Presidencia
Anexo 1101

CARTA Nº 362 -2016/PRE-INDECOPI

Lima, 16 de junio de 2016

Señora
Ana Castillo Aransaenz
Secretaria General
Registro Nacional de Identificación y Estado Civil
Jr. Bolivia 109
Lima.

Referencia: Oficio Nº 000365-2016/SGEN/RENIEC

De mi consideración:

Me dirijo a usted en atención al oficio de la referencia, mediante el cual traslada el Informe Nº 0002-2016/AGM/GCRD/SGCD/RENIEC referido al Análisis comparativo sobre la firma a distancia (server signing) en la IOFE del Perú y bajo el esquema de servicios de confianza y el marco racionalizado para la estandarización de la firma electrónica en la Unión Europea.

Sobre el particular sírvase encontrar adjunto el Informe Nº 006-2016/CFE-INDECOPI emitido por la Secretaría Técnica de la Comisión Transitoria para la Gestión de la Infraestructura Oficial de Firma Electrónica.

Hago propicia la oportunidad para renovarle los sentimientos de mi consideración.

Atentamente,

Heberi Tassano Velaochaga
Presidente del Consejo Directivo

TRP/lv.

Adjunto: Informe Nº 006-2016/CFE-INDECOPI

30899

OFICINA DE ADMINISTRACIÓN DOCUMENTARIA
MESA DE PARTES
JR. BOLIVIA 109 - EDIFICIO CENTRO CÍVICO - LIMA CERCADO
22 JUN. 2016
LA RECEPCION DE ESTE DOCUMENTO NO SIGNIFICA LA CONFORMIDAD DEL MISMO
HORA: 12:13 FIRMA:

Decenio de las Personas con Discapacidad en el Perú
Año de la Consolidación del Mar de Grau

Comisión Transitoria para la Gestión de la I.O.F.E.
Anexo 3613; jdiazm@indecopi.gob.pe

INFORME Nro. 006 -2016/CFE-INDECOPI

A : **Hebert Tassano Velaochaga**
Presidente del Consejo Directivo

DE : **Pedro Castilla del Carpio**
Encargado de la Secretaría Técnica

ASUNTO : **Informe presentado por el Reniec sobre nueva modalidad de firma digital.**

FECHA : **San Borja, 11 de mayo de 2016.**

I. ANTECEDENTES

Se ha recibido el Oficio 0365-2016/SGEN/RENIEC y el Informe 0002-2016/AGM/GCRD/SGCD/RENIEC y se ha requerido la opinión de esta Secretaría Técnica sobre su contenido.

II. ANÁLISIS

1.- Una "Infraestructura de Clave Pública" –en adelante, ICP- es un conjunto de Entidades de Certificación Digital, Entidades de Registro o de Validación de Firmas Digitales y Entidades Prestadoras de Servicios de Valor Agregado[1] sometidas a reglamentos y estándares técnicos y usualmente supervisadas por una autoridad o un organismo de acreditación. En la medida en que las entidades cumplan dichos reglamentos, los servicios que prestan a ciudadanos, empresas y Administración Pública garantizan la autenticidad, la invulnerabilidad, la privacidad y el carácter no repudiable de toda clase de transacciones comerciales y actos jurídicos en general, celebrados a distancia y a través de medios inseguros como la internet.

La ICP nacional tiene la denominación reglamentaria de "Infraestructura Oficial de Firma Electrónica –IOFE-". Por mandato del artículo 57 del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado por el Decreto Supremo 052-2008-PCM y modificado por el Decreto Supremo 026-2016-PCM, el Indecopi es su organismo de acreditación y

---

[1] La denominación de "servicios de valor agregado" abarca, por ejemplo, a los servicios de intermediación electrónica y a los de estampado electrónico de tiempo.

supervisión. Asimismo, en la IOFE el Reniec ejerce los roles de Entidad de Certificación Nacional para el Estado Peruano, Entidad de Certificación y Entidad de Registro.

2.- El fundamento lógico de los servicios provistos en una ICP es la encriptación asimétrica o encriptación de clave pública. En una ICP, una persona natural o jurídica es titular de un par de claves criptográficas y utiliza una de ellas –de carácter estrictamente privado- y un algoritmo de encriptación para generar una secuencia numérica en función de algún documento electrónico *DE* producido o aprobado por ella[2]. La secuencia numérica es denominada "firma digital asociada al documento *DE*"[3]. Cualquier otra persona puede verificar la autenticidad de esta firma digital ya que, por razones matemáticas, es posible revertir los efectos del proceso mediante el uso de la otra clave del titular en el mismo algoritmo. Esta segunda clave tiene carácter público y está expuesta en un certificado digital cuya veracidad es garantizada por una entidad pública o privada digna de confianza. En una ICP la verificación de que una firma digital ha sido generada con determinada clave privada y sólo con ella, puede realizarse por cualquier tercero –por ejemplo, un juez o un árbitro-, que de este modo comprobará la autenticidad del documento electrónico firmado digitalmente. La probabilidad de un fraude basado en la deducción matemática de la clave privada por terceros no autorizados es de varios órdenes de magnitud menor que la probabilidad de fraude en las firmas ológrafas en documentos manuscritos.

3.- Generalmente, el titular de las claves posee una tarjeta (*smart card*) o un *token* criptográfico con un circuito integrado, que a su vez contiene un software de generación de firmas digitales que ejecuta las operaciones descritas en el numeral 2. En años recientes, sin embargo, se ha desarrollado una nueva modalidad que prescinde de *tokens, smart cards* y dispositivos lectores de *smart cards* y que por consiguiente genera ahorro de recursos y elimina el riesgo de la pérdida de estos elementos portátiles. En esta nueva modalidad, las claves privadas de un alto número de personas -eventualmente, de miles de personas- son alojadas en un "Módulo de Seguridad Hardware" (HSM). Después de demostrar su identidad mediante la digitación de una contraseña o mediante el registro de una condición biométrica, cada titular accede desde su computadora personal o su teléfono móvil a su clave privada alojada en el HSM y firma digitalmente sus documentos electrónicos. Se denomina "firma digital centralizada", "firma digital a distancia" o "firma digital en servidor" a la generada mediante este proceso.

---

[2] Para los fines del presente informe esta definición simplificada es suficiente.

[3] Al margen de los temas principales de este informe, cabe indicar que la firma digital no es la única clase de firma electrónica. Otros casos de firmas electrónicas son, por ejemplo: 1) la firma biométrica; 2) la firma escaneada o digitalizada, con la que la Superintendencia Nacional de Aduanas y Administración Tributaria imprime docenas de miles de circulares, notificaciones, órdenes de pago, etc; 3) la firma gráfica que se realiza sobre una tablilla o soporte en algunas empresas (por ejemplo, clínicas) o en algunas entidades públicas como la Dirección Nacional de Migraciones; 4) incluso el nombre que se teclea al pie de un correo electrónico calza en el concepto de "firma electrónica" contenido en el Reglamento de la Ley de Firmas y Certificados Digitales.

4.- La Ley Nro. 27269, Ley de Firmas y Certificados Digitales, y su Reglamento fijan condiciones para el reconocimiento de efectos legales a la firma digital, pero no contienen referencias a la modalidad descrita en el numeral 3[4]. Más bien, en el artículo 7° del Reglamento[5] se indica que la generación de la firma digital –en otras palabras, la aplicación de la clave privada y del algoritmo de encriptación sobre el *hash* o resumen del documento electrónico- ha de estar bajo el control exclusivo del suscriptor del certificado digital asociado. En el artículo 10° se indica que el suscriptor está obligado a mantener el control y la reserva de la clave privada[6].

Este contexto reglamentario nacional no es el más propicio para el empleo de la firma digital centralizada, ya que corresponde a un marco tecnológico en donde la clave privada y el software de generación de firma digital se encuentran alojados, como ya se dijo antes, en una *smart card* o en un token criptográfico. En tales circunstancias es razonable y proporcional responsabilizar al legítimo poseedor de la tarjeta o del token por la reserva de su clave privada; pero ya no lo es tanto cuando su clave privada se encuentra alojada en un dispositivo electrónico físicamente distante, probablemente ubicado en la jefatura informática de la empresa o entidad donde el titular de la clave labora.

5.- En el informe presentado por el Reniec se analiza con encomiable detalle la reglamentación europea y el documento preliminar del estándar técnico que el Comité Europeo de Normalización viene elaborando sobre las condiciones que deberían cumplirse para reconocer a la firma digital centralizada el mismo efecto legal que a otras modalidades de firma digital. Además, se analizan las Guías aprobadas por el Indecopi para la acreditación de Entidades de Certificación Digital, Entidades de Registro, Prestadoras de Servicios de Valor Agregado y Software de Firma Digital, y la Declaración de Prácticas y Políticas de Certificación emitida por el Reniec en su condición de Entidad de Certificación del Estado Peruano. Esta Secretaría Técnica coincide con el informe del Reniec en los siguientes puntos:

1. En las Guías no se incluyen disposiciones relacionadas con la firma digital centralizada. Más bien, en la Guía correspondiente a Entidades de Certificación Digital expresamente se indica que los dispositivos donde puede alojarse la clave privada son: (1) la computadora del titular del certificado digital, (2) el token criptográfico y (3) la *smart card*. Las Guías fueron aprobadas en el año 2008, cuando la tecnología necesaria para la generación de la firma digital centralizada no se hallaba madura aún.

---

[4] Lo cual no es de extrañar si se recuerda que el Reglamento fue promulgado en el año 2008.

[5] **REGLAMENTO DE LA LEY DE FIRMAS Y CERTIFICADOS DIGITALES, APROBADO POR EL DECRETO SUPREMO 052-2008-PCM. ARTÍCULO 7.-** De las características mínimas de la firma digital. Las características mínimas de la firma digital generada dentro de la IOFE son: (...) d) su generación está bajo el control exclusivo del suscriptor.

[6] **REGLAMENTO DE LA LEY DE FIRMAS Y CERTIFICADOS DIGITALES, APROBADO POR EL DECRETO SUPREMO 052-2008-PCM. ARTÍCULO 10.-** De las obligaciones del suscriptor. Las obligaciones del suscriptor son: (...) c) mantener el control y la reserva de la clave privada bajo su responsabilidad.

2. En esta Secretaría Técnica no se ha encontrado en la normativa técnica internacional un documento vigente que sistematice los requisitos para la incorporación de la firma digital centralizada en una ICP oficial, ya sea en América, Europa o Asia. El Reglamento 910/2014 de la Unión Europea se expresa en términos genéricos y favorables a esta modalidad[7], pero no entra en detalles de aplicación efectiva. El documento emitido por el Comité Europeo de Normalización titulado "*Security Requirements for Trustworthy Systems Supporting Server Signing*"[8] es, como se dijo antes, un *Draft* o proyecto de carácter preliminar.

6.- Para esta Secretaría Técnica es claro que en este caso la evolución tecnológica ha desbordado al marco jurídico. Esta circunstancia no es de extrañar si se considera que las tecnologías de la información conforman el sector que progresa más rápidamente en el conjunto general de la técnica. Además el país no puede monitorear la evolución de tecnologías que nacen y maduran en las sociedades desarrolladas del mundo antes de comercializarse aquí.

En todo caso, en el cumplimiento de sus funciones administrativas como organismo de acreditación de la IOFE, el Indecopi debe iniciar acciones para la incorporación reglamentada de esta modalidad de firma digital a la ICP nacional.

A la fecha, esta Secretaría Técnica está actualizando las cuatro Guías de Acreditación para Prestadores de Servicios de Certificación Digital y Servicios Afines. La nueva Guía de Software ya fue aprobada por la CFE. La resolución administrativa que la oficializa se publicará en las próximas semanas en el Diario Oficial El Peruano.

La nueva Guía de Prestadores de Servicios de Valor Agregado está en la última etapa de incorporación de recomendaciones. En la última reunión sostenida con los representantes de las empresas y entidades acreditadas para debatir el contenido del proyecto de esta nueva Guía, se tuvo oportunidad de intercambiar opiniones con los funcionarios del Reniec respecto a la firma digital centralizada. En aquella oportunidad se indicó, y ahora se ratifica, que después de culminar el procedimiento de actualización de las restantes dos Guías -las de Entidades de Certificación Digital y Entidades de Registro- la CFE iniciará el proceso de elaboración de una nueva Guía, la quinta, que se enfocará en esta modalidad de firma digital.

7.- Sin embargo, se debe recordar que el Reglamento de la Ley de Firmas y Certificados Digitales contiene disposiciones –citadas en el previo numeral 4- que no son las más propicias para la incorporación de la firma digital centralizada en el marco jurídico nacional. Cabe indicar que en la Mesa de Trabajo que elaboró el proyecto del Decreto Supremo 026-2016-PCM modificatorio del Reglamento, el Indecopi propuso que se le

---

[7] Se lee en el Considerando 52: *"Debido a sus múltiples ventajas económicas, debe desarrollarse la creación de firmas electrónicas a distancia en un entorno de creación de firma electrónica gestionado por un prestador de servicios de confianza en nombre del firmante."*

[8] "Requerimientos de Seguridad para Sistemas confiables que soportan Firmas en Servidor" (traducción propia). "Firma en Servidor" es otra denominación para la firma digital centralizada.

otorgase la facultad de establecer nuevas modalidades de acreditación cuando la evolución tecnológica lo hiciera necesario y existiesen estándares técnicos internacionales pertinentes. Esta propuesta fue aprobada por los demás integrantes de la Mesa de Trabajo, y de haberse convertido en norma legal hubiera facilitado notoriamente el proyecto de compatibilizar el marco reglamentario nacional con las nuevas modalidades de firma digital. Lamentablemente la propuesta normativa del Indecopi fue descartada en la Comisión de Coordinación Viceministerial y en el texto final del Decreto Supremo 026-2016-PCM, publicado el pasado 29 de abril en el Diario Oficial El Peruano, sólo se otorga al Indecopi la facultad de presentar sugerencias para incorporar en el Reglamento nuevas modalidades de acreditación respaldadas por la evolución tecnológica[9]. Otorgamiento redundante, pues desde 2008 la mera presentación de propuestas para la mejora de la IOFE está en el campo de acción del Indecopi y de cualquiera de los actores de la IOFE.

III CONCLUSIONES

1.- La Ley de Firmas y Certificados Digitales y su Reglamento no contienen referencias a la firma digital centralizada. Algunas disposiciones reglamentarias parecen concebidas en función de los dispositivos de alojamiento de las claves privadas que ya se encontraban en uso durante el proceso de elaboración del Reglamento (años 2007-2008).

2.- Las Guías de Acreditación de Prestadores de Servicios de Certificación Digital y Servicios Afines tampoco incluyen disposiciones relacionadas con la firma digital centralizada.

3.- Una vez que culmine la actualización de las cuatro Guías de Acreditación, el Indecopi debe iniciar acciones para la incorporación reglamentada de esta modalidad de firma digital a la IOFE.

4.- Sin embargo, la eventual aprobación por parte del Indecopi de una eventual quinta Guía de Acreditación centrada en esta modalidad de firma digital no altera el hecho de que el Reglamento contiene disposiciones concebidas para otro escenario tecnológico. No sólo el Indecopi sino otros actores importantes en la IOFE y en el Gobierno Electrónico –el Reniec, la Oficina Nacional de Gobierno Electrónico e Informática, la Superintendencia Nacional de Aduanas y Administración Tributaria, por ejemplo- habrán de sumar esfuerzos para la solución de esta circunstancia.

SECRETARÍA TÉCNICA
CFE

Pedro Castilla
Encargado de la Secretaría Técnica

[9] **DECRETO SUPREMO 026-2016-PCM. DISPOSICIÓN COMPLEMENTARIA MODIFICATORIA SEGUNDA. Incorporación de un segundo párrafo en el artículo 23 (...).** (...) Cuando la evolución tecnológica lo haga necesario, la AAC puede proponer las modificaciones que corresponda al Reglamento de la Ley (...), a fin de establecer modalidades adicionales para los Prestadores de Servicios de Certificación Digital, en base a estándares técnicos internacionales (...).