Entersekt

Transakt:
PSD2 SCA compliance report

After rigorous evaluation, Entersekt's Transakt product has been declared to be a **state-of-the-art compliant solution for PSD2 SCA** by Security Research & Consulting GmbH. This report summarizes how Transakt meets the European Banking Authority's regulatory technical standards on strong customer authentication and common and secure open standards of communication.

How Transakt meets the RTS requirements

REFERENCE	REQUIREMENT	COMPLIANCE
Article 4.1	"[A]uthentication shall be based on two or more elements which are categorized as knowledge, possession and inherence and shall result in the generation of an authentication code"	The authentication codes used by Transakt in the form of cryptographic signatures are based on the elements of possession and knowledge and/or inherence.
Article 4.2 (a)	"[N]o information on any of the elements [should be able to] be derived from the disclosure of the authentication code"	No authentication code (digital signature) generated by Transakt contains information about any of the authentication elements.
Article 4.2 (b)	"[I]t [should] not [be] possible to generate a new authentication code based on the knowledge of any other authentication code previously generated"	No authentication code (digital signature) generated by Transakt can be reused or used to create a signature that is valid for any future transactions and/or authentications.
Article 4.2 (c)	"[T]he authentication code [should not be able to] be forged"	The industry-standard PKI principles that Transakt uses to create digital signatures make it unfeasible for these signatures to be forged.
Article 4.3 (a)	"[In the case of failure] to generate an authentication code […] it shall not be possible to identify which of the elements […] was incorrect"	The information on those authentication elements that failed is not passed on to the user by Transakt.
Article 4.3 (c)	"[C]ommunication sessions [must be] protected against the capture of authentication data transmitted during the authentication and against manipulation by unauthorized parties"	Transakt's authentication and authorization data is always transmitted via a dedicated encrypted channel.

REFERENCE	REQUIREMENT	COMPLIANCE
Article 5.1 (b)	"[T] the authentication code generated [must be] specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction"	The authentication code (digital signature or OTP) generated by Transakt includes the payment amount.
Article 5.1 (d)	"[A]ny change to the amount or the payee [should] result in the invalidation of the authentication code generated"	Any change in the payment amount or payment recipient will invalidate the authentication code (digital signature or OTP) generated by Transakt.
Article 5.2 (a)	"[T]he amount of the transaction and the payee [should be displayed] throughout all of the phases of the authentication"	Digital signatures and OTPs generated by Transakt ensure the visibility, authenticity, and integrity of the amount and the payee at all times.
Article 6.1	"PSPs shall adopt measures to mitigate the risk that the elements of strong customer authentication categorized as knowledge are uncovered by, or disclosed to, unauthorized parties"	Transakt transmits the PIN (knowledge element) in encrypted form only. The PIN is only valid in conjunction with the authorized possession factor, e.g. the registered mobile device.
Article 7.1	"PSPs shall adopt measures to mitigate the risk that the elements of strong customer authentication categorized as possession are used by unauthorized parties"	The possession element comprises the registered user's mobile device, on which an individual instance of Transakt is installed. In the case of loss or theft of the mobile device, Transakt can temporarily deactivate that instance and make it unusable.
Article 7.2	"[T]hose] elements shall be subject to measures designed to prevent replication"	Transakt implements device binding, which prevents the unauthorized duplication of an instance and its use on an unauthorized device.
Article 9.1	"PSPs shall ensure that […] the breach of one of the elements does not compromise the reliability of the other elements"	Were Transakt's possession element to be compromised, the attacker would in no way be able to access the knowledge element, and vice versa. When an inherence (biometric) element is compromised, this affects neither the knowledge of the PIN nor the possession of the mobile device.
Article 9.3 (a)	"[M]itigating measures shall include […] the use of separate secure execution environments through the software installed inside the device"	Transakt's authentication and authorization procedures are dependent on the secure vault stored exclusively on the user's mobile device. The secure execution environment for each Transakt instance is provided through device binding. The secure execution environment for verifying the user's fingerprint is provided by the manufacturer of the mobile device.
Article 14.1	"PSPs shall apply strong customer authentication when a payer creates, amends, or initiates […] a series of recurring transactions with the same amount and […] payee"	Transakt can be used for creating, amending, or initiating recurring transactions in the same manner as for non-recurring ones.

REFERENCE	REQUIREMENT	COMPLIANCE
Article 18.2 (c)	"A […] transaction […] shall be considered as posing a low level of risk where […] a real-time risk analysis ha[s] not identified unusual information about the payer's device [or an] abnormal location of the payer"	Transakt detects unusual geographic locations and circumstances of operation, like rooting or jailbreaking.
Article 22.2 (b)	"PSPs shall ensure that […] personalized security credentials [and] cryptographic materials […] are not stored in plain text"	Transakt never stores personalized security credentials or cryptographic material in plain text.
Article 22.3	"PSPs shall fully document the […] management of cryptographic material"	Cryptographic material used by the Transakt is kept inside the system at all times, and therefore does not need to be managed separately.
Article 26	"[R]enewal or re-activation of personalized security credentials [must] adhere to the procedures for the creation, association and delivery of the credentials"	The reactivation of Transakt is identical to the first activation.
Article 27 (a)	"PSPs shall ensure that they have effective processes in place [for] the secure destruction, deactivation or revocation of the personalized security credentials"	An individual Transakt instance and the associated personalized security credentials are revoked by unlinking the mobile device from the user's identity. The security credentials then become devoid of any functionality.

The verdict

Entersekt's Transakt version 18.1 for iOS and Android fulfils all requirements of the EBA RTS which are in scope for the product. Transakt can be considered a state-of-the-art solution, since it makes use of widely accepted industry best practices in its design and use of technology, especially in cryptographically securing and authenticating credentials and client-server communication.

About Security Research & Consulting (SRC) GmbH

SRC is a consultancy serving the banking industry in Germany. The firm uses its up-to-date knowledge of IT security and information technology to help its customers develop and implement secure systems.