Migration Steps for Secure Acceptance and Cruise API

I. Merchants connected via SA/Secure Acceptance (Gateway is Ready and Not using API):

No action

II. Merchants connected via SA/Secure Acceptance (Gateway is Not Ready or also using API):

1. Contact support to activate 2.x
    a. must specify cards, currencies, etc.
2. Run test transactions to confirm 2.x transactions are working properly

III. Merchants connected via API:

Note: Pre-requisite is readiness of acquiring processor for processing and clearing for all necessary card schemes.

Activate your Cybersource MID (Required)

- Reach out to Client Services to request activation of 3DS 2.x for your MID(s) in test and/or production environment
    - Will need to specify cards, currencies, etc.
    - It is strongly recommended testing your new implementation in Cybersource test environment before deploying it to production

1. Update Payer Authentication implementation (Required)
    - Server side or back-end changes:
        1. Add Payer Authentication Setup Application to your transaction flow.
        2. Update Payer Authentication Enrollment application to include additional required and optional fields.
            a. Will need to include reference ID and return URL (mandatory technical fields), and other additional fields appropriate for your business (such as conditional 3DS 2.x fields, order data, customer data, etc.)
        3. Update Payer Authentication Validation application to include additional required fields and modify existing fields

    a. Will need to include transaction ID (mandatory technical field)
- Website or Front-end changes:
  1. Add device data collection (device data collection is mandatory for 3DS 2.x)
  2. Modify implementation for step-up Authentication

2. Update Payment Implementation (optional)
   If you are using Cybersource Payment application combined with Payer Authentication Enrollment or Validate, then there is no action required on your end.

   If you are making separate calls and/or using a payment gateway outside of Cybersource, then you will need to make modifications to your payment application.
   Consult the Cybersource Payer Authentication Developer Guide and Credit Card Services Developer Guide to pass appropriate 3DS information on to the payment transaction. Please ensure your payment implementation is compliant for each card scheme.

3. Test your 3DS 2 Implementation.
   This testing ensures that you understand the possible use cases as part of implementation. Refer to "Testing Payer Authentication" and run the test cases in "Test Cases for 3-D Secure 2.x."

4. Once ready to go live you can proceed to switch over to your new implementation in the production environment.

Resources:

Payer Authentication Developer Guide:

http://apps.cybersource.com/library/documentation/dev_guides/Payer_Authentication_SO_API/Payer_Authentication_SO_API.pdf

Credit Card Services Developer Guide:

https://developer.cybersource.com/library/documentation/dev_guides/CC_Svcs_SO_API/Credit_Cards_SO_API.pdf

IV. Partners:

(Acquirer/reseller)

- *First pre-requisite is readiness of acquiring processor for2.0 processing.*
- *Second pre-requisite is readiness of acquirer for processing and clearing for all necessary card schemes (incl. the TC33A files for Visa Platform Connect)*

1. Pre-registration - Acquirer to register merchants (by MID) within their system and also within Mastercard portal directly (ISSM) to be enabled for 3DS 2.x

2. Raise support case via Support Center portal. For further details on how to contact support see the following article:
   How to Contact Cybersource Client Services
3. Request MIDs to be enabled for 2.0
   a. Click on below link for an outline of data which needs to be collected prior to submitting a ticket
      How do I update to EMV 3DS
4. Acquirer will hear back from CYB support team regarding progress and timeline for registering credentials to 2.0
   a. Note that the merchant can test their integration while waiting for the card schemes to be updated.
   b. Timing will depend on number of card schemes which need to be activated, average timing may be found below.

Directory server typical lead-times

Card Scheme	Lead-time (Business Days)
Visa (Verified by Visa)	Immediate
MasterCard / Maestro (SecureCode)	Managed by Acquirer
American Express (SafeKey)	Immediate
Diners / Discover (ProtectBuy)	Immediate
JCB (J-Secure)	Immediate
ELO (Compra Segura)	Managed by Acquirer
Cartes Bancaire (FAST'R)	Managed by Acquirer

5. Once the credentials are registered, Cybersource support will send a support ticket confirmation to the acquirer that the set-up is ready.
6. The Cruise Credentials will then be visible to both the acquirer for their portfolio, as well as the merchant if they have access to EBC.
7. The merchant(s) should be able to start development and testing for the new configuration.

MERCHANT SET UP

1. Once merchant is setup with Acquirer, the merchant can be registered within Cybersource and Payer Authentication services can be enabled.
2. Update Payer Authentication implementation (Required)

- Server side or back-end changes:
    1. Add Payer Authentication Setup Application to your transaction flow.
    2. Update Payer Authentication Enrollment application to include additional required and optional fields.
        a. Will need to include reference ID and return URL (mandatory technical fields), and other additional fields appropriate for your business (such as conditional 3DS 2.x fields, order data, customer data, etc.)
    3. Update Payer Authentication Validation application to include additional required fields and modify existing fields
        a. Will need to include transaction ID (mandatory technical field)
- Website or Front-end changes:
    1. Add device data collection (device data collection is mandatory for 3DS 2)
    2. Modify implementation for step-up Authentication

3. Update Payment Implementation (optional)
   If you are using Cybersource Payment application combined with Payer Authentication Enrollment or Validate, then there is no action required on your end.

   If you are making separate calls and/or using a payment gateway outside of Cybersource, then you will need to make modifications to your payment application.
   Consult the Cybersource Payer Authentication User Guide and Credit Card Services Implementation Guide to pass appropriate 3DS information on to the payment transaction. Please ensure your payment implementation is compliant for each card scheme.

4. Test your 3DS 2 Implementation.
   This testing ensures that you understand the possible use cases as part of implementation. Refer to "Testing Payer Authentication" and run the test cases in "Test Cases for 3-D Secure 2.x."

5. Once ready to go live you can proceed to switch over to your new implementation in the production environment.