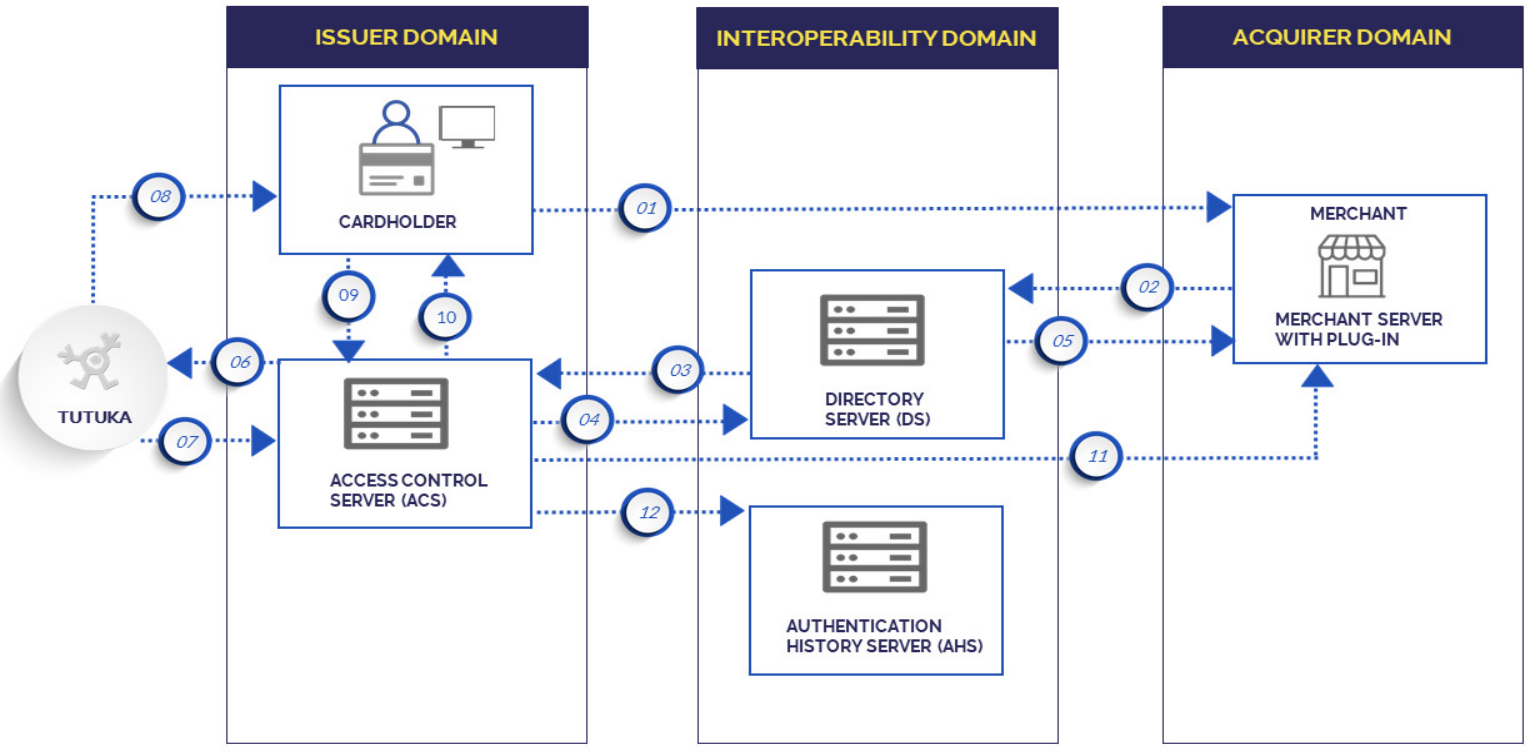
Mastercard Dynamic 3D SecureCode *Information*

For a purchase on an e-commerce store with 3D SecureCode, the following steps are involved in the 3D SecureCode validation process and the transaction authorisation steps:

3D SecureCode Validation:

1. The cardholder enters their card details on the checkout screen on the merchant's online store.
2. To check if a BIN is registered, the merchant sends a message to Mastercard directory server.
3. Mastercard's directory server confirms with the ACS server that the BIN is registered for 3D SecureCode.
4. ACS server confirms if the BIN is registered and card range is loaded on Mastercard's directory server.
5. Mastercard then directs the merchant to the URL for the pop-up screen where a cardholder will enter the 3D SecureCode. A pop-up screen then appears on the web store interface. The pop-up screen is set up by the ACS provider on a specific URL as the process is now handed over to the ACS provider for the rest of the 3D Secure steps.
6. ACS server will send Tutuka the request to generate a One-time PIN (OTP).
7. Tutuka generates the OTP and sends on to the ACS server and the wallet provider.
8. Cardholder receives the Dynamic 3D SecureCode (OTP) via SMS or through the app supplied by the wallet provider.
9. Cardholder inputs Dynamic 3D SecureCode and clicks "submit", and the Dynamic 3D secure code goes to the ACS server and gets validated by ACS.
10. The ACS server confirms validation back to the store web page which is visible to the cardholder.
11. The ACS server then sends the result and UCAF information to the merchant.
12. The ACS server sends a message back to AHS server at Mastercard to confirm validation took place, so there is history of validation that took place.

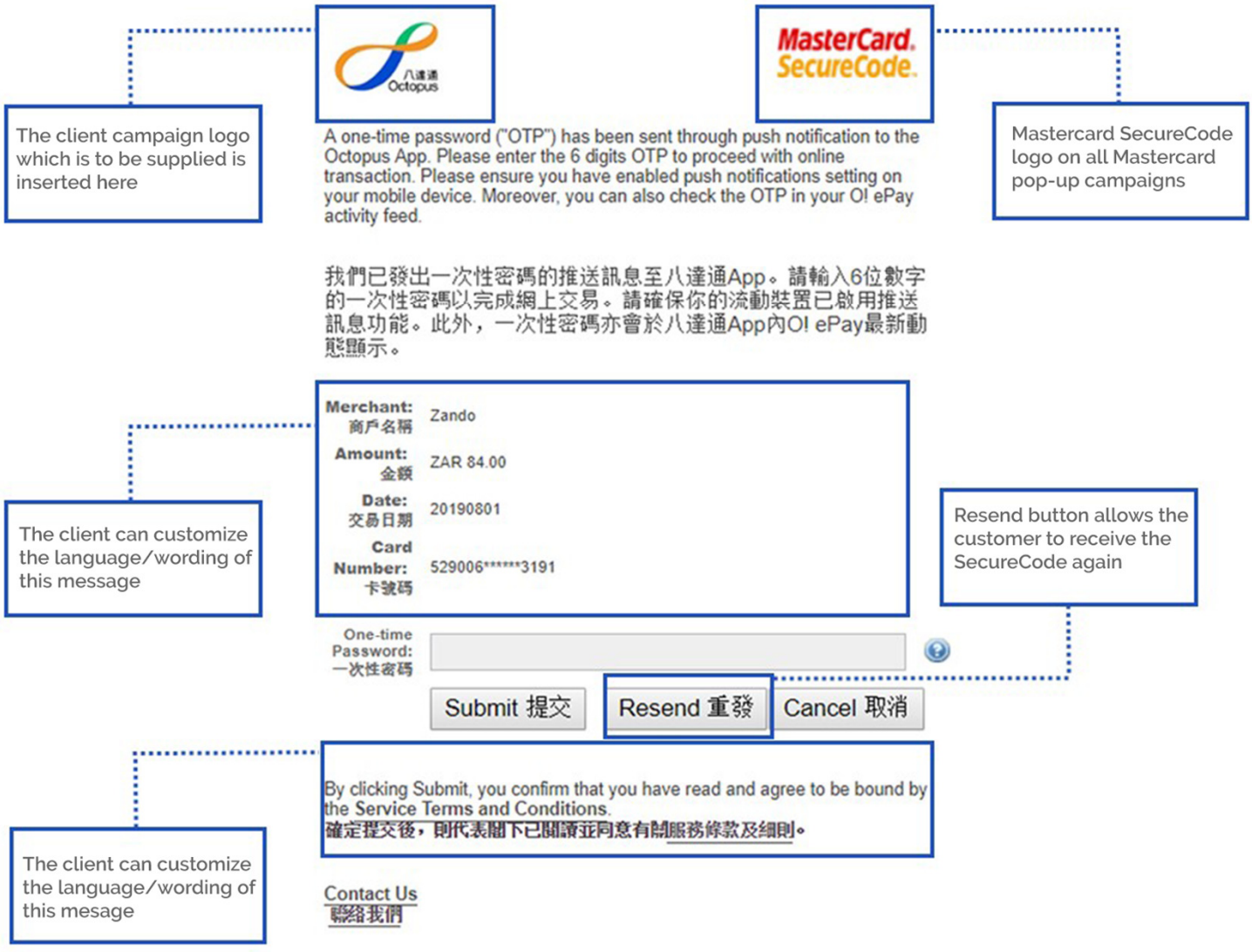


Mastercard Dynamic 3D SecureCode *Information*

Transaction Authorisation:

1. The merchant then sends the transaction (with UCAF information in the transaction message) to Mastercard for authorization like any other transaction.
2. Mastercard then sends on to Tutuka.
3. Tutuka validates UCAF information (AAV is included in UCAF information).
4. If it is validated successfully, then Tutuka does all other relevant checks on the card for an authorization request.
5. If all the checks are successful, then the transaction authorization is sent to Mastercard and Mastercard sends it on to the merchant.
6. The merchant then presents the approved response on the web interface which is visible to cardholder.

Mastercard SecureCode Pop-up Customization available to Issuers



Mastercard Dynamic 3D SecureCode *Information*

- We require the client to provide their logo for insertion
- Logo to be supplied in the following format:
  PNG format, no larger than 50px by 150px
- Client can customize multiple languages/wording in pop-up and set a default language
- 3D SecureCode:
  - 3D standard SecureCode is 5 digits long
  - 3D standard SecureCode in the Asia region is 6 digits long
- Customised wording can be highlighted where necessary in **bold**

Pop-up for when error occurs after cardholder enters SecureCode OTP:

- System Error name can be customized
- System Error pop up wording can be customized