Version 1.4

Onboarding Guide

3D-Secure

- The Three Domain Secure (3-D Secure™ or 3DS) Protocol has been developed to improve transaction performance online and to accelerate the growth of e-commerce. The objective is to benefit all participants by providing issuers with the ability to authenticate cardholders during an online purchase, thus reducing the likelihood of fraudulent usage of payment cards and improving transaction performance.

Access Control Server (ACS)

- VCAS is an ACS. An ACS is a hardware/software server entity that supports 3-D Secure authentication and other functions. The ACS is operated by the issuer or the issuer's agent. In response to Directory Server inquiries, the ACS verifies that the individual card account number is eligible for authentication, receives authentication requests from merchants, authenticates the cardholder during online purchases, and provides digitally-signed authentication response messages (containing authentication results and other 3-D Secure data) to the merchant and to the Authentication History Server.

Directory Server

- A server that determines how to route 3-D Secure messages (i.e., which ACS to route the messages to). For a VCAS project, the card brand Directory Server (i.e., the Visa Directory Server for Verified by Visa and the Mastercard Directory Server for SecureCode) needs to be set up to route the issuer's 3-D Secure transactions to VCAS.

Electronic Commerce Indicator (ECI)

- A value that indicates the level of authentication on the transaction. VCAS provides the merchant with the appropriate ECI value to use, or the merchant determines the ECI value based on the outcome of the transaction. The merchant then populates the ECI in the authorization message. ECI values are:
- Cardholder authentication successful

  Visa: 05

  MasterCard: 02
- Merchant attempted to authenticate the cardholder

  Visa: 06

  MasterCard: 01
- Non-authenticated e-commerce transaction

  Visa: 07

  MasterCard: 00

- Onboarding Forms
  - Used to collect required information from the Financial Institution to validate before project kick off. This information is also important to properly submit correct documentation requirements to the card networks.

- Risk-Based Authentication
  - The real-time analysis of data and purchase history to determine the riskiness of a transaction. This information is fed real-time into a risk model to generate a score per transaction.
  - Pass/Fail Risk-Based Authentication

    Using the risk score as well as other data elements to determine whether to pass of fail authentication for each transaction.
- BIN Range
  - The 16-digit lower and upper ranges that will be participating in 3D-secure. These ranges will be implemented in VCAS and activated at the Directory Server(DS).
- Authentication Keys
  - Authentication Value (AV) is a double- length DES key. A cryptographic value, unique for each transaction, that provides evidence that cardholder authentication (or merchant attempted authentication) took place. The recommended number of keys for each card network is one.
  - CAVV: Cardholder Authentication Verification Value

    Card Brand: Visa

    Created & Validated by Visa
  - AAV: Accountholder Authentication Value

    Card Brand: MasterCard

    Created by Cardinal and Validated by MasterCard

An Issuer has the option to utilize 1 AV key for all BINs or to apply a key per BIN. Most issuers elect to use 1 key for their institution as a whole.

- Primary Mastercard ICA (associated with the BIN)
  - A four to six-digit identification assigned by **MasterCard** for use by a member to uniquely identify activity the member is responsible for. The primary ICA number is also the ICA number under which quarterly billing occurs.
- MasterCard Company ID
  - Is unique to each MasterCard franchise company and serves as an identifier at the highest level. (e.g. CIS-2017-15419)
- MasterCard CIS Number (Customer Interface Specification)
  - A number MasterCard gives to a project when it is opened.
- Visa CIQ
  - A key management client information questionnaire can be used by financial institutions and processors to request BASE I and VIP cryptographic keys to be created by Visa, copied between existing BINs, transferred from Visa to client/processor or from client/processor to Visa.
  - You will need to complete the highlighted sections of the attached CIQ.
- Logo (Page 3 Processing Screen)
  - PNG Format
  - 200x70 or 2.85 ratio
  - Preferably transparent background

- Opening a Visa Project
  - CardinalCommerce will open the project with Visa on your behalf, once all assets are collected.
- Opening a project with Mastercard
  - Financial institution will email the CIS_NorthAmerica_Support@mastercard.com alias to kick off the project, copying ICBA.
  - Mastercard will provide a 1265, 1267 & 1270 forms.
  - Mastercard will typically reply within three business days and provide a CIS number. That CIS number will be added to the 3D-secure client Onboarding Package.
- Testing
  - Testing takes place to ensure that the issuer's program is ready for production. This testing includes ensuring that the issuer's overall setup is correct, checking the issuer's consumer screens, and performing Authentication Value validation, from authentication to authorization.
  - What information to provide to Cardinal Project Manager?

    Production PAN (Project Manager will reach out to obtain this information)

    Tester Name and Email to coordinate testing with.
  - When will testing begin/contacted for testing?

    Cardinal Project Manager will coordinate testing needs.
- Estimated Timeline
  - Once all assets are turned over to CardinalCommerce.

    Verified by Visa
    - Estimated 6 weeks

    Mastercard Securecode
    - Estimated 8 weeks
- Processing Screen
  - This screen may appear to the cardholder when shopping on a 3D-secure participating merchant's website.