Cliente/Servicio – ***Client/Service*****:** **ES0040/S007**
Referencia - ***Reference*****:** **ES004000701475722**
Fecha de validez – ***Valid until*****:** **31/12/2023**

Proveedor de servicio / ***Service provider***

RedSys Servicios de Procesamiento, SL

Identificación del servicio calificado/
Rated Service identification

Pago móvil/
Mobile payment

Descripción del servicio calificado / ***Rated service description***

Pago móvil se encuentran disponibles los siguientes servicios:

- HCE (Host Card Emulation): Servicio que permite digitalizar una tarjeta mediante tokenización para realizar pagos EMV Contactless. El servicio se compone de dos partes principales: el componente host y el SDK móvil para el sistema operativo Android. Este servicio soporta los esquemas de Visa, MasterCard y Discover.
- X-PAY: REDSYS integra en una única conexión diferentes soluciones, reduciendo con ello la complejidad para las Entidades, permitiéndolas dar servicio a los titulares que quieren hacer uso de pago presencial con Smartphone NFC.
  X-Pay ofrece tres servicios principales, cada uno de ellos con diversas funcionalidades:
  - Hub de Emisión: Conjunto de interfaces que permite a las Entidades Financieras realizar gestiones para el mantenimiento de sus servicios en Redsys y la gestión del enrolamiento y del ciclo de vida de sus tokens para los pagos con móvil. El servicio actúa como intermediario entre la Entidad Financiera y los diferentes servicios de Redsys, facilitando el consumo de servicios de una forma mucho más sencilla.
  - Hub de Pago: Conjunto de interfaces que permite a las Entidades Financieras y a sus titulares la destokenización. Este servicio soporta los esquemas de Visa y MasterCard.
  - Hub Admin: Herramienta web que permite a los usuarios gestionar diversas configuraciones del Servicio, monitorizar el estado de las conexiones con las marcas o revisar la mensajería gestionada.

Mobile payment the following services are available:

- *HCE (Host Card Emulation): Service that allows digitizing a card through tokenization to make EMV Contactless payments. The service is made up of two main parts: the host component and the mobile SDK for the Android operating system. This service supports Visa, MasterCard and Discover schemes.*
- *X-PAY: REDSYS integrates different solutions into a single connection, thereby reducing the complexity for Entities, allowing them to provide service to holders who want to make face-to-face payments with NFC Smartphones.*
  X-Pay offers three main services, each with different functionalities:
  - *Issuance Hub: Set of interfaces that allows Financial Institutions to carry out procedures for the maintenance of their services in Redsys and the management of the enrollment and life cycle of their tokens for mobile payments. The service acts as an intermediary between the Financial Institution and the different Redsys services, facilitating the consumption of services in a much simpler way.*
  - *Payment Hub: Set of interfaces that allows Financial Institutions and their holders to detokenize. This service supports Visa and MasterCard schemes.*
  - *Hub Admin: Web tool that allows users to manage various Service configurations, monitor the status of connections with brands or review managed messaging.*

Cliente/Servicio – *Client/Service*: **ES0040/S007**
Referencia - *Reference*: **ES004000701475722**
Fecha de validez – *Valid until*: **31/12/2023**

Alcance / *Scope*

HCE: se comunica directamente con el SDK HCE y con el host del emisor para el aprovisionamiento, la gestión de cuentas, la gestión del ciclo de vida y el procesamiento posterior al pago.

- SDK HCE: Incluye el software de pagos, el cual los emisores pueden integrar fácilmente en sus aplicaciones.
- Gestión de perfiles EMV: Proporciona preparación de datos EMV, incluyendo generación de claves de uso limitado y personalización ODA (Offline Data Authentication)
- Proveedor de servidor de Tokenización

HUB XPAY es un sistema interlocutor entre entidades y Tokenizadores (gestión, generación/digitalización y pan mapping en pagos tokenizados).

El servicio HCE emplea servidores con sistema operativo AIX en entorno de producción y el servicio X-PAY emplea servidores virtuales con sistema operativo AIX en el entorno de producción.

HCE: Communicates directly with the HCE SDK and the issuer host for provisioning, account management, lifecycle management, and post-payment processing.

- *HCE SDK: Includes payment software, which issuers can easily integrate into their applications.*
- *EMV Profile Management: Provides EMV data preparation, including limited-use key generation and ODA (Offline Data Authentication) personalization.*
- *Tokenization server provider*

HUB XPAY is an interlocutor system between entities and Tokenizers (management, generation/digitization and pan mapping in tokenized payments).

The HCE service uses servers with AIX operating system in production environment and the X-PAY service uses virtual servers with AIX operating system in production environment.

Proceso de calificación

El proceso de calificación consta de cuatro etapas:

- Elaboración de la memoria justificativa por parte del proveedor del servicio o realización de auditoría de tercero independiente conforme a la norma internacional ISAE 3402
- Pre-evaluación documental de la memoria justificativa (o del informe de auditoría) y solicitud, en caso de que sea necesario, de subsanación de errores y/o aclaraciones
- Evaluación *in situ* de una muestra de controles incluidos en la memoria justificativa (solo en caso de que no se haya realizado auditoría previa)
- Elaboración de informe final y emisión del sello con la calificación obtenida

Una vez obtenido el sello, se ponen en funcionamiento los mecanismos de supervisión del esquema:

- Canal de incidencias
- Monitorización en fuentes abiertas
- Auditorías aleatorias

Este nivel de calificación se obtiene sobre la base de las respuestas indicadas por el proveedor de servicios en cuanto a la aplicabilidad y, en su caso, existencia de los controles incluidos en la metodología de calificación en su versión 3.1 y las evidencias aportadas por el mismo u obtenidas por el equipo de la agencia durante la revisión *in situ* en las instalaciones del proveedor del servicio.

Rating proces

Cliente/Servicio – ***Client/Service*****:** **ES0040/S007**
Referencia - ***Reference*****:** **ES004000701475722**
Fecha de validez – ***Valid until*****:** **31/12/2023**

Rating and certification process have four steps:

- *Preparation of a memory by the service provider or conducting an audit by an independent third party according to ISAE 3402.*
- *Documentary pre-assessment based on previous memory (or audit report) and require, if needed, correction or errors and/or clarifications.*
- *In situ assessment based on a sample of controls included in the memory.*
- *Preparation of final report and issue of the label and certification with the rating level obtained.*

Once the label has been issued, supervision mechanisms come into place:

- *Incident channel*
- *Cybersecurity online monitoring*
- *Random exhaustive audits*

This report corresponds to the third step of the rating process and it shapes the final assessment of service rating, based on the answers that the service provider has included in the memory about applicability and implementation of controls included in rating methodology version 3.1 and evidences provided by the provider or obtained by the agency team during the onsite visit in service provider facilities.

Calificación

El nivel de calificación obtenido por el servicio una vez realizado el proceso de calificación mencionado y su evolución respecto a años anteriores se muestran en los gráficos siguientes:

Rating

The rating level obtained by the service and the comparison with previous years according to the qualification level after the aforementioned rating process has been carried out are the following:

Confidencialidad *Confidentiality*	**Integridad** *Integrity*	**Disponibilidad** *Availability*
A+ **--A--** B C D	A+ **--A--** B C D	A+ **--A--** B C D

Los criterios para asignar la calificación global, según se establece en la versión 3 de la metodología son, implantar:

- El 100% de las medidas generales y para la dimensión correspondiente de prioridad '1'.
- Al menos, el 85% de las medidas generales y para la dimensión correspondiente de prioridad '2'.
- Al menos, el 50% de las medidas generales y para la dimensión correspondiente de prioridad '3'.

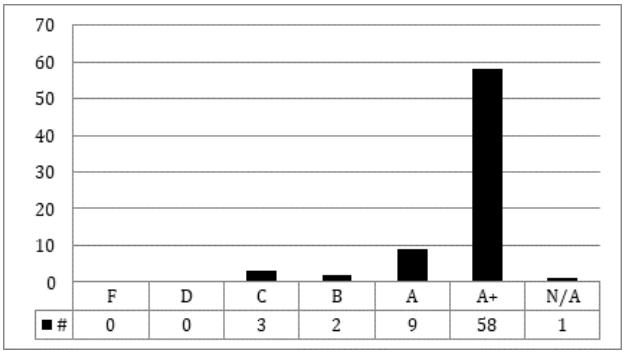
La evaluación de las secciones individuales que se resumen en el gráfico adjunto considera el 100% de los controles (con independencia de su prioridad). La calificación cuantitativa es una suma ponderada (base mil) de los niveles en los que han sido evaluadas las secciones (con más peso de aquellas que más contribuyen a una seguridad más ágil).

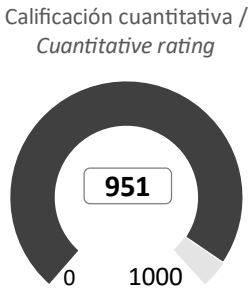
The criteria for assigning the global rating, as established in version 3 of the methodology are:

- *100% of the general measures and for the corresponding dimension of priority '1'.*
- *At least 85% of the general measures and for the corresponding dimension of priority '2'.*
- *At least 50% of the general measures and for the corresponding dimension of priority '3'.*

Cliente/Servicio – *Client/Service*: **ES0040/S007**
Referencia - *Reference*: **ES004000701475722**
Fecha de validez – *Valid until*: **31/12/2023**

The evaluation of individual sections considers 100% of the controls (regardless of their priority) and it is showed in the following diagram. Quantitative rating is a weighted sum (base thousand) of levels achieved by sections (with a higher weight of those with a closer relation to agile security).





Madrid, 12 de mayo de 2023/ *May 12th, 2023*

Firmado digitalmente por LOPEZ CASADO, PATRICIA (FIRMA)
Fecha: 2023.05.19 11:06:23 +02'00'

D. Patricia López Casado
Rating Evaluation Team – Operations Direction

Certifico la precisión e integridad de este documento

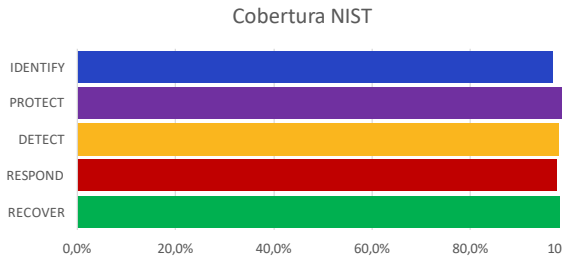
Cliente/Servicio – ***Client/Service*****:** **ES0040/S007**
Referencia - ***Reference*****:** **ES004000701475722**
Fecha de validez – ***Valid until*****:** **31/12/2023**

ANEXO / *ANNEX*

COBERTURA RESPECTO A ESTÁNDARES INTERNACIONALES
INTERNATIONAL STANDARDS COVERAGE

Cobertura respecto a NIST

Este gráfico muestra el porcentaje de implementación de las prácticas aplicables en el servicio, para el nivel objetivo evaluado (barra decolorada) y con respecto al nivel máximo (barra de color intenso), por cada una de las cinco etapas del marco de ciberseguridad del National Institute of Standards and Technology (NIST)[1].



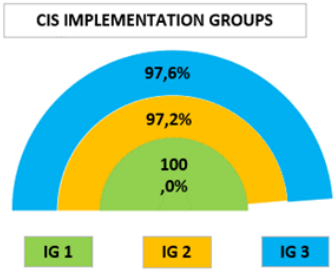
NIST coverage

This chart shows the implementation porcentaje of practices aplicable in the service, for the goal level reviewed (discolored bar) and for the máximum level (intense bar) in each of the five steps of NIST Cybersecuerity Framework.

Cobertura respecto a CIS

El Center for Internet Security (CIS) recoge y publica las prácticas de defensa frente a los ataques más comunes, conocidas como CIS Controls.

Los 20 controles de su versión 7[2] están divididos en tres grupos: *Basic, Foundational y Organizational*, que a su vez de se clasifican en tres grupos de implementación: IG 1, IG 2 e IG 3, según el nivel de exigencia en seguridad que se marque la propia organización. El siguiente diagrama muestra su grado de implementación en el servicio evaluado.



CIS coverage

Center for Internet Security (CIS) collects and publishes the defense practices for most common attacks, known as CIS Controls.

The 20 controls of versión 7 are divided in three groups: Basic, Foundational and Organizational, that are also classified in three implementaton groups: IG1, IG2 and IG3 in growing order of demand. Following chart shows the implementation grade in the service in scope.

[1] https://www.nist.gov/cyberframework

[2] https://www.cisecurity.org/controls/v7

Cliente/Servicio – ***Client/Service*****:** **ES0040/S007**
Referencia - ***Reference*****:** **ES004000701475722**
Fecha de validez – ***Valid until*****:** **31/12/2023**

INFORMACIÓN ANALÍTICA DE SU EVALUACIÓN
ANALYTIC INFORMATION OF YOUR RATING

Resultado por áreas

Los controles han sido clasificados según los principios de *security economics* lo que permite obtener los gráficos siguientes con el porcentaje de implementados por cada tipo respecto al nivel evaluado como objetivo.

Results by areas

Controls have been classified according to security economics principles which allows getting the attached diagram showing the percentage of practices implemented in relation to those required by your goal level.