Entersekt

PSD2
Strong Customer Authentication Checklist

Entersekt offers PSD2-compliant, one-touch multi-factor authentication and digital signing solutions to banks and other participants in Europe's new digital economy. This checklist – based on the EBA's regulatory technical standards on strong customer authentication – explains how we do it.

From the RTS

CHAPTER 2 - SECURITY MEASURES FOR THE APPLICATION OF STRONG CUSTOMER AUTHENTICATION

Article 4: Paragraphs 1, 2(a), 2(b), and 2(c)

Authentication Code

1 Where payment service providers apply strong customer authentication in accordance with Article 97(1) of Directive (EU) 2015/2366, the authentication 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 code shall be only accepted once by the payment service provider when the payer uses the authentication code to access its payment account online, to initiate an electronic payment transaction or to carry out any action through a remote channel which may imply a risk of payment fraud or other abuses.

2 For the purpose of paragraph 1, payment service providers shall adopt security measures ensuring that each of the following requirements is met:

(a) no information on any of the elements referred to in paragraph 1 can be derived from the disclosure of the authentication code;

(b) it is not possible to generate a new authentication code based on the knowledge of any other authentication code previously generated;

(c) the authentication code cannot be forged

IN SIMPLIFIED TERMS

Your organization (the "payment service provider") must implement strong customer authentication (SCA) to comply with the RTS. This means that your customers will verify their transactions using at least two of the following three factors of authentication: knowledge (something they know), possession (something they have), and inherence (something they are).

Entersekt's response

MULTI-FACTOR AUTHENTICATION

1 Entersekt's Transakt product provides a state-of-the-art, patented means of securing the customer's mobile phone, and converting it into a unique and trusted possession factor, (something the user has). Transakt uses mutual certificate validation in order to establish an end-to-end encrypted channel between the customer's mobile phone and the payment service provider. This trusted channel enables the customer to securely capture any knowledge-based factors (things the user knows) on their mobile, and securely transmit these to the payment service provider. Finally, Transakt can also integrate with the biometric capabilities provided by the mobile device or supported by a third-party biometrics library, thereby enabling an inherence factor (something the user is) to be securely captured and transmitted to the service provider via the trusted channel.

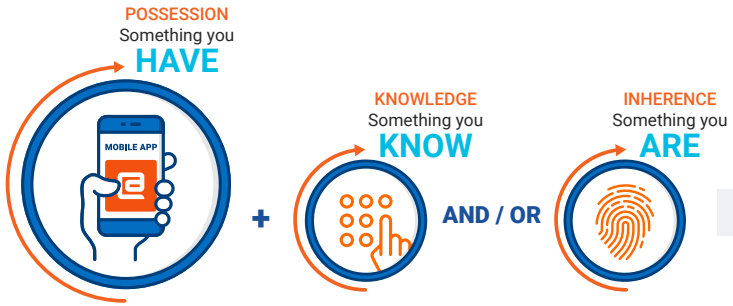
Transakt uses the transaction details to create a digital signature that is unique for each transaction and is used as a one-time authentication code. The digital signature is packaged together with multi-factor context, such as a knowledge factor or inherence factor, in order to link the customer to the signed transaction.

2 (a) Transakt generates a digital signature from the transaction details, which serves as the unique one-time authentication code. The digital signature does not include any information on any of the authentication factors referred to above.

(b) Transakt uses PKI infrastructure to digitally sign each transaction and/or authentication request, which results in a unique signature every time. This ensures that the request cannot be reused or used to create a signature that is valid for any future transactions and/or authentications.

(c) Transakt uses industry-standard PKI principles to create digital signatures, which means it is not feasible for these signatures to be forged. The fact that each authentication request and its response are digitally signed also supports non repudiation, and provides legally binding, signed proof of a customer's consent to proceed with the transaction.

Strong customer authentication must be based on two or more of the following three factors of authentication:



From the RTS

CHAPTER 2 - SECURITY MEASURES FOR THE APPLICATION OF STRONG CUSTOMER AUTHENTICATION

Article 7: Paragraphs 1 and 2

Requirements of the Elements Categorized as Possession

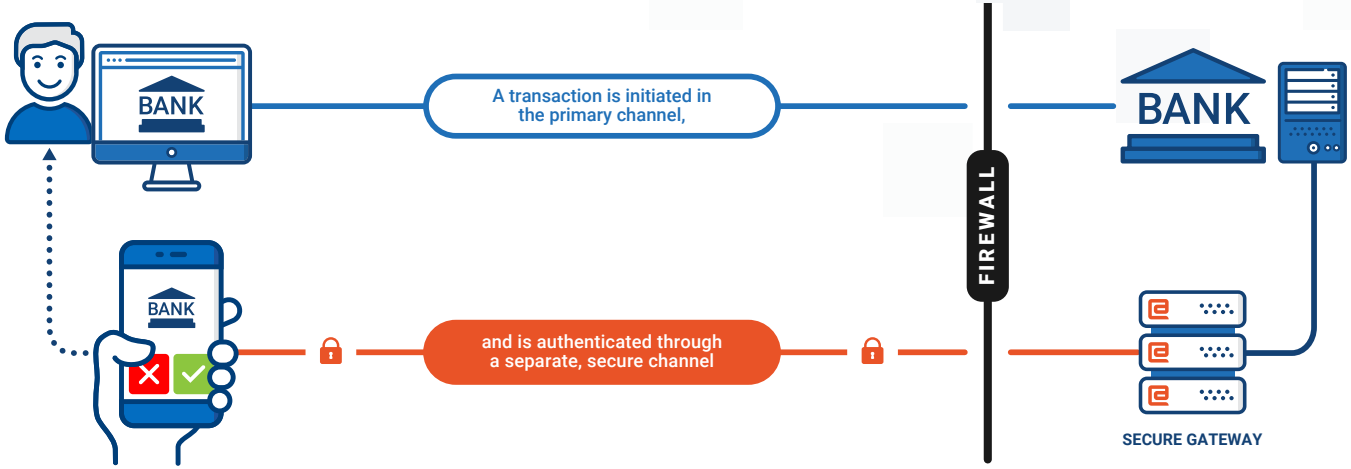
1 Payment service providers shall adopt measures to mitigate the risk that the elements of strong customer authentication categorized as possession are used by unauthorized parties.

2 The use by the payer of those elements shall be subject to measures designed to prevent replication of the elements.

IN SIMPLIFIED TERMS

One factor that can be used in strong customer authentication is possession, i.e. something the user has. This can be a hardware token, but it can also be the user's mobile device. If you use the mobile device, then you (the "payment service provider") need to ensure that your app on the user's mobile device is not vulnerable to attacks aimed at forging or co-opting the possession factor, and that the communication between your service and the user's mobile device is impervious to cyber-attacks.

Entersekt's out-of-band authentication model

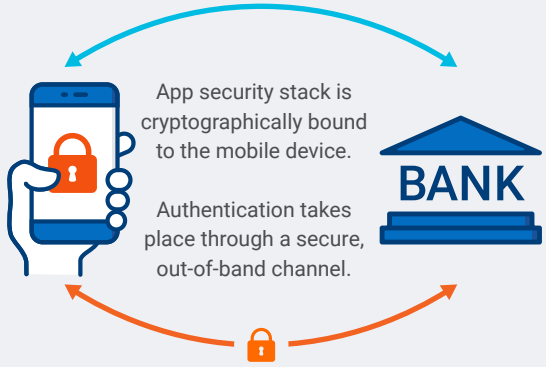


Entersekt's response

PROTECTING THE MOBILE DEVICE

1 Transakt secures the connection between the user's mobile device and the payment service provider on multiple levels. This includes securing the underlying connections using mutual TLS, employing the latest cypher suites, digitally signing authentication requests and responses with a shared PKI infrastructure, implementing certificate pinning to eliminate man-in-the-middle attacks, and storing the key material securely, ensuring that neither the user nor the application developer ever has access to it.

2 Transakt implements a state-of-the-art app security stack that cryptographically binds to the mobile device, creating a strong, unique device ID that attests to the integrity of that device. Transakt further ensures that this device ID cannot be copied, or re-created on another device. This means that Transakt turns the mobile device into a strong possession factor. Transakt also provides the ability to combine the mobile device (possession factor) with a knowledge factor or inherence factor to ensure that only the legitimate user can authorize transactions on that device.



- Secured using mutual TLS
- Employing the latest cypher suite
- Digitally signed authentications with a shared PKI
- Certificate pinning to eliminate man-in-the-middle attacks
- Key material stored securely

From the RTS

CHAPTER 4 - CONFIDENTIALITY AND INTEGRITY OF THE PAYMENT SERVICE USERS' PERSONALIZED SECURITY CREDENTIALS

Article 21: Paragraphs 1, 2(a), 2(b)

Association with the Payment Service User

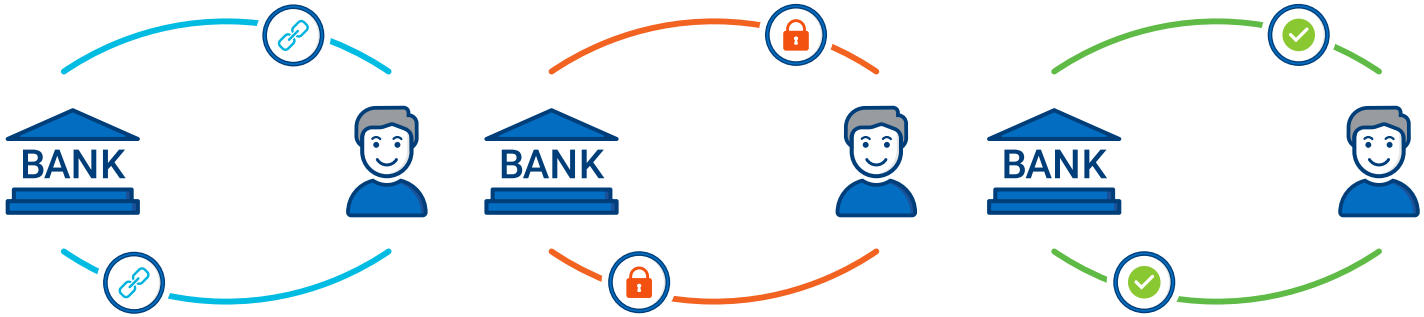
1 Payment service providers shall ensure that only the payment service user is associated, in a secure manner, with the personalized security credentials, the authentication devices and the software.

2 For the purpose of paragraph 1, payment service providers shall ensure that each of the following requirements is met:

(a) the association of the payment service user's identity with personalized security credentials, authentication devices and software is carried out in secure environments under the payment service provider's responsibility comprising at least the payment service provider's premises, the internet environment provided by the payment service provider or other similar secure websites used by the payment service provider and its automated teller machine services, and taking into account risks associated with devices and underlying components used during the association process that are not under the responsibility of the payment service provider;

(b) the association by means of a remote channel of the payment service user's identity with the personalized security credentials and with authentication devices or software is performed using strong customer authentication.

The three elements of customer engagement



LINK TO THE CUSTOMER
Connect with the customer for the first time

SECURE THE LINK
Secure the link between you and your customer

VERIFY COMMUNICATION
Verify that the customer receives the message and verify their response

IN SIMPLIFIED TERMS

You (the "payment service provider") must create a secure digital link between each user and the information ("security credentials") that they use to authenticate themselves, i.e. their password, PIN, hardware and/or software tokens. This process of enrollment or on-boarding, must take place securely on your premises, at one of your ATMs, or on your website or app, and must make use of strong customer authentication principles.

A secure digital link between each user and the information

Entersekt's response

SECURE ONBOARDING

1 Entersekt's Transakt product generates a unique digital certificate, signed by a certificate authority, for each user's mobile device. This certificate is then linked to that specific user. Each certificate can only be linked to a single user.

2 (a) Transakt provides a pseudonymous certificate to each mobile application instance, which creates a unique link between the service provider and that specific mobile device. During customer registration (onboarding), this certificate (and by extension the mobile device) is linked to the device owner.
If the device is stolen or lost, or that user gets a new device, the provider simply breaks the link between the certificate and the user, rendering the application instance unusable.

(b) Transakt enables the end-to-end encrypted transfer of knowledge-based authentication factors between the user and the initiating institution. The possession factor is represented by the mobile device itself.

From the RTS

CHAPTER 2 - SECURITY MEASURES FOR THE APPLICATION OF STRONG CUSTOMER AUTHENTICATION

Article 5: Paragraphs 1(a), 1(b), 1(c), 1(d) and 2(a)

Dynamic Linking

1 Where payment service providers apply strong customer authentication in accordance with Article 97(2) of Directive (EU) 2015/2366, in addition to the requirements of Article 4 of this Regulation, they shall also adopt security measures that meet each of the following requirements:

(a) the payer is made aware of the amount of the payment transaction and of the payee;

(b) the authentication code generated is specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction;

(c) the authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to the identity of the payee agreed to by the payer;

(d) any change to the amount or the payee results in the invalidation of the authentication code generated.

2 For the purpose of paragraph 1, payment service providers shall adopt security measures which ensure the confidentiality, authenticity and integrity of each of the following:

(a) the amount of the transaction and the payee throughout all of the phases of the authentication;

IN SIMPLIFIED TERMS

Any time a user makes a payment using your service, they (the "payer") must be informed of the amount they are about to pay and to whom (the "payee"). Only the user should be able to see this information. This information must be linked to the authentication code the user is issued, and it must be impossible to change this information without voiding the payment.

Entersekt's response

PROTECTING THE MOBILE DEVICE

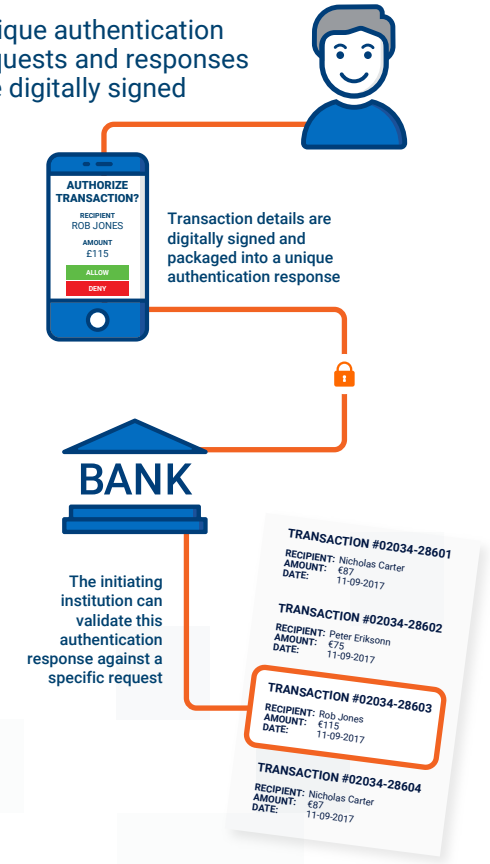
1 (a) Entersekt's solution allows the initiating institution to specify the content of an authentication message, as well as the values of the requested user responses via a well defined API. All of the specified values, as well as the user's response, are digitally signed and packaged into a single authentication response.

b) Entersekt's solution ensures that every authentication request is unique. Any alteration of the content of the message or response, including a change in time sent, will result in the signed authentication failing validation.

(c) The Transakt authentication message contains an initial code reference, allowing the initiating institution to validate it against a specific request.

(d) See 1(b) above.

2 (a) See 1(a) above.



Discover more

Entersekt is an innovator of mobile-first fintech solutions. Financial services providers and other enterprises rely on its patented mobile identity system to provide both security and the best in convenient new digital experiences to their customers, irrespective of the service channel.

Whether pursuing compliance through strong authentication and state-of-the-art app security or looking to meet consumer demand for on-the-go information sharing and payment capabilities, Entersekt's clients always enjoy a competitive advantage.

For more information visit entersekt.com or email info@entersekt.com.

AFRICA

CAPE TOWN
+27 21 815 2800

JOHANNESBURG
+27 11 568 7000

MAURITIUS
+230 403 0800

EUROPE

UTRECHT
+31 20 505 0200

MUNICH
+49 173 342 8240

UNITED KINGDOM
+44 2033 193 058

NORTH AMERICA

ATLANTA
+1 404 698 1001