SISTEMA NACIONAL DE COMPENSACIÓN ELECTRÓNICA

SUBSISTEMA GENERAL DE TRANSFERENCIAS SEPA

INSTRUCCIÓN SNCE/CE/13/009

Asunto: Medidas de Ciberseguridad en las comunicaciones de extremo a extremo del subsistema de transferencias SEPA.

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 que las entidades se intercambian a través de la plataforma CICLOM, comenzando esta implantación por el subsistema de Transferencias SEPA.

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 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 intercambiados a través del Centro Común de Procesos del SNCE, 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.

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.

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

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

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 el 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 entidad solicitará al SNCE el reenvío del fichero a través del canal habitual, siguiendo lo descrito en el apartado 2.6 sobre procedimiento de reenvío de ficheros del Capítulo II de las Instrucciones Operativas Comunes.

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.

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

ENTRADA EN VIGOR

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

En Madrid, a 23 de abril de 2019

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