verifone

Server to Server Payments with 3D Secure Setup Guide

Overview

This guide describes how to collect card details using verifone.JS and authenticate the customer with 3D Secure (3DS) as well as perform 3D Secure authenticated, server-to-server payments.

In addition, this document focuses on the the steps that you (as a merchant) need to complete to accept 3D Secure transactions with card payments offering code samples and implementation tips and a brief glossary.

Glossary

- The **client** - is a computer or software program that requests services or resources from a server over a network.
- The **server** - is a computer or software program that provides services or resources to other computers, known as clients, over a network. Servers are designed to handle requests from clients and fulfill those requests by providing data, processing tasks, or performing computations.
- **Client-server** is a relationship in which one program, the client, requests a service or resource from another program, the server.
- **Songbird** - is a JavaScript file used used for performing 3D Secure Assessment
- **3DS** - 3-D means 3-domain: issuer domain, acquirer domain, and interoperability domain (the schemes). See more in the 3D Secure documentation.
- **verifone.js library** - is a quick and secure way to collect sensitive credit card data. This allows users full control over the checkout experience while maintaining a minimum SAQ A-EP level.
- **JSON Web Token (JWT)** - is a standardized way to securely send data between two parties (a client and a server). JWTs contain information (claims) encoded in the JSON format. These claims help share specific details between the parties involved. A JWT is a mechanism for verifying the authenticity of some JSON data.
- **Server-to-Server payments** - a method used to transfer funds between financial institutions through a secure electronic communication mechanism. This kind of transfer usually entails the direct exchange of data between the servers of the participating financial institutions and is utilized for big or high-volume transactions, including business-to-business payments.

Compatibility

- This guide assumes a basic understanding of HTML and JavaScript.
- This integration requires the ability to run two .JS URLs on the front-end browser.
- This integration also requires the ability to make server-side REST API calls. API calls should not be made from the client-side.
- 3D Secure authentication is included in this flow, which is required for countries following SCA regulations.

Before you get started

Starting from scratch? Follow these steps to get started.

- Have a Verifone Central account in either our Sandbox or Production environment with API Access.
- Don’t have a Verifone Central Account already?
    - Contact your regional sales team to get started.
- Have access to a Verifone Central account that has the Merchant Cashier or Merchant Supervisor User Role.
- Forgot your password?
    - Click the portal link for your region and reset your password.
- Generate a Secure Card Capture Key on your user’s organization.