

1. Description

- 1.1 Click to Pay (C2P) is a standardized e-commerce checkout experience developed by Card Schemes based on EMVCo Secure Remote Commerce (SRC) standards. It provides users with a fast, secure, and consistent online payment experience similar to the simplicity of contactless payments in physical stores.
- 1.2 By leveraging network tokenization, Click to Pay eliminates the need for users to manually enter their card details at checkout. Once enrolled, users can be recognized as returning users and complete payments in just a few clicks. Users only need to enroll once to C2P to become returning users.
- 1.3 C2P is device-agnostic and merchant-agnostic, and it supports interoperability across Card Schemes through a unified technical integration.
- 1.4 C2P is offered within our Checkout SDK, Checkout UI and Pay-by-Link solutions.

2. How does the solution work?

- 2.1 C2P operates through a one-time user enrolment process, whereby payment credentials are securely tokenized by Card Schemes and stored within a network-managed wallet.

2.2 Log in

2.2.1 For first-time users:

- (a) User proceeds to the checkout page on the Customer's website.
- (b) Among the payment options, the user sees a clear "Click to Pay" button, often displaying the MasterCard logo alongside other participating Card Schemes logos (for example, American Express, Discover, Visa).
- (c) User clicks or taps the "Click to Pay" button.
- (d) User is asked to create a "Click to Pay" account. Email address and/or telephone number are required.
- (e) User enters card details (card number, expiry date, CVV) and creates a profile.
- (f) User will be asked to verify their identity for each card added, potentially through an OTP (one-time password) sent via SMS or email.
- (g) User will be asked to agree to the Click to Pay terms and conditions, when applicable.

Click to Pay offers a streamlined enrollment process: first-time users can register directly on a merchant's site or through their issuing bank. Since the solution is merchant-agnostic, once a card is enrolled, it is automatically recognized across all participating merchants. This eliminates the need for repeat registrations, significantly reducing checkout friction.

2.2.2 For returning users (when the user has enrolled before):

- (a) User proceeds to the checkout page on the Customer's website.
- (b) Among the payment options, the user sees a clear "Click to Pay" button within the Card Payments section.
- (c) Once user clicks or taps the "Click to Pay" button, user is recognized via email, phone number, or web cookies.
- (d) If user switches devices or browsers, they might need to re-identify themselves, via previously OTP (one-time password) sent via SMS or email, or biometrically, if available.

Upon successful authentication, the user will be granted access to their securely stored payment credentials. Furthermore, the user will have the ability to enroll and provision additional payment cards into the Click to Pay directly within the checkout interface.

2.3 3D Secure (3DS) authentication, if applicable:

- 2.3.1 Depending on Customer's configuration, the card issuer's requirements, and risk scoring, the payment transaction might trigger 3DS authentication.
- 2.3.2 When 3DS authentication is initiated, the user will typically be presented with an authentication challenge by their card issuer. This will involve entering an OTP (one-time password) sent via SMS or email.
- 2.3.3 Once the user successfully authenticates, 3DS authentication result is sent back to our Payment Platform.

- 2.4 Fraud check, if applicable:
 - 2.4.1 In parallel or sequentially with 3DS authentication, fraud checks are conducted.
 - 2.4.2 The outcome of the fraud check influences whether the transaction proceeds to authorization.
- 2.5 Authorization:
 - 2.5.1 Once the 3DS authentication is completed (if triggered) and the fraud checks are satisfactory, the result of the authorization request is sent to the relevant card issuer.
 - 2.5.2 This request includes details about the transaction (amount, currency, merchant information, and the payment details through a network token provided by C2P).
 - 2.5.3 The issuer then approves or declines the transaction based on factors like the cardholder's available balance and their risk assessment.
- 3. Key features**
 - 3.1 Seamless user recognition
 - 3.1.1 Click to Pay enables secure recognition of returning customers without requiring a specific device.
 - 3.1.2 Users can be identified using email address, mobile phone number, browser cookies, or remembered sessions.
 - 3.1.3 This allows customers to retrieve their stored card credentials across different devices and browsers, creating a consistent and convenient checkout experience.
 - 3.2 Network tokenized payments
 - 3.2.1 Click to Pay replaces the use of raw card numbers with network tokens (DPAN).
 - 3.2.2 Card credentials are securely stored within the card network vaults, while Customer receives only tokenized credentials during payment processing.
 - 3.2.3 Each transaction includes network token (DPAN), and dynamic cryptogram.
 - 3.3 Multi-network support
 - 3.3.1 We integrate Click to Pay through MasterCard's unified API, while the solution is designed to support all major Card Schemes within a unified integration model.
 - 3.3.2 Supported card schemes include American Express, Discover, MasterCard, and Visa.
 - 3.3.3 This enables Customer to offer a consistent checkout experience across multiple Card Schemes.
 - 3.4 Improved payment performance
 - 3.4.1 By leveraging network tokenization and card network authentication capabilities, Click to Pay helps Customer to increase authorization success rates, reduce cart abandonment, and improve checkout conversion.
 - 3.5 Reduced PCI DSS exposure
 - 3.5.1 Because card credentials remain stored in the card network vaults, Customer does not directly handle sensitive card data when network tokenization is used.
 - 3.5.2 This can help reduce PCI DSS scope and compliance obligations for Customer.
 - 3.5.3 Click to Pay aligns with global Card Schemes initiatives to standardize secure remote commerce.
- 4. Disclaimers and limitations**
 - 4.1 Customer must accept MasterCard terms and conditions set out here <https://www.mastercard.us/content/dam/public/mastercardcom/na/us/en/smb/other/mastercard-click-to-pay-terms-conditions.pdf>.
 - 4.2 If the issuer does not support Click to Pay, transactions may fall back to traditional card processing using the original card number (FPAN).
 - 4.3 If the issuer supports Click to Pay, but the acquirer does not, transactions may fail for certain Card Schemes that do not allow fallback to FPAN.

- 4.4 We held certification for the checkout flows for our Checkout UI and Pay-by-Link solutions, which are fully controlled by us. For Checkout SDK, certification of the user experience must be completed between Customer and MasterCard.
- 4.5 We provide a pre-certified user experience (UX) for the Click to Pay solution when integrated with our Checkout UI or Pay-by-Link solutions.
- 4.6 If Click to Pay is integrated with our Checkout SDK solution or if Customer requests or implements any customizations to our managed user interfaces (Checkout UI or Pay-by-Link solutions), Customer shall be solely responsible for obtaining all necessary approvals and re-certifications from MasterCard. We are not liable from any modifications made or requested by Customer.
- 4.7 Click to Pay solution does not support certain payment features, including split payments across multiple cards, combined payments using gift cards or vouchers, exchange rate or surcharge calculations, and instalment payment options.
- 4.8 We are not responsible for Customer's compliance with the Law or Industry Mandates.

5. Dependencies

- 5.1 Customer must contract any of our Checkout SDK, Checkout UI or Pay-by-Link solutions, and our orchestration module.
- 5.2 Payment transactions must be processed through our Payment Platform.
- 5.3 Network tokens (DPAN) and cryptograms must be passed for authorization
- 5.4 For 3D Secure and Fraud Management, Customer must contract our solutions.
- 5.5 Customer must contract Amadeus front-ends to receive this solution through them.
- 5.6 Click to Pay availability depends on the readiness of Customer's payment ecosystem, including issuers, acquirers, Card Schemes, and Third-Party Providers. Click to Pay is also dependent on the geographic and technical coverage provided by the Card Schemes.

Customer accepts that supported countries, participating issuers, and acquirer's compatibility are determined solely by the Card Schemes and may be subject to change without prior notice.

6. Integrations

- 6.1 This solution can be integrated with the PNR.
- 6.2 This solution can be integrated via webservices with Customer's front-ends.
- 6.3 This solution can be integrated in the following Amadeus front-ends/channels:
- 6.4 Other integrations with Customer's front-ends may be available, subject to further scoping.