



Términos y Condiciones Particulares para 3D Secure para operaciones de pago *online* con tarjeta

Los siguientes Términos y Condiciones Particulares regularán el uso de 3D Secure para operaciones de pago online realizadas con una tarjeta de pago emitida por Solarisbank AG (el “**Banco**”):

1. Objeto, definiciones

1.1 El Banco permite al titular de una tarjeta de pago emitida y aprobada por el Banco para la realización de operaciones online (la “**Tarjeta**”) y beneficiarse del proceso 3D Secure¹ habilitado por comerciantes (*merchants*) con el objeto de proteger operaciones de pago online realizadas con Tarjeta.

1.2 3D Secure (el denominado “Mastercard Identity Check” en el entorno Mastercard, y “VISA Secure” en el entorno Visa) es un estándar de autenticación de pago para las compras por internet con Tarjeta.

1.3 Para autorizar las operaciones online con la Tarjeta, el titular de la misma debe utilizar determinados elementos de autenticación (véanse las cláusulas 4.1 y 7.1 de las Términos y Condiciones de banca online).

1.4 Los elementos de autenticación incluyen un número de autenticación de transacción móvil (*mobile transaction authentication number*, en lo sucesivo, “**TAN móvil**”). El Banco envía un TANmóvil al dispositivo móvil del titular de la Tarjeta a través de un SMS (servicio de mensajes cortos); una autenticación dentro de la aplicación, en la que los titulares de la Tarjeta son redirigidos a la aplicación bancaria de los socios colaboradores del Banco (“**autenticación dentro de la aplicación**”); o preguntas de seguridad que solo el titular de la Tarjeta puede responder.

1.5 El Banco podrá rechazar una operación online con Tarjeta si el titular de la de la misma quiere realizar una operación sin utilizar 3D Secure en un comercio electrónico participante.

2. Requisitos previos de su uso

2.1 Cada titular de una Tarjeta válida y no bloqueada participa automáticamente en el procedimiento 3D Secure. La inscripción para la utilización de este procedimiento tiene lugar de forma automática cuando la Tarjeta se activa. No se requiere por tanto ningún tipo de

inscripción independiente. Para utilizar 3D Secure, el titular de la Tarjeta necesita su número de móvil registrado por el Banco.

2.2 Para realizar una autenticación mediante 3D Secure a través de un TAN móvil, el titular de la Tarjeta debe proporcionar un número móvil al Banco a través de uno de sus socios colaboradores. El número podrá cambiarse en cualquier momento.

2.3 Para llevar a cabo una autenticación mediante 3D Secure a través de la autenticación en la aplicación, el titular de la Tarjeta debe haber vinculado correctamente el dispositivo móvil a la cuenta asociada a la Tarjeta.

3. Autenticación a través de 3D Secure

3.1 El TAN móvil transmitido por SMS estará compuesto al menos de seis dígitos y deberá introducirse para autenticar la operación online con Tarjeta. En lo que respecta a sincronización de los datos, el titular de la Tarjeta visualizará los últimos dígitos del número de móvil proporcionado al Banco en la pantalla.

3.2 El Banco enviará el SMS gratuita.

3.3 Para la autenticación dentro de la aplicación, el titular de la Tarjeta tiene que iniciar sesión en la aplicación bancaria del socio colaborador del Banco, a la que se dirige al titular de la Tarjeta, y confirmar la operación en línea con la Tarjeta.

3.4. Para autenticarse mediante la respuesta a una pregunta de seguridad, el titular de la Tarjeta debe responder correctamente a una pregunta que solo él conoce.

4. Obligaciones de diligencia del titular de la Tarjeta

4.1 El titular de la Tarjeta se asegurará de que ningún tercero acceda a su dispositivo móvil para la ejecución de operaciones *online*. El Banco no pedirá al titular de la Tarjeta que se inscriba o proporcione sus datos de inscripción, ni por correo electrónico, ni por teléfono.

¹ 3D Secure es una característica de seguridad adicional y no pretende sustituir las obligaciones de seguridad que el cliente debe cumplir según lo establecido en las Condiciones Generales del Banco y otros términos y condiciones aplicables en cada momento.



4.2 El titular de la Tarjeta debe tomar los pasos necesarios para mantener la seguridad de los SMS, por ejemplo, protegiendo el acceso al teléfono con una contraseña. El Banco no será responsable cuando, en caso de pérdida, robo o transmisión del dispositivo móvil, terceros obtengan acceso no autorizado al contenido del SMS y lo utilicen..

4.3 El titular de la Tarjeta debe verificar los datos transmitidos por SMS (véase la cláusula 3.2). En caso de que los datos sean incorrectos, el titular de la Tarjeta deberá cancelar la operación e informar al Banco sin demora.

5. Tratamiento de datos y proveedores de servicios

5.1 Cuando se utiliza 3D Secure, se almacenará el número de Tarjeta, la fecha y la hora de la operación, el importe de la operación, la información del comerciante (*merchant*) (nombre, ID, URL) y la dirección IP desde la que se inició la operación de pago con Tarjeta.

5.2 El Banco podrá encargar a proveedores de servicios que lleven a cabo el procedimiento 3D Secure. El Banco proporciona a estos proveedores de servicio datos personales del titular de la Tarjeta (por ejemplo, número de Tarjeta de crédito) exclusivamente dentro del alcance del objeto de la relación contractual.

5.3. Para un mayor detalle respecto del procesamiento de sus datos personales por favor remítase al documento "*Información para el cliente sobre el tratamiento de datos*".