Actualización de algoritmo de firma SHA-256

Tengo un comercio. ¿Me afecta este cambio?

Este cambio afecta a cualquier comercio que utilice TPV-PC de Redsýs comercializado por entidades financieras, ya sea de forma directa, o indirectamente a través de otros integradores técnicos. En general todos los comercios que utilizan el TPV-PC están afectados.

No confundir este cambio del algoritmo de firma de los mensajes intercambiados con TPV-PC con el cambio de certificado realizado el año pasado en Octubre de 2016. En los siguientes puntos mencionamos cómo afecta a los comercios este cambio de algoritmo de firma.

¿Qué es la firma, el SHA-1 y donde se utiliza en relación con TPV-PC?

Toda comunicación entre un comercio y el TPV-PC de Redsýs actualmente va firmada electrónicamente utilizando un algoritmo llamado **SHA-1**. Esto incluye tanto la llamada desde el comercio para solicitar cualquier tipo de pago/devolución/anulación, consulta de operaciones o envío de ficheros, como la respuesta por parte de TPV-PC al servidor del comercio para informar del resultado.

El algoritmo SHA-1 ha sido declarado **obsoleto** por la industria al no considerarse suficientemente seguro (podría ser atacado) y está siendo retirado de todos los sitios web, certificados y software de seguridad. SHA-1 debe ser **sustituido por algoritmos más robustos**, que utilizan una clave de tamaño mayor que hace imposible a día de hoy que un atacante pueda romper su seguridad sin conocer la clave.

Al igual que el resto de la industria, el TPV-PC de Redsýs ha cambiado el sistema de firma entre el comercio y TPV-PC para **adecuarse a los nuevos estándares de seguridad**, por lo que todos los comercios que utilizan TPV-PC deben adecuar sus sistemas para utilizar el nuevo método.

¿Quién puede ayudarme a realizar el cambio?

Los cambios a realizar en el software del comercio dependen de las características de cada uno y de la plataforma software que utilice, por lo que se recomienda que cada comercio emplee los mismos recursos técnicos que fueron utilizados en la implementación original del TPV-PC en su comercio, ya

que no hay una implementación estándar aplicable a todos los comercios.

¿En qué me afecta este cambio?

El cambio del algoritmo de firma afecta tanto a las peticiones como a las respuestas enviadas entre el comercio y TPV-PC. A continuación, se listan los diferentes servicios afectados y los cambios que deberán realizar los comercios:

❖ Web-Service

El proceso de obtención de la firma será siempre el mismo en todos los casos. Lo único que variará es el algoritmo usado para cifrar la cadena sobre la que se firma. Los pasos a seguir son los siguientes:

- Generación de la cadena a firmar: se obtiene concatenando una serie de campos del mensaje con la clave de comercio (proporcionada por Redsýs y única por comercio). La formación de dicha cadena es la misma que está realizando actualmente el comercio.

  Por ejemplo:

  Cadena = tarjeta + caducidad + importe + moneda + comercio + claveComercio

- Generación de la firma: se aplica el algoritmo **SHA-256** sobre la cadena obtenida.

  *Firma = **SHA-256**(Cadena)*

La firma resultante tiene una longitud de 32 Bytes, y será incluida en el mensaje en formato **HEXADECIMAL** (64 caracteres) con mayúsculas.

Redsýs ofrece a los comercios la siguiente URL donde validar la generación de la firma. La página solicitará los siguientes datos:

- Clave de Firma. Clave de comercio obtenida del módulo de Administración de TPVPC.
- Cadena de datos. Datos de la operación según el formato correspondiente.

https://sis-d.redsys.es/TPV_PC/html/sha/sha256_WebService.html

Al pulsar sobre el link "Calcular SHA-256" se calculará la firma y se mostrará un ejemplo del registro de operación completo a incluir en la petición para su posterior procesamiento.

Para este cálculo no se envía ninguna información a TPVPC, todo el código de la página de prueba se ejecuta en el navegador del cliente.

❖ Ficheros

El proceso de obtención de la firma será siempre el mismo en todos los casos en los que sea necesario firmar las operaciones. Para poder garantizar la integridad de las mismas, éstas se firman de forma individual. Lo único que variará es el algoritmo usado para cifrar la cadena sobre la que se firma. Los pasos a seguir son los siguientes:

- Generación de la cadena a firmar: se obtiene concatenando la operación con la clave de comercio (proporcionada por Redsýs y única por comercio). La formación de dicha cadena es la misma que está realizando actualmente el comercio.

  Por ejemplo:

  Operación = 0211111111111111010000491671026022553604061230000000010.009 7812344321001

  ClaveComercio = AAABBB

  Cadena = 0211111111111111010000491671026022553604061230000000010.009 7812344321001AAABBB

- Generación de la firma: se aplica el algoritmo **SHA-256** sobre la cadena obtenida.

  *Firma = **SHA-256**(Cadena)*

La firma resultante tiene una longitud de 32 Bytes, y será incluida en el mensaje en formato **HEXADECIMAL** (64 caracteres) con mayúsculas.

Redsýs ofrece a los comercios la siguiente URL donde validar la generación de la firma. La página solicitará los siguientes datos:

- Clave de Firma. Clave de comercio obtenida del módulo de Administración del TPVPC.
- Cadena de datos. Datos de la operación según el formato correspondiente.

https://sis-d.redsys.es/TPV_PC/html/sha/sha256_Ficheros.html

Al pulsar sobre el link "Calcular SHA-256" se calculará la firma y se mostrará un ejemplo del registro de operación completo a guardar en el fichero para su posterior procesamiento.

Para este cálculo no se envía ninguna información a TPVPC, todo el código de la página de prueba se ejecuta en el navegador del cliente.

❖ Implantado Web

El proceso de obtención de la firma será siempre el mismo en todos los casos. Lo único que variará es el algoritmo usado para cifrar la cadena sobre la que se firma. Los pasos a seguir son los siguientes:

- Generación de la cadena a firmar: se obtiene concatenando una serie de campos del mensaje con la clave de comercio (proporcionada por Redsýs y única por comercio). La formación de dicha cadena es la misma que está realizando actualmente el comercio.

  Por ejemplo:

  Cadena = tarjeta + caducidad + importe + moneda + comercio + claveComercio

- Generación de la firma: se aplica el algoritmo **SHA-256** sobre la cadena obtenida.

  *Firma = **SHA-256**(Cadena)*

La firma resultante tiene una longitud de 32 Bytes, y será incluida en el mensaje en formato **HEXADECIMAL** (64 caracteres) con mayúsculas.

Redsýs ofrece a los comercios la siguiente URL donde validar la generación de la firma. La página solicitará los siguientes datos:

- Clave de Firma. Clave de comercio obtenida del módulo de Administración del TPVPC.
- Cadena de datos. Datos de la operación según el formato correspondiente.

https://sis-d.redsys.es/TPV_PC/html/sha/sha256_WebService.html

Al pulsar sobre el link "Calcular SHA-256" se calculará la firma y se mostrará un ejemplo del registro de operación completo a incluir en la petición para su posterior procesamiento.

Para este cálculo no se envía ninguna información a TPVPC, todo el código de la página de prueba se ejecuta en el navegador del cliente.

❖ Implantado Windows

Redsýs proporcionará la nueva librería con firma SHA-256 a aquellos comercios que actualmente estén trabajando con Tpv-Pc **Implantado** en SHA-1. Una vez registrada, el comercio deberá comprobar que las peticiones se procesan correctamente y que las repuestas se envían firmadas en SHA-256. Los pasos a seguir para validar la firma de respuesta son los siguientes:

- Generación de la cadena a firmar: se obtiene concatenando una serie de campos del mensaje de respuesta con la clave de comercio (proporcionada por Redsýs y única por comercio). La formación de dicha cadena es la misma que está realizando actualmente el comercio para validar la firma de respuesta.

  Por ejemplo:

  Cadena = importe + comercio + pedido + estado + resultado + claveComercio

- Generación de la firma: se aplica el algoritmo **SHA-256** sobre la cadena obtenida.

  *Firma = **SHA-256**(Cadena)*

La firma resultante tiene una longitud de 32 Bytes, y será incluida en el mensaje en formato **HEXADECIMAL** (64 caracteres) con mayúsculas.

Redsýs ofrece a los comercios la siguiente URL donde validar la generación de la firma. La página solicitará los siguientes datos:

- Clave de Firma. Clave de comercio obtenida del módulo de Administración del TPVPC.
- Cadena de datos. Datos de la operación según el formato correspondiente.

https://sis-d.redsys.es/TPV_PC/html/sha/sha256_WebService.html

Al pulsar sobre el link "Calcular SHA-256" se calculará la firma y se mostrará un ejemplo del registro de operación completo a incluir en la petición para su posterior procesamiento.

Para este cálculo no se envía ninguna información a TPVPC, todo el código de la página de prueba se ejecuta en el navegador del cliente.

❖ Implantado Java

Redsýs proporcionará la nueva interfaz con firma SHA-256 a aquellos comercios que actualmente estén trabajando con Tpv-Pc **Implantado Java** en SHA-1. Una vez registrada, el comercio deberá comprobar que las peticiones se procesan correctamente y que las repuestas se envían firmadas en SHA-256. Los pasos a seguir para validar la firma de respuesta son los siguientes:

- Generación de la cadena a firmar: se obtiene concatenando una serie de campos del mensaje de respuesta con la clave de comercio (proporcionada por Redsýs y única por comercio). La formación de dicha cadena es la misma que está realizando actualmente el comercio para validar la firma de respuesta.

  Por ejemplo:

  Cadena = importe + comercio + pedido + estado + resultado + claveComercio

- Generación de la firma: se aplica el algoritmo **SHA-256** sobre la cadena obtenida.

  *Firma = **SHA-256**(Cadena)*

La firma resultante tiene una longitud de 32 Bytes, y será incluida en el mensaje en formato **HEXADECIMAL** (64 caracteres) con mayúsculas.

Redsýs ofrece a los comercios la siguiente URL donde validar la generación de la firma. La página solicitará los siguientes datos:

- Clave de Firma. Clave de comercio obtenida del módulo de Administración del TPVPC.
- Cadena de datos. Datos de la operación según el formato correspondiente.

https://sis-d.redsys.es/TPV_PC/html/sha/sha256_WebService.html

Al pulsar sobre el link "Calcular SHA-256" se calculará la firma y se mostrará un ejemplo del registro de operación completo a incluir en la petición para su posterior procesamiento.

Para este cálculo no se envía ninguna información a TPVPC, todo el código de la página de prueba se ejecuta en el navegador del cliente.

❖ Implantado Linux

Redsýs proporcionará la librería con firma SHA-256 a aquellos comercios que actualmente estén trabajando con Tpv-Pc **Implantado Linux** en SHA-1. Una vez registrada, el comercio deberá comprobar que las peticiones se procesan correctamente y que las repuestas se envían firmadas en SHA-256. Los pasos a seguir para validar la firma de respuesta son los siguientes:

- Generación de la cadena a firmar: se obtiene concatenando una serie de campos del mensaje de respuesta con la clave de comercio (proporcionada por Redsýs y única por comercio). La formación de dicha cadena es la misma que está realizando actualmente el comercio para validar la firma de respuesta.

  Por ejemplo:

  Cadena = importe + comercio + pedido + estado + resultado + claveComercio

- Generación de la firma: se aplica el algoritmo **SHA-256** sobre la cadena obtenida.

  *Firma = **SHA-256**(Cadena)*

La firma resultante tiene una longitud de 32 Bytes, y será incluida en el mensaje en formato **HEXADECIMAL** (64 caracteres) con mayúsculas.

Redsýs ofrece a los comercios la siguiente URL donde validar la generación de la firma. La página solicitará los siguientes datos:

- Clave de Firma. Clave de comercio obtenida del módulo de Administración del TPVPC.
- Cadena de datos. Datos de la operación según el formato correspondiente.

https://sis-d.redsys.es/TPV_PC/html/sha/sha256_WebService.html

Al pulsar sobre el link "Calcular SHA-256" se calculará la firma y se mostrará un ejemplo del registro de operación completo a incluir en la petición para su posterior procesamiento.

Para este cálculo no se envía ninguna información a TPVPC, todo el código de la página de prueba se ejecuta en el navegador del cliente.

❖ Web

Los comercios que empleen la web de Canales proporcionada por Redsýs para el uso de TPV-PC no necesitan realizar ningún cambio. Las modificaciones asociadas a la firma son responsabilidad de TPV-PC y por lo tanto es transparente para el comercio.

¿Por qué debo hacer modificaciones en mi sistema?

El algoritmo actual (SHA-1) en el que se basa la seguridad de la conexión del comercio con TPV-PC (y viceversa) es un algoritmo declarado obsoleto por la industria y los estándares de seguridad, y podría ser objeto de ataques en el futuro. Para asegurar la mayor seguridad en la conexión con los servicios de pagos, los métodos actuales deben actualizarse a los nuevos estándares basados en algoritmos de firma más potentes.

Los comercios deben adecuar sus sistemas a las nuevas especificaciones para garantizar la continuidad del servicio de TPV-PC.

Es muy importante para el comercio actualizar su software de comunicación con TPV-PC lo antes posible de cara a garantizar la actividad y continuidad del negocio.

¿Cuál es la fecha límite para adaptar mi tienda?

Redsýs notificará a través de los medios habituales la fecha de inicio de migración. Se proporcionará toda la información necesaria para realizar los cambios, así como los datos de contacto y soporte. Desde la implantación del algoritmo SHA-256 existirá un periodo de convivencia de ambos algoritmos en el cual los comercios deberán realizar los cambios oportunos.

¿Qué tipos de comunicación con TPV-PC se ven afectadas?

Deben actualizarse todas las formas de comunicación desde el comercio a TPV-PC que utilizan SHA-1 en la firma. Igualmente, el comercio debe actualizar el procesamiento de las respuestas que informan del resultado de una operación desde TPV-PC al servidor del comercio.

¿Cómo activo el nuevo tipo de firma?

Para activar el nuevo tipo de firma no es necesaria ninguna configuración específica en TPV-PC. Puede empezar a enviar conexiones en cuanto haya comprobado que su implementación es correcta.

El nuevo tipo de firma se genera con la misma clave de comercio actual para SHA-1. Por favor, asegúrese de su valor accediendo (con el usuario que se les proporcionó cuando se dio de alta el comercio/terminal) a la web de canales '***Módulo de administración – Configuración – Consultar Clave de Comercio***'.