

Wirecard CEE Integration Documentation



Created: 2019-11-14 00:19

Change in Security Protocols

The secure transmission of card holder data requires, amongst others, the use of a secure encryption protocol.

Consistent with Requirement no. 4.1 and Annex II of the PCI Data Security Standard (in the current valid version 3.2.1, January 2018), strong security protocols must be used to safeguard sensitive card holder data during transmission over open, public networks.

Wirecard CEE offers its customers (merchants) services for the technical processing of eCommerce payment transactions. In the course of such payment processing and on behalf of its customers, Wirecard CEE stores, processes and transmits payment related card holder data from credit cards. As payment service provider, Wirecard CEE must thus comply with the PCI DSS security requirements in the current valid version and is obliged to ensure compliance especially with Requirement no. 4.1 and Annex II.

Disablement of TLS 1.0

Subject to the PCI DSS requirements and in line with the guidelines of the National Institute of Standards and Technology (NIST Special Publication 800-52 Revision 1), **all service providers must offer a secure service no later than June 30, 2016 and no longer use any earlier versions of TLS or SSL as encryption protocol as of June 30, 2018**. In other words, according to the NIST, TLS 1.0 and SSL (e.g. SSL 1.0, SSL 2.0, SSL 3.0) are considered unsafe as of April 2014. For this reason, Wirecard CEE is obliged to disable the mentioned protocols. Disablement of the protocols affects merchants using Wirecard Checkout Page or Wirecard Checkout Seamless and the following domains:

secure.wirecard-cee.com

checkout.wirecard.com

www.qenta.at

www.qenta.com

Information for merchants

Due to internal certification processes, affected merchants will be informed that disablement of the mentioned protocols will take place as of July 31, 2017.

As of August 1, 2017 payment processing will only be supported by TLS 1.1 or higher.

Encryption protocols such as SSL 1.0, SSL 2.0, SSL 3.0 and TLS 1.0 are no longer acceptable as strong standards for encryption but can pose in fact a serious risk for final consumers in online business. We therefore appreciate your understanding as this security update is for your own benefit and offers maximum security in eCommerce transactions.

For any questions regarding the disablement of unsafe protocols, contact support.at@wirecard.com, including your customer number.

Additional information regarding TLS

For additional information and overviews regarding TLS/SSL and supported web browsers and libraries, visit

- https://en.wikipedia.org/wiki/Transport_Layer_Security#Web_browsers
- https://en.wikipedia.org/wiki/Transport_Layer_Security#Libraries