Nivel de garantía
Level of assurance

Fully audited

Certified in EU

Resumen ejecutivo de calificación / *Rating executive summary*

Cliente/Servicio – *Client/Service*: **ES0040/S008**
Referencia - *Reference*: **ES004000801548876**
Fecha de validez – *Valid until*: **31/12/2025**

Proveedor de servicio / *Service provider*

RedSys Servicios de Procesamiento SL

Identificación del servicio calificado/ *Rated Service identification*

Servicios de Autenticación/
Authentication Services

Descripción del servicio calificado / *Rated service description*

El servicio de autenticación que implementa el componente ACS de EMV 3DSecure, es una solución de seguridad certificada por EMVCo, que se utiliza para verificar la identidad del titular de la tarjeta en transacciones de comercio electrónico y garantiza la seguridad de los pagos.
Opera como intermediario entre el emisor, el titular de la tarjeta y la red de la marca (Visa Secure, Mastercard Id Check...), validando la identidad del usuario a través de diversos factores (como biometría, OTP, etc.).
Realiza comunicación con los emisores para la autenticación del titular en banca móvil. Adicionalmente, permite autenticación sin fricción basadas en riesgo (denominada frictionless o exención), además de soportar entornos móviles y aplicaciones nativas.

The authentication service implemented by the ACS component of EMV 3DSecure, is a security solution certified by EMVCo, which is used to verify the identity of the cardholder in e-commerce transactions and ensures the security of payments.
It operates as an intermediary between the issuer, the cardholder and the brand's network (Visa Secure, Mastercard Id Check...), validating the user's identity through various factors (such as biometrics, OTP, etc.).
It communicates with issuers for cardholder authentication in mobile banking. Additionally, it allows frictionless authentication based on risk (called frictionless or exemption), in addition to supporting mobile environments and native applications.

Alcance / *Scope*

Recibe las peticiones de solicitud de autenticación desde el entorno del comercio a través del componente de EMV 3DSecure denominado Directory Server.
Evalúa el riesgo de la transacción mediante Lynx analizando datos de la misma: información del titular, ubicación, dispositivo, entre otras.
Autenticación del titular de la tarjeta con posibilidad de autenticación basada en riesgo (frictionless) o desafío (challenge).
Realiza comunicaciones con los distintos emisores a través del hub de emisión con el objetivo de realizar la autenticación en la banca móvil del titular de la tarjeta (OoB)
Capacidades de autenticación en respaldo si existiesen problemas de comunicación con el emisor utilizando métodos de autenticación basados en OTP siempre que se disponga del teléfono del titular de la tarjeta
Exenciones aplicables TRA y LV:

- Exenciones por Análisis de riesgo de la transacción (TRA):
  - Puede ser solicitada por el comercio o el emisor
  - Puede aceptar la exención si el nivel de riesgo percibido es bajo, evaluando mediante Lynx.
- Exenciones por bajo valor (LV)
  - Se aplica a operaciones inferiores o iguales a 30 euros y puede ser gestionada directamente por el ACS sin requerir autenticación reforzada siempre que no se hayan superado un determinado número de transacciones consecutivas exentas o el total acumulado de transacciones exentas no supere una cantidad determinada en euros.

Receives authentication request requests from the merchant environment through the 3DSecure EMV component called Directory Server.
Assesses transaction risk through Lynx by analyzing transaction data: cardholder information, location, device, among others.

Cardholder authentication with the possibility of risk-based authentication (frictionless) or challenge-based authentication (challenge).
Communications with the different issuers through the issuing hub in order to perform cardholder authentication in mobile banking (OoB).
Back-up authentication capabilities in case of communication problems with the issuer using OTP-based authentication methods as long as the cardholder's phone is available.
Applicable TRA and LV exemptions:

- *Transaction Risk Analysis (TRA) Exemptions:*
  - *May be requested by the merchant or issuer.*
  - *Can accept the exemption if the perceived level of risk is low, assessed by Lynx.*
- *Low Value (LV) Exemptions*
  - *Applies to transactions less than or equal to €30 and can be handled directly by ACS without requiring enhanced authentication provided that a certain number of consecutive exempt transactions have not been exceeded or the cumulative total of exempt transactions does not exceed a certain amount in euros.*

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 process

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

Cliente/Servicio – *Client/Service*: **ES0040/S008**
Referencia - *Reference*: **ES004000801548876**
Fecha de validez – *Valid until*: **31/12/2025**

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:

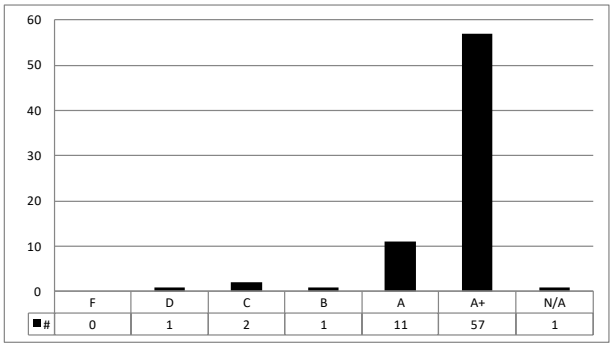
- El 100% de las medidas generales y para la dimensión correspondiente de prioridad '1'.
- Al menos, el 85% de las medidas generales y para la dimensión correspondiente de prioridad '2'.
- Al menos, el 50% de las medidas generales y para la dimensión correspondiente de prioridad '3'.

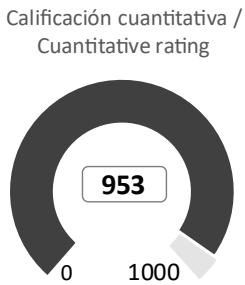
La evaluación de las secciones individuales que se resumen en el gráfico adjunto considera el 100% de los controles (con independencia de su prioridad). La calificación cuantitativa es una suma ponderada (base mil) de los niveles en los que han sido evaluadas las secciones (con más peso de aquellas que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

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).





Cliente/Servicio – *Client/Service*: **ES0040/S008**
Referencia - *Reference*: **ES004000801548876**
Fecha de validez – *Valid until*: **31/12/2025**

Madrid, 14 de mayo de 2025/ *May 14th, 2025*

D. Patricia López Casado
Rating Evaluation Team – Operations Direction

Cliente/Servicio – ***Client/Service*****:** **ES0040/S008**
Referencia - ***Reference*****:** **ES004000801548876**
Fecha de validez – ***Valid until*****:** **31/12/2025**

ANEXO / *ANNEX*

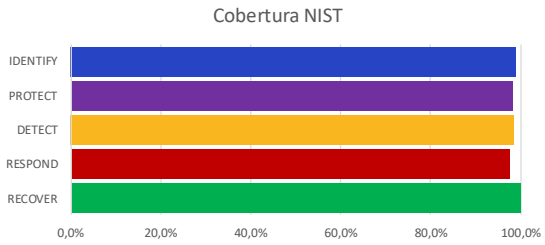
COBERTURA RESPECTO A ESTÁNDARES INTERNACIONALES
INTERNATIONAL STANDARDS COVERAGE

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

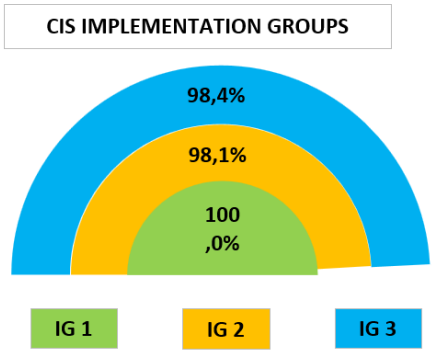
El Center for Internet Security (CIS) recoge y publica las prácticas de defensa frente a los ataques más comunes, conocidas como CIS Controls.

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/S008**
Referencia - ***Reference*****:** **ES004000801548876**
Fecha de validez – ***Valid until*****:** **31/12/2025**

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.