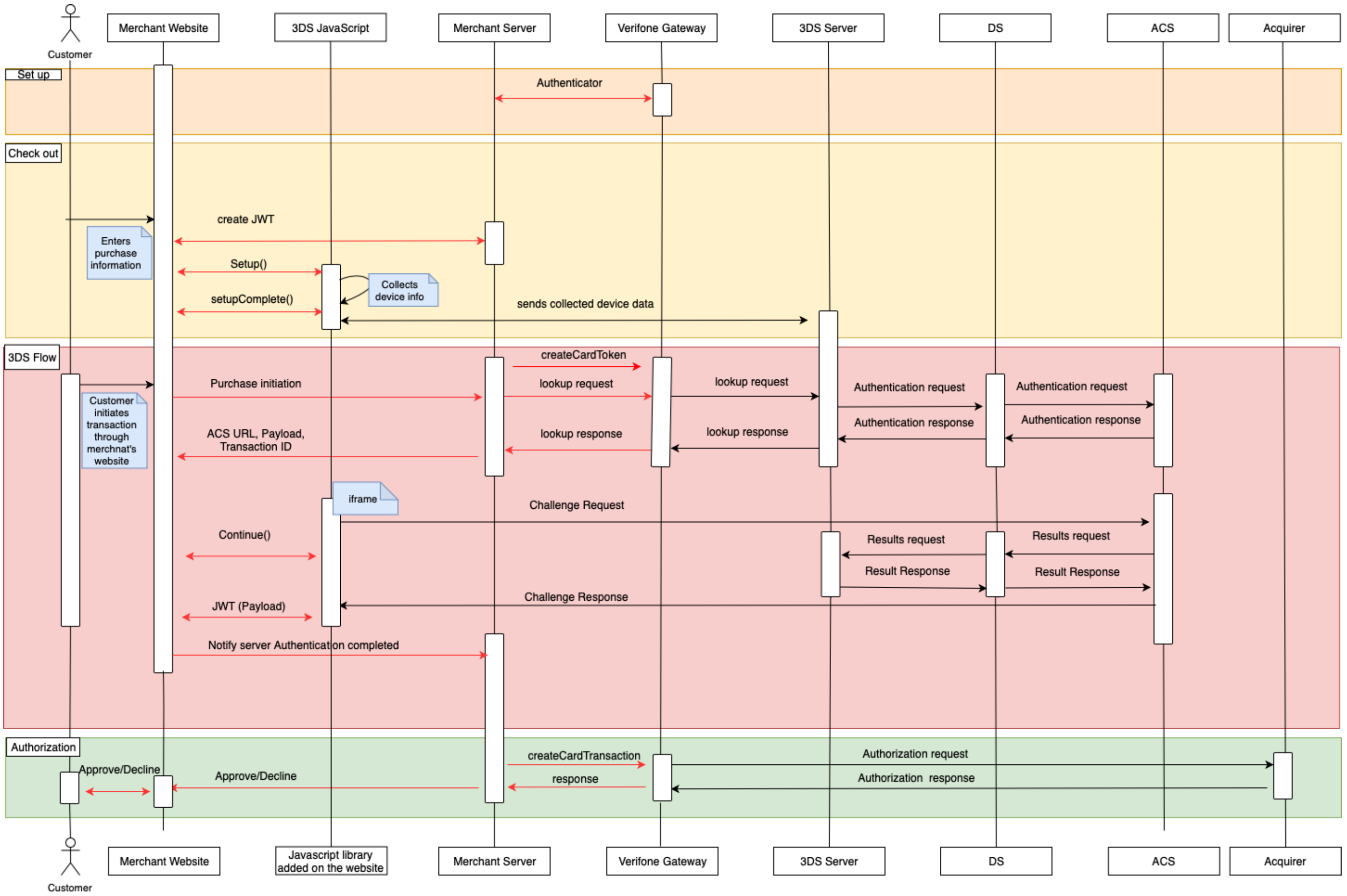
3-D Secure

For using directly our API to perform 3DS transactions you need to integrate on your website a JavaScript that handles the step up interaction with Cardholder and gathers the browser information. The figure below presents the complete flow when a browser is used by the cardholder to purchase a good. The payment flow consists of four parts: the setup, the actions before the customer initiates the purchase (clicks buy button), the Authentication and finally, the Authorisation.



Set up

During the set up part, the merchants will receive their credentials and assistance how to set an authenticator and 3DS account details.

Check out

The check out section takes place when the cardholder fills in the payment details. The following steps shall be completed prior to the cardholder initiating the transaction (clicks ‘Buy/Order’).

1. Create a JWT in the backend server as described here
2. Include the JavaScript on the website as described here

a. Configure it (optional)

b. Listen for events

c. Initialize the Songbird

d. Use the BIN detection to successful complete the 3DS Method

e. When 'payments.setupComplete' event is returned the set up step has been completed

3DS Flow

The Authentication flow, begins when the Cardholder initiates the transaction (clicks ‘Buy/Order’).

1. The Cardholder has initiated the transaction send the lookup request using the lookup API and in response receive the lookup response
2. In the lookup response the Issuer has defined whether the Cardholder is required to continue with the challenge flow (step up). If the Issuer requests a challenge to happen send the Cardinal.Continue as described in section 1.5 here.
3. When "payments.validated” is event returned (see section 1.3.2 payments.validated), send the JWT to the backend and validate it (see JWT Validation)
4. Use the payment details to authorise the payment.

Processing the Lookup Response

After the ‘Lookup Response’ is returned, the merchant shall analyse the result of ‘enrolled’ and ‘pares_status’ to verify that the transaction is eligible for Authentication. A transaction is eligible to continue the Authentication when the data element ‘enrolled’ contains a ’Y’ value.

1. If the data element ‘enrolled’ contains a ’Y’ value and the ‘pares_status’ contains the value ‘Y’ then the authentication was successfully completed in a frictionless way (frictionless flow).
2. If the data element ‘enrolled’ contains a ’Y’ value and the ‘pares_status’ contains ‘C’, then get the acs_url (AcsURL), payload (Payload), and transaction_id (TransactionId) and include them in the Cardinal.continue function in order to proceed with the authentication session. The Cardinal.continue will display a modal window and automatically post the consumer's session over to the acs url for authentication (section 1.5 Cardinal.Continue).
3. If the data element ‘enrolled’ contains a ’Y’ value and the ‘pares_status’ contains the value ‘R’, then the issuer is rejecting authentication/verification and request that authorisation should not be attempted.

If the ‘enrolled’ value is NOT Y, then the transaction is NOT eligible for Authentication. The ‘eci’ value represented on the Lookup response should be passed on the authorization message to Verifone.