Wirecard CEE Integration Documentation

() -

Created: 2019-09-22 18:43

Securing your Online Shop

Please take the following security issues into consideration before starting the integration of Wirecard Checkout products into your online shop.

Payment Card Industry Data Security Standard

The Payment Card Data Security Standard (PCI DSS) is a binding set of rules and procedures established by four major credit card companies (Visa, Mastercard, Discover and American Express) in 2004 and is aimed at companies that accept credit cards as payment method. The primary objective of PCI DSS is the prevention of fraud and theft of credit card data on the Internet.

Please visit PCI DSS for further information and details.

For more detailed information regarding PCI DSS we invite you to have a look at PCI DSS and Mastercard and PCI DSS and Visa.

Self-Assessment Questionnaires

Self-Assessment Questionnaires (SAQ) are tools which you may use upon request by your acquirer to determine whether your online shop meets established PCI DSS requirements.

SAQ compliance for your online shop

To ensure the highest level of data security, your acquirer will request from you to fill out a specific Self-Assessment Questionnaire (SAQ) prior to concluding an acceptance contract with you. The handling and management of sensitive financial data in online shops is always a crucial issue in fulfilling the relevant SAQs and obtaining PCI-compliance. However, there is **no need for your online shop** to handle or store sensitive data since all necessary financial and personal data required for the payment process are handled by the Wirecard Checkout Server.

Also, when choosing Wirecard as your PCI-compliant third-party payment processor, it becomes much easier for you to comply with the relevant SAQ requested by your acquirer and no additional PCI-compliance for your online shop is required.

Applicable SAQs for Wirecard solutions

There are various SAQ versions available to select from to best suit your business profile. The following SAQs are applicable when using Wirecard products:

SAQ version	Business scenario	Applicable for Wirecard solution
SAQ A	Applicable for card-not-present merchants, when **all** cardholder data functions are outsourced to a PCI-compliant payment processor. Eligible e-commerce implementations: when merchant web site is entirely hosted and administered by a compliant third-party payment processor, or provides an iframe to a PCI-compliant third-party payment processor or contains a URL link redirecting consumers from merchant web site to a PCI-compliant payment processor. Visit implementation examples eligible for SAQ A vs. SAQ A-EP for more information and details.	Wirecard Checkout Page (also in native app as web view).
		Wirecard Checkout Seamless with “PCI DSS SAQ A Compliance” (also in native app as web view).
SAQ A-EP	Applicable for card-not-present merchants who **partially** outsource their e-commerce payment channel to PCI DSS validated third parties and do not electronically store, process or transmit any cardholder data on their systems or premises.	Wirecard Checkout Seamless without “PCI DSS SAQ A Compliance” (also in native app as web view).
SAQ C-VT	Applicable for merchants using only web-based virtual terminals, without electronic cardholder data storage.	Wirecard Checkout Terminal
SAQ D	All other merchants not covered by any SAQ and all service providers defined by a payment brand as eligible to complete an SAQ.	Wirecard Checkout Automated

Please visit PCI DSS Self-Assessment Questionnaire for further information and details.

Hiding security information

Please put the file(s) where your secret or password is defined within a folder on the file system of your web server which cannot be accessed from users accessing your web server via their web browsers.

Encrypting your online shop

We strongly recommend that you encrypt any communication in your online shop to allow access only by a secure communication via https.

Wirecard Checkout Page and Wirecard Checkout Seamless also use secure communication based on https and if your online shop or parts of your online shop are accessed by http the consumer in your online shop will receive the following security warning from the web browser:

```
Although this page is encrypted, the information you enter will be sent
via an unencrypted connection and could easily be read by third parties.
```

```
Are you sure you want to send this information?
```

To prevent such warning messages from appearing, ensure the consistent use of https within your online shop.

Saving order data and payment process results

We strongly recommend that your online shop saves all relevant order data of each purchase and of each consumer before you start the Wirecard Checkout Page or Wirecard Checkout Seamless and immediately after the payment has been made by your consumer. This way you may assign and correlate each order with the relevant payment process results at a later date.

Disabling change of shopping basket

Ensure, according to the functionalities of your online shop, that your consumer has no possibility to change the items in the shopping basket once the payment process was started.

Regular security updates

We advise you to check all security updates available for all software you use within your online shop, your database and your web server on a regular basis.

OWASP Top 10

Have a look at OWASP regarding typical security risks and their impacts on online sites.

Scheduled backups

We recommend you to configure scheduled backups for all order and checkout related information of the consumers of your online shop to ensure that you have these data at your disposal in case of any later complaints or frauds.

Secret and fingerprint

What is a "secret"?

A secret is a pre-shared key (see Wikipedia) which is only known to you, the integrator of the online shop and Wirecard CEE.

The secret you will get from our support teams is used to secure the transfer of all sensitive parameters and their values between your online shop and the Wirecard Checkout Page and Wirecard Checkout Seamless.

Keep your secret really secret!

To ensure a secure communication it is essential that you NEVER disclose or share your pre-shared key with persons who are not involved in developing the online shop!

NEVER forward this pre-shared key via unsecured communication channels e.g. mail, e-mail, fax or instant messaging. When the pre-shared key is submitted by fax make sure that the contents of the fax is disclosed only to the intended and authorized persons!

NEVER send the secret as a parameter to the Wirecard Checkout Page or Wirecard Checkout Seamless!

If you suspect that your pre-shared key is known to unauthorized persons contact our support teams immediately to request the creation and submission of a new secret.

What is a "fingerprint"?

A fingerprint is a method to ensure that sensitive parameters and their values sent from your online shop to the Wirecard Checkout Server and vice versa are not changed by anyone while transferring the data over the Internet.

A fingerprint is created by concatenating all parameter values to a string and hashing this string by an HMAC-SHA-512 algorithm using the secret (also called pre-shared key) as cryptographic key.

When submitting data from your online shop to Wirecard Checkout products you also transmit the fingerprint and the name and order of all parameters used for creating the fingerprint (fingerprint order). The Wirecard Checkout Server then creates the fingerprint of all received parameter values with the specific secret stored in the Wirecard Checkout Server. If the fingerprint you sent us and the fingerprint computed on the Wirecard Checkout Server are identical, the values of the parameters transmitted by you were not modified, e.g. during a man-in-the-middle attack (for details have a look at Wikipedia).

Please remember the following information for response fingerprint calculation: If *magic_quotes_gpc* or *magic_quotes_runtime* is enabled on your server or in your shop, use stripslashes to remove unnecessary slashes within the fingerprint seed.

Please also remember that any data which are not sent URL-encoded could lead to error “FINGERPRINT is invalid” because special characters may be interpreted differently.

Firewall settings

When integrating Wirecard Checkout Page or Wirecard Checkout Seamless into your online shop you may need to adjust the security settings of your firewall.

To receive confirmation information from Wirecard regarding a transaction via the `confirmUrl` you need to enable incoming communication from our following IP-addresses:

- 195.93.244.97
- 185.60.56.35 and
- 185.60.56.36

To send data or commands to Wirecard Checkout Page or Wirecard Checkout Seamless you need to enable outgoing communication to the following servers:

Name	IP address
checkout.wirecard.com	185.60.56.34:443
secure.wirecard-cee.com	185.60.56.33:443
www.qenta.at	185.60.56.43:443
www.qenta.com	185.60.56.44:443