elegir una nueva tecnología que contribuirá al desarrollo de sus organizaciones deben tener el mínimo impacto en su infraestructura, y esto es un tema que siempre que uno se enfrenta. Es por ello que en base a experiencias pasadas y en estudios realizados sobre la importancia y los avances significativos que ha sufrido la firma digital , se demuestra que es posible implementar una solución de firma digital web totalmente independiente de componentes terceros como applets de JAVA, JVM, ActiveX, plugins de navegadores y en definitiva de aplicaciones de terceros. Esto ayudará a que se pueda tener un único estándar sobre el cual las entidades dentro del estado peruano puedan realizar la firma digital con valor legal y respaldo jurídico, creando un vínculo de no repudio con la información firmada digitalmente por el firmante a través de un dispositivos criptográfico en donde reside su identidad digital.*

Palabras clave: firma digital, certificado digital, invocación por protocolos, independencia, PKI.

Abstract: *The motivation behind the development of this paper is to introduce the digital signature technology that is a current reality for Peru, and is made possible to implement in web systems based on PKI technology and protocol invocation , avoiding future incompatibilities between software that currently live inside the informatics reality, as far as we know , we always face with new and complex software integrations and even to do some proof of concept it takes time, costs and technological resources in order to deploy a new technology. The hard work for developers, CIOs and managers is to choose a new technology that will contribute to the development of their organizations must have the minimal impact on their infrastructure, and this is an issue that that one always faces. Based on experience and applied studied related on the importance and significant advances that digital signature has suffered, this paper shows the importance of using a digital signature technology that is completely independent of any JAVA (applets, JVM, etc.), ActiveX, add-ons, plugins or in general any third party software technology and it is possible to implement through the invocation protocols. This will help to get or establish a unique standard that could be implemented in the Peruvian government to make digital signatures with legal valued and legal support over currents laws, policies and decrees, generating a strong link between the singer and the information signed digitally through a cryptographic device where the digital identity of its owner resides.*

Palabras clave: firma digital, certificado digital, invocación por protocolos, independencia, PKI.

1 Introducción

La tecnología de la firma digital está teniendo, cada vez mayor protagonismo e impacto en las soluciones tecnológicas, las cuales sufren constantes ataques malintencionados de terceros, incluso usuarios internos hacia el recurso más valioso de cualquier organización, la información, que fluye por los sistemas y reside en los repositorios pudiendo comprometer la integridad y la confidencialidad de esta información representada en un conjunto de bits que son fácilmente manipulables por los mismo usuarios, el administrador de base datos o el responsable tecnológico de cada organización sin que se pueda repudiar o negar los cambios realizados de manera fehaciente y con un respaldo legal que lo ampare.

Es por ello que la firma digital se basa en un concepto de claves o llaves asimétricas (una de ellas, la privada permite cifrar la información y, la pública, permite descifrar y poder validar la información por el destinatario) proporcionando así una robustez y garantía que cuando un documento electrónico es firmado digitalmente este sea integro, autentico, no repudiable y se confíe de la procedencia del mismo [11]. La tecnología PKI permite generar un "código" hash resumen [9], el cual es vinculado al archivo original y con la clave privada del poseedor del certificado digital, es posible encriptarla y firmar el hash obtenido anteriormente. Esto garantiza que nadie más pueda tener una firma digital idéntica [1], luego de haber firmado el documento es verificable por cualquier software tercero que implemente un algoritmo de verificación de firma digital en un momento post firma. Si bien la solución involucra diferentes entes del tipo humano, hardware y software para que pueda coexistir y funcionar esta tecnología, siempre ha tenido el problema de la integración de la firma digital en diferentes sistemas informáticos llevando a costes excesivos y cambios de infraestructura tanto

hardware y software.

Podemos recordar que exigen algunas soluciones que utilizan applets de Java [12] para poder funcionar y/o interfieren con la accesibilidad como fue el caso de la tecnología ActiveX en el Gobierno de Korea [2] que no permitía un correcto desempeño en sus computadoras para poder hacer firma digital y no era accesible para los usuarios finales que eran los ciudadanos.

2 Teoría del dominio y trabajos previos

El Gobierno Electrónico, según lo define la Organización de las Naciones Unidas (ONU), es el uso de las Tecnologías de la Información y la Comunicación (TIC), por parte del Estado, para brindar servicios e información a los ciudadanos, aumentar la eficacia y eficiencia de la gestión pública, e incrementar sustantivamente la transparencia del sector público y la participación ciudadana.

Como parte de aumentar dicha eficiencia y eficacia, existen diferentes entidades que promueven y propician el uso de la tecnología para brindar al ciudadano un gobierno transparente utilizando las herramientas tecnologías vigentes.

La firma digital cumple con los siguientes pilares establecidos en:

Según la ONGEI [39], «El uso eficiente de las Tecnologías de la Información y la Comunicación (TIC) es un elemento transversal en la definición de políticas nacionales relacionadas con la gobernabilidad democrática, la transparencia y el desarrollo equitativo y sostenible» es necesario para un gobierno abierto dentro del Perú.

En el siguiente gráfico se muestra cómo el Gobierno Electrónico es uno de los ejes transversales de una política de modernización que apoya el desarrollo de una gestión pública orientada a resultados.

Figura 1: Pilares centrales de la Política de Modernización de la Gestión Pública en el Perú [36]

Según el Plan de desarrollo de la Sociedad de la Información y el Conocimiento, Agenda Digital 2.0 publicado en el CODESI y en cumplimiento de la sociedad peruana acceda a los beneficios que brinda el desarrollo de las tecnologías de la información y comunicación en todos sus aspectos; la firma digital contribuye al logro de la Estrategia 1 «Impulsar la Interoperabilidad entre las instituciones del Estado para la cooperación, el desarrollo, la integración y la prestación de más y mejores servicios para la sociedad» y la Estrategia 3 «Desarrollar e implementar mecanismos para asegurar el acceso oportuno a la información y una participación ciudadana como medio para aportar a la gobernabilidad y transparencia de la gestión del Estado» del Objetivo 7 «Promover una Administración Pública de Calidad orientada a población».

Según la PCM [36], Gobierno Electrónico es uno de los ejes transversales de una política de modernización que apoya el desarrollo de una gestión pública orientada a resultados.

Las soluciones basadas en la PKI no son un tema nuevo, se han venido trabajando en soluciones tecnológicas que a la fecha los usuarios convencionales no se han percatado que existía, es así que podemos mencionar que soluciones como e-commerce que garantizan las transacciones en línea a través de internet cifrando los datos enviados desde el navegador cliente hacia el servidor donde son descifrados, la manera más sencilla para saber si un navegador web es seguro es verificando la barra de direcciones URL del navegados donde deberá empezar como en sufijo https:// , que denota que se utiliza un certificado SSL que garantiza y se confía en la comunicación punto a punto.

En la actualidad existen leyes, reglamentos y normativas que propician la tecnología de la PKI, servicios de valor añadido (SVA) y la aplicación de la firma digital pueda tener el mismo valor legal y jurídico como una firma manuscrita, se listan a continuación los documentos que respaldan la aplicación dela firma digital en la República del Perú:

- Ley N° 27269 – Ley de Firmas y Certificados Digitales.
- Ley N°27310 – Ley que modifica el artículo 11 de la Ley N°27269.
- Ley N°27291 – Ley que permite el uso de medios electrónicos para la manifestación de voluntad y la utilización de la firma electrónica.
- Decreto Supremo N°052-2008-PCM – Reglamento de la Ley de Firmas y Certificados Digitales.
- Decreto Supremo N° 070-2011-PCM – Decreto Supremo que modifica el Reglamento de la Ley N°27269, Ley de Firmas Certificados Digitales y establece normas aplicables al procedimientos registral en virtud del Decreto Legislativo N°681 y ampliatorias.
- Decreto Supremo N°105-2012-PCM- Establecen disposiciones para facilitar la puesta en marcha de la firma digital y modifican el Decreto Supremo N°052-2008-PCM – Reglamento de la Ley de Firmas y Certificados Digitales.

RENIEC, es reconocido como la Autoridad de Certificación y de Registro del Estado Peruano creado por ley, el cual está encargado de la emisión, revocación y renovación de los certificados digitales soportados en el DNIe o en archivos *.pfx*[10] para las personas jurídicas y sistemas automatizados de firma digital.

[10] Pfx: Los certificado en software son generados en este tipo de formato.

La Autoridad Administrativa Competente, INDECOPI, que es el encargado de regular a todas las empresas que suministran software de firma digital, autoridades de certificación privadas, servicios de sellado de tiempo y servicios de valor añadido, los cuales deben cumplir satisfactoriamente las guías de acreditación vigentes [25], [26], [27], para ser incorporadas a la TSL[11] garantizando así un control y gestión que permita la armonía del uso de la firma digital en los diferentes ámbitos.

La firma digital es el único mecanismo electrónico con el cual podemos garantizar los siguientes aspectos:

- Integridad. Permite que la verificación del documento original no haya sido modificada.[11]
- Autenticidad. La pertenencia al autor del documento firmado. [11]
- No repudio. Sirve para que el firmante no pueda negar un documento firmado con su clave privada. [11].

3 Componentes de la firma digital

A continuación se explica el modelo de firma digital en un entorno web utilizando la invocación por protocolos de aplicaciones nativas en el cliente

3.1 Función hash

La función nos permite garantizar parte de la seguridad de la firma digital ya que es una operación unidireccional que relaciona un hash resumen a un documento, existe actualmente algunos algoritmos que ya han sufrido ataques de colisiones y son fácilmente vulnerados y no proporciona la seguridad para este tipo de aplicaciones.

Esto es posible ya que se genera un hash resumen del documento o los datos a firmar son generados por una función unidireccional, y para poder obtener el archivo original desde el hash es necesario realizar ataques de colisión a fin de obtener el valor original [9].

Tabla 1: Comparación de operaciones lógicas, estado actual y complejidad de hardware [9]

ALGORITHM	LOGICAL OPERATION	CURRENT STATUS	HARDWARE COMPLEXITY
MD5 algorithm	AND,OR,NOT,Rotating shifts	Collision	Medium
SHA1 algorithm	AND,OR,NOT,Rotating shifts,XOR	Collision	Large-scale
SHA2 algorithm	AND,OR,NOT,Rotating shifts,XOR	Running	Large

Como se puede apreciar el algoritmo vigente que es recomendado utilizar para aplicaciones de firma digital es la de SHA2 ya que a la fecha no ha sufrido una colisión y es el algoritmo más seguro.

3.2 Firma digital

Existen diferentes algoritmos que permiten la realización de la firma digital entre los cuales tenemos el DSS, RSADS, ECDSA. Existe una gran ventaja en el número del tamaño de las claves o llaves públicas utilizadas entre el ECDSA y el RSADS, pero la falencia que se encuentra es que no está acreditada por FIPS[12] para poder ser utilizada para la firma digital, lo cual es una oportunidad no aprovechada. Sugerimos que pueda ser considerada dentro de un algoritmo seguro de firma digital y se empiecen a hacer implementaciones basadas en él.

Tabla 2: Algoritmos de Firma Digital [1]

Name of Algorithm	Type and Characteristics	Min. Key Size
Digital Signature Standard (DSS) [5]	FIPS 186-2 digital signature Digital signature based on SHA1 hash, unencumbered (no patents, no licenses)	1024bits
RSA Digital Signature [6]	RSA digital signature (FIPS approved) Previously patented digital signature	1024 bits
Elliptic Curve Digital Signature (ECDSA) [7]	Digital signature based on elliptic curve key technology uses smaller keys than other public key technologies but may be encumbered by various	160 bits

3.3 Sellado de tiempo

El sellado de tiempo es otra firma digital adicional que se encarga de acreditan la fecha y hora en el cual los datos han existido y se firman digitalmente, y esto puede ser verificable a lo largo del tiempo si se aplica una firma longeva incluyendo en el mismo documento firmado digitalmente, la CRL[13], OCSP[14], y cadena de certificación de la CA[15] asociado al poseedor del certificado digital quien hace la firma.

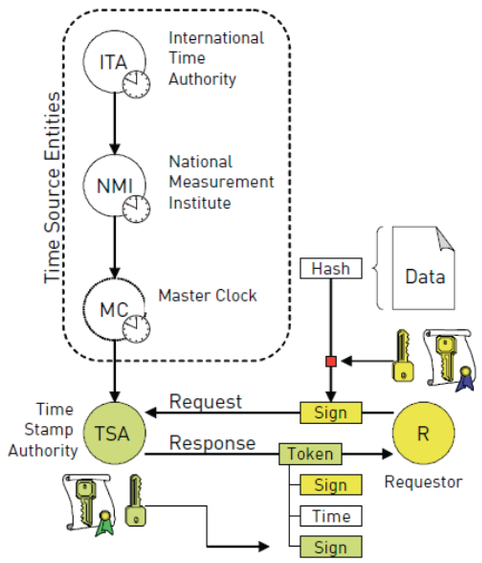

Figura 2: Sello de tiempo de confianza [6]

[11] TSL: Lista de Servicios de Confianza

[12] FIPS: Estándares Federales de Procesamiento de Información, en su traducción en español, hace referencia

[13] CRL: Lista de Certificados Revocados

[14] OCSP: Protocolo en Línea de Estado del Certificado

[15] CA: Autoridad de Certificación

3.4 Marca gráfica

La marca gráfica es básicamente una representación visual de una imagen que hace referencia a la firma digital en un formato PAdES [13], es conveniente realizar una firma gráfica por firmante ya que de otro se incrementa el tamaño del PDF firmado. Si bien la firma gráfica no es la firma digital propiamente hablando, pero los usuarios confían más en una marca que haga referencia a su firma digitalizada o un sello referenciado a su persona o entidad de trabajo. Esto es un tema más cultural y de transición tecnológica.

4 Esquema de firma digital propuesto

En esta sección se describe el flujo de la firma digital web propuesto.

Para este ejemplo se debe tener un token o tarjeta inteligente insertado en la computadora cliente desde donde se realiza la petición de firma digital, así mismo debe contener un certificado digital reconocido que pueda realizar firma digital.

Paso 1: El componente cliente nativo debe encontrarse instalado en el Sistema Operativo host, desde donde se realizará la petición de la firma digital.

Paso 2: Desde un cliente web se envía una petición a través de unos parámetros obligatorios y necesarios para realizar la firma digital, esta petición es enviada a un servidor donde se encuentra presente el servicio de firma digital.

Paso 3: Este servidor autoriza el proceso de firma digital, y responde enviando un script a través de HTTP, y despierta el aplicativo cliente ya instalado previamente.

Paso 4: Se obtiene el documento PDF a firmar de manera local.

Paso 5: Se solicita el PIN correspondiente del dispositivo criptográfico donde reside el certificado digital.

Paso 6: Se genera el HASH del documento.

Paso 7: Se encripta el HASH con el algoritmo RSADS.

Paso 8: Se reconstruye los bytes firmados a través de un servicio POST y reconstruye el PDF.

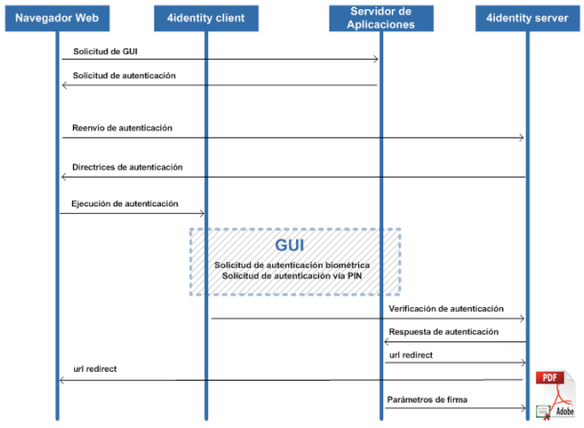

Figura 3: Diagrama de Flujo de Firma Digital [41]

5 Conclusiones y trabajos futuros

El esquema de firma digital basado en el paradigma de invocación por protocolos de una aplicación nativa que residen del lado del cliente es una solución tecnológica basada en PKI que permite la independencia de componentes basados en tecnología JAVA, ActiveX, o cualquier otro plugin requeridos en los navegadores web convencionales para poder operar.

Es posible replicar este modelo de firma digital web en cualquier empresa o entidades públicas del Perú, que gestione sus documentos o información electrónica a través de una solución de workflow web o flujo de trabajo que use el protocolo HTTP o HTTPS permitiendo así la fácil integración dentro de los sistemas.

La carga de la firma digital se hace siempre en el lado del usuario, ya que los firmantes poseen su identidad o certificado digital en un token criptográfica o smartcard, sin sobrecargar al servidor para la realización del procedimiento de firma.

Como trabajo futuro se plante realizar la implementación de un repositorio de certificados digitales centralizados en HSM, permitiendo así la posibilidad de disponer en cualquier momento, en cualquier lugar y en cualquier dispositivo su respectivo certificado digital que permita firmar archivos electrónicos, historias clínicas electrónicas, facturas electrónicas, boletas de pago electrónicas, etc. , todo esto es posible realizar a través de mecanismos de autenticación de doble factor (algo que tengo y algo que se), como por ejemplo mi certificado digital y mi PIN.

Referencias bibliográficas

[1] Ravneet Kaur, Amandeep Kaur, “DIGITAL SIGNATURE”. Presentado en el International Conference on Computing Sciences .978-0-7695-4817-3/12 $26.00 © 2012 IEEE. DOI 10.1109/ICCS.2012.25

[2] Hun Myoung Park, “The Web Accessibility Crisis of the Korea’s Electronic Government: Fatal Consequences of the Digital Signature Law and Public Key Certificate”. Presentado en el45th Hawaii International Conference on System Sciences. 978-0-7695-4525-7/12 $26.00 © 2012 IEEE. DOI 10.1109/HICSS.2012.591

[3] Na Zhu, GuoXi Xiao, “The Application of a Scheme of Digital Signature in Electronic Government”. Prsentado en el International Conference on Computer Science and Software Engineering. 978-0-7695-3336-0/08 $25.00 © 2008 IEEE. DOI 10.1109/CSSE.2008.929.

[4] Konstantinos Markantonakis, Michael Tunstall, Gerhard Hancke, Ioannis Askoxylakis, Keith Mayes, “Attacking smart card systems: Theory and practice” Information Security Technical Report I4, 2009, pp 46-56. doi:10.1016/j.istr.2009.06.001x

[5] Francesco Buccafurri, Gianluca Caminiti, and Gianluca Lax, “Signing the Document Content is not enough: A new Attack to Digital Signature”. 2008,

pp.520-525. 978-1-4244-2624-9/08/$25.00 ©2008 IEEE.

[6] Jeff Stapleton, Paul Doyle, Steven Teppler Esquire, "The Digital Signature Paradox". Presentado en Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 2005 IEEE. 0~7803-9290-6105/$20.000 2005 IEEE.

[7] Desheng Fu, Zhongxuan Wei, "Research and implementation of a digital signature scheme based on middleware", pp.2468-2471. 978-1-4244-8165-1/11/$26.00 ©2011 IEEE.

[8] Ingo Naumann, Giles Hogben, "Privacy Features of European eID Card Specifications".ENISA Position paper,2009.

[9] Erfaneh Noroozi, Salwani Mohd Daud, Ali Sabouhi, "Secure Digital Signature Schemes Based on Hash Functions", Presentado en International Journal of Innovative Technology and Exploring Engineering (IJITEE). ISSN: 2278-3075, Volume-2, Issue-4, March 2013,pp 321-325.

[10] Prakash Kuppuswamy, Peer Mohammad Appa,Dr. Saeed Q Y Al-Khalidi, "A New Efficient Digital Signature Scheme Algorithm based on Block cipher", Presentado en IOSR Journal of Computer Engineering (IOSRJCE). ISSN: 2278-0661, ISBN: 2278-8727Volume 7, Issue 1 (Nov. - Dec. 2012), PP 47-52.

[11] Mr. Parag S.Deshmukh, Mr. Pratik Pande, "A Study of Electronic Document Security". Journal of Computer Science and Information Technology. Vol. 3, Issue. 1, January 2014, pg.111 – 117.

[12] US-CERT.Alert (TA12-240A) Oracle Java 7 Security Manager Bypass Vulnerability (Disponible en: https://www.us-cert.gov/ncas/alerts/TA12-240A).

[13] ETSI TS 102 778-1 V1.1.1, (2009). Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES.

[14] ETSI TS 101 903 V1.4.2 (2010) - Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES).

[15] ETSI TS 101 733 V2.1.1 (2012) - Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES).

[16] Cánovas, Óscar (2002). Propuesta de una Infraestructura de Clave Pública y su Extensión Mediante un Sistema de Gestión Distribuida de Credenciales Basado en Delegación y Roles (Tesis para la obtención del grado de Doctor). Murcia: Universidad de Murcia – Facultad de Informática.

[17] CIPHER, 2012. CRYPTOGRAPHIC OPERATION, Public Key Infrastructure (PKI) [Online] (Disponible en: http://www.cipher.risk.tsukuba.ac.jp/?page_id=609&lang=en).

[18] COMISIÓN MULTISECTORIAL PARA EL DESARROLLO DE LA SOCIEDAD DE LA INFORMACIÓN (2011). Plan de Desarrollo de la Sociedad de la Información del Perú: Agenda Digital 2.0 [Online]. (Disponible en:

http://www.codesi.gob.pe/docs/AgendaDigital20_28octubre_2011.pdf).

[19] CONGRESO DE LA REPÚBLICA DEL PERÚ, 2001. Ley N° 27269, Ley de Firmas y Certificados digitales.

[20] EL PERUANO, 2011. Decreto Supremo que modifica el Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales, y establece normas aplicables al procedimiento registral en virtud del Decreto Legislativo N°681 y ampliatorias. Pág. 447328 – 447329.

[21] EL PERUANO, 2012. Establecen disposiciones para facilitar la puesta en marcha de la firma digital y modifican el Decreto Supremo Nº 052- 2008-PCM Reglamento de la Ley de Firmas y Certificados Digitales. Pág. 476913 – 476914.

[22] Gaikwad, A. P. (2015). Role of Digital Signature for Authentication of E-Documents. International Journal of Scientific Research, Volumen: 4, Issue: 1. January 2015 ISSN No 2277 – 8179, p. 68-7.

[23] García Rojas, 2008. Implementación de Firma Digital en una Plataforma de Comercio Electrónico (Tesis para optar el Título de Ingeniero Informático). Lima: Pontificia Universidad Católica del Perú - Facultad de Ciencias e Ingeniería.

[24] IETF, 2013. X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol. Disponible en: https://www.rfc-editor.org/rfc/pdfrfc/rfc6960.txt.pdf.

[25] INDECOPI-IOFE 2007, "Guía de Acreditación de Entidades de Certificación EC" Versión 3.3, Rev: 03/23-02-2007.

[26] INDECOPI-IOFE 2007A, "Guía de Acreditación de Entidades de Registro ER" Versión 3.3, Rev: 03/23-02-2007.

[27] INDECOPI-IOFE 2008, "Guía de Acreditación de Aplicaciones de Software" Versión 3.4, Rev: 05/04-02-2008.

[28] Kulkarni, S., Chole, V. y Prasad, P. S (2014). Review on Authentication Mechanisms of Digital Signatures used for Certification. IJCSMC, Vol. 3, Issue. 2, February, p.735 – 738.

[29] Ncryptoki, Ugo Chirico. (2014). (Disponible en: http://www.ncryptoki.com/.

[30] NIST, 1998. Public Key Infrastructure (PKI) Technical Specifications: Past A – Technical Concept of Operations. (Disponible en:

http://csrc.nist.gov/archive/pki-twg/baseline/pkicon20b.PDF.

[31] NIST, 2011. Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms

and Key Lengths. NIST Special Publication 800-131A, January 2011.

[32] NIST, 2014. National Cyber Awareness System: Vulnerability Summary for CVE-2013-2465. (Disponible en:

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2465.

[33] NIST, 2015. Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules. (Disponible en:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm.

[34] ONGEI, 2002. Infraestructura de Llave Pública para el Estado Peruano (PKI) Framework (Disponible en:

http://www.ongei.gob.pe/publica/proyectos/4821.pdf)

[35] ONGEI, 2013. Política Nacional de Gobierno Electrónico 2013-2017. (Disponible en: http://www.ongei.gob.pe/docs/Pol%C3%ADtica_Nacional_de_Gobierno_Electronico_2013_2017.pdf)

[36] PCM, 2013. Política Nacional de Modernización de la Gestión Pública al 2021. Disponible en:

http://www.pcm.gob.pe/wp-content/uploads/2013/05/PNMGP.pdf.

[37] WEBTRUST, 2011. Trust Service Principles and Criteria for Certification Authorities Version 2.0 (Disponible en: http://www.webtrust.org/homepage-documents/item54279.pdf.

[38] Oracle, Enero 2016.Whitepaper: Migrating from Java Applets to plugin-free Java technologies Disponible en:
http://www.oracle.com/technetwork/java/javase/migratingfromapplets-2872444.pdf

[39] ONGEI, 2013: Política Nacional de Gobierno Electrónico 2013-2017. Disponible en: http://www.ongei.gob.pe/docs/Pol%C3%ADtica_Nacional_de_Gobierno_Electronico_2013_2017.pdf

[40] CODESI, 2011: COMISIÓN MULTISECTORIAL PARA EL DESARROLLO DE LA SOCIEDAD DE LA INFORMACIÓN (2011). Plan de Desarrollo de la Sociedad de la Información del Perú: Agenda Digital 2.0. Disponible en: http://www.codesi.gob.pe/docs/AgendaDigital20_28octubre_2011.pdf

[41] Best Information Technology for Identification. (Disponible en: http://www.bit4id.com/es/)