SISTEMA NACIONAL DE COMPENSACIÓN ELECTRÓNICA

INSTRUCCIONES OPERATIVAS COMUNES DEL SERVICIO DE CENTRALIZACIÓN DE INTERCAMBIOS

INSTRUCCIÓN SNCE/CE/01/054
MODIFICACIÓN DE LA INSTRUCCIÓN SNCE/CE/01/001

Asunto: Medidas de Ciberseguridad en las comunicaciones de extremo a extremo del SNCE.

Las comunicaciones entre las entidades participantes en el SNCE y la plataforma CICLOM del Centro Común de Procesos del SNCE se establecen, bien a través de la red VPN MPLS dedicada de Iberpay, bien mediante la red SWIFT y su servicio File Act. Sobre estas redes, se soportan todas las comunicaciones relacionadas con todos los subsistemas del SNCE. Ambas redes de comunicaciones incorporan sus propios elementos de seguridad que proporcionan amplias garantías de integridad sobre los datos que diariamente intercambian las entidades participantes en los distintos subsistemas del SNCE.

No obstante, el Comité Técnico Asesor del SNCE, a propuesta del Grupo de Ciberseguridad del SNCE, ha considerado oportuno implantar medidas adicionales de seguridad basadas en la incorporación de una firma electrónica extremo a extremo en los ficheros de operaciones que las entidades se intercambian a través de la plataforma CICLOM.

El procedimiento de utilización de la firma electrónica está definido en el documento de "Especificaciones sobre la seguridad extremo a extremo en el SNCE" publicado por Iberpay, de aplicación al subsistema de Transferencias SEPA (SNCE-13) y, básicamente, recoge:

1. La estandarización de un procedimiento de firma electrónica que deberá incorporarse en los intercambios de ficheros de operaciones, tanto desde los Participantes Directos como desde las Entidades Representadas con presentación directa de operaciones, al Centro Común de Procesos del SNCE, como desde éste a las entidades receptoras de los mismos.
2. Un mínimo impacto técnico y operativo en la implantación de los citados procedimientos de firma electrónica, por su sencillez técnica, tanto para las entidades como para Iberpay.
3. Una mayor garantía de autenticidad e integridad de los datos de extremo a extremo, rechazándose los ficheros intercambiados, siempre que no superen los controles de firma electrónica o que ésta sea inconsistente.

Asimismo, el procedimiento de incorporación, validación y aceptación o rechazo de la firma electrónica, contempla los siguientes pasos:

1. La entidad presentadora, una vez generado el fichero de intercambio, realiza un proceso que le permite generar la firma electrónica, que incorpora a los mismos;
2. Una vez firmado el fichero, lo remite a través de la red VPN MPLS o la red Swift al Centro Común de Procesos del SNCE para su proceso;

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

3. Si tras el proceso de validación de la firma electrónica, el Centro Común de Procesos detectara alguna inconsistencia, procede a rechazar el fichero indicando el motivo de dicho rechazo y, una vez subsanado el error, la entidad envía de nuevo el fichero;
4. Asimismo, una vez procesadas las operaciones recibidas, el Centro Común de Procesos del SNCE incorpora la firma electrónica a los ficheros de presentación a las entidades receptoras;
5. Si tras el proceso de validación de la firma electrónica en la entidad receptora, ésta detectara alguna inconsistencia, informa a Iberpay y solicita el reenvío de un nuevo fichero a través del canal habitual; y
6. Una vez superados todos los controles sin incidencias se da por finalizado el proceso de intercambio.

En virtud de lo expuesto, la Sociedad Española de Sistemas de Pago, S.A, a propuesta del Comité Técnico Asesor del SNCE y una vez concluido el trámite de aprobación de su normativa por parte de Banco de España (establecido en la Circular 1/2007, de 26 de enero), ha dispuesto la publicación de la presente instrucción.

ENTRADA EN VIGOR

La presente instrucción entrará en vigor el día 18 de noviembre de 2019, inclusive, fecha de intercambio.

Se acompañan, las hojas modificadas de la Instrucción SNCE/CE/01/001, en las que se incorporan las modificaciones introducidas por la presente instrucción.

En Madrid, a 23 de abril de 2019

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

establecido en la normativa y procedimiento de adhesión del o de los subsistemas implicados;

- Tener en cuenta que esta funcionalidad podrá ser solicitada y utilizada por subsistema, siendo de aplicación a todas sus operaciones.

- Mantener cada mecanismo durante un periodo de tiempo razonable.

- Asumir los gastos propios del mecanismo elegido.

- En el caso de elección de la red SWIFT, asumir los gastos propios de Swift y solicitar su adhesión al Grupo Cerrado de Usuarios (CUG) de Iberpay con carácter previo a las pruebas (CUG de test) y a la puesta en funcionamiento (CUG live).

Asimismo, las entidades que utilicen como mecanismo de envío y recepción de operaciones la opción de EDITRAN-MPLS, podrán, si así lo decide la entidad, tener configurada también la opción de File Act de SWIFT, de cara a su posible utilización en situaciones de contingencia y a la inversa.

La interconexión entre los centros de proceso de los gestores técnicos del Sistema y los centros de procesos de las entidades, permiten llevar a cabo la presentación y recepción de operaciones en los horarios establecidos, así como la distribución de informes y lanzamiento de consultas, en su caso, relativos a la presentación y recepción de operaciones, a los procesos de liquidación y asiento en cuenta, datos estadísticos, etc.

La publicación de los aspectos funcionales y técnicos necesarios para la instalación de los mecanismos de envío y recepción de operaciones y normativa sobre su funcionamiento, así como las sucesivas modificaciones a los mismos, se realizará mediante instrucciones operativas o comunicaciones del SNCE dirigidas a las entidades desde Iberpay. Asimismo, las entidades disponen de Manuales de Operación, Especificaciones Funcionales y Técnicas de cada subsistema en los que se recogen los requerimientos técnicos

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

aplicables en cada momento. Esta documentación complementaria será también de obligado cumplimiento y aplicación para las entidades participantes.

Las entidades vendrán obligadas a prestar cuanta colaboración les sea requerida en la realización de las pruebas necesarias y en los plazos que se fijen para la puesta en funcionamiento de nuevas versiones de los mecanismos de envío y recepción de operaciones que hayan de efectuarse.

2.1 Seguridad en los intercambios del SNCE

2.1.1 Seguridad en las redes de comunicaciones

Tanto la red de comunicaciones VPN MPLS del SNCE como la red FileAct de SWIFT, sobre las que se soportan las comunicaciones del SNCE, incorporan sus propios elementos de seguridad, proporcionando amplias garantías de integridad sobre los datos que diariamente intercambian las entidades participantes en los distintos subsistemas del SNCE en los que participan.

Por lo tanto, no requiere el intercambio de claves criptográficas, salvo en los intercambios de operaciones a través del subsistema de Transferencias SEPA Inmediatas, en el caso de aquellas entidades que utilicen la plataforma de procesamiento online de un proveedor que contemple el uso de estas u otras claves como un requisito necesario.

2.1.2 Seguridad extremo a extremo mediante la firma electrónica de ficheros

Adicionalmente a la seguridad de las redes de comunicaciones, el SNCE incorpora una serie de medidas de ciberseguridad complementarias y enfocadas a garantizar, de extremo a extremo, la integridad de los datos de las operaciones intercambiadas, basadas en la firma electrónica.

La incorporación de la firma electrónica, tras la generación un fichero que contenga operaciones, garantiza la autenticidad de la información contenida en el fichero firmado, al poder detectar una posible

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

manipulación del mismo en caso de que el resultado del proceso de verificación de la firma electrónica en el momento de su recepción no sea el esperado.

a) Definición y objetivo

Se establece el uso de un procedimiento estándar de firma electrónica que se incorpora a los ficheros de operaciones del subsistema de Transferencias SEPA, tanto en los generados por las entidades con conexión directa al Centro Común de Procesos del SNCE, como en los generados por el propio Centro Común de Procesos del SNCE.

Este procedimiento de firma electrónica, basado en el estándar XML Advanced Electronic Signatures - Basic Electronic Signature (XAdES-BES), supone un mínimo impacto técnico y operativo por respetarse la estructura de los ficheros de operaciones al incorporar dicha firma.

La firma electrónica aplica únicamente a los ficheros de operaciones (transferencias, devoluciones, solicitudes de retrocesión y negaciones a dichas solicitudes), quedando excluidos los ficheros de procedimientos de investigación, los de reclamación de información y sus respuestas, así como los ficheros que el Centro Común de Procesos del SNCE envía a las entidades con la confirmación o validación de operaciones y los correspondientes a la información de la liquidación.

b) Procedimiento de incorporación y validación de la firma electrónica

La entidad presentadora, una vez generado el fichero de operaciones correspondiente en el formato adecuado y antes de enviarlo al Centro Común de Procesos del SNCE, firma el fichero siguiendo las especificaciones definidas en el anexo de “Especificaciones sobre la seguridad extremo a extremo en el

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

SNCE" que figure en el Manual de Operación de los subsistemas SEPA del SNCE.

Una vez generada la firma, se envía, junto al fichero de operaciones, al Centro Común de Procesos del SNCE por el canal habitual. Este mismo proceso lo lleva a cabo Centro Común de Procesos del SNCE antes de enviar los ficheros hacia las entidades.

Una vez recibido el fichero con la firma, tanto en las entidades como en el Centro Común de Procesos del SNCE, se inicia un proceso de verificación de dicha firma antes de procesar el contenido del fichero de operaciones. Si este proceso de verificación resulta exitoso, el fichero de operaciones es apto para su proceso.

Por el contrario, si este proceso de verificación de firma resulta fallido, tiene las siguientes consecuencias:

- Proceso fallido en el Centro Común de Procesos del SNCE: el fichero de operaciones no puede procesarse y es rechazado. Ese rechazo se informa a la entidad correspondiente a través del fichero de validación indicando el motivo del rechazo: certificado revocado, firma no correcta o fichero manipulado.
  Tal y como se indica en el apartado anterior, este fichero de validación enviado desde el Centro Común de Procesos del SNCE hacia la entidad, no es objeto de firma electrónica.

  Una vez resuelto el problema que había provocado el proceso fallido de verificación de la firma electrónica, la entidad vuelve a enviar el fichero, debidamente firmado, al Centro. Común de Procesos del SNCE.

- Proceso fallido en la entidad: el fichero de operaciones no puede procesarse. Se informa inmediatamente a Iberpay sobre el error detectado a través de correo electrónico y/o llamada al departamento de operaciones de Iberpay. Adicionalmente, la

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

entidad solicitará a Iberpay el reenvío del fichero a, siguiendo lo descrito en el apartado 2.6 sobre procedimiento de reenvío de ficheros del Capítulo II.

2.2 Configuración del EDITRAN

La configuración de la opción principal básica de comunicación entre los centros de procesos de las entidades y el Centro Común de Procesos del SNCE, en la que es necesario llevar a cabo la identificación de las sesiones, la relación de las sesiones requeridas para los distintos subsistemas y la configuración de los perfiles de cada una de ellas, se llevará a cabo de acuerdo con las Especificaciones Técnicas de cada subsistema, que los gestores técnicos del Sistema pondrán a disposición de las entidades y mantendrá actualizado mediante la oportuna publicación en la Web de Iberpay en la sección Soporte Técnico del SNCE, dándose a conocer mediante correo electrónico de Iberpay.

2.3 Configuración FILEACT

Para la configuración de la opción alternativa a través del servicio File-Act de SWIFT Net, las entidades deberán atender a las instrucciones que para cada subsistema le sean requeridas por los gestores técnicos del Sistema, dadas a conocer mediante la oportuna publicación en la WEB de Iberpay en la sección de Soporte Técnico del SNCE, que se dará a conocer mediante correo electrónico de Iberpay.

2.4 Configuración para Transferencias SEPA Inmediatas

La configuración del mecanismo de intercambio necesario para la comunicación de transferencias SEPA inmediatas entre los centros de proceso de las entidades y el Centro Común de Procesos del SNCE, se llevará a cabo de acuerdo con el documento de Especificaciones Técnicas para las entidades del subsistema de Transferencias SEPA Inmediatas, que se encuentran a disposición de las entidades a través de la página Web de Iberpay.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)