Use Cases

What Enrollment Creates

Enrolling a card into Click to Pay creates two linked artefacts within the TSP's SRC System:

- A Consumer Profile (SRC Profile): Tied to the cardholder's verified identity (email address and/or phone number). A single consumer profile can hold multiple enrolled cards across multiple networks.
- A Token (Network Token / DPAN): A surrogate value that replaces the PAN for use at Click to Pay checkout. The token is domain-controlled — it is only usable in the SRC context and is bound to the consumer's profile.

From an issuer's perspective, enrollment is the act of provisioning the cardholder's PAN and identity into the TMP API, which in turn creates or updates the SRC Profile and requests token issuance from the relevant network SRCS.

Available Enrollment Channels

An issuer may offer Click to Pay enrollment through any or all of the following channels. The TMP API is the same regardless of channel; the channel determines how the cardholder's identity is verified and consent is captured before the API call is made.

Channel	Description	Typical Consent Mechanism
Mobile Banking App (user initiated)	Cardholder opts in via the issuer's iOS or Android app.	In-app consent screen + biometric or PIN confirmation. **Channel supported by synchronous card enrollment endpoint.**
Internet web banking (user initiated)	Cardholder opts in via the issuer's online banking portal	Web consent form + OTP or step-up authentication **Channel supported by synchronous card enrollment endpoint.**

Card management portal (user initiated)	Standalone issuer-hosted portal for card services	Portal login + SMS OTP or email OTP **Channel supported by synchronous card enrollment endpoint.**
No UI, auto enrollment (issuer initiated)	Issuer pushes enrollment without a real-time cardholder session	Prior consent captured (T&Cs presented alongside card activation, opt-in campaign, card issuance agreement) **Channel supported by asynchronous bulk enrollment endpoint.**

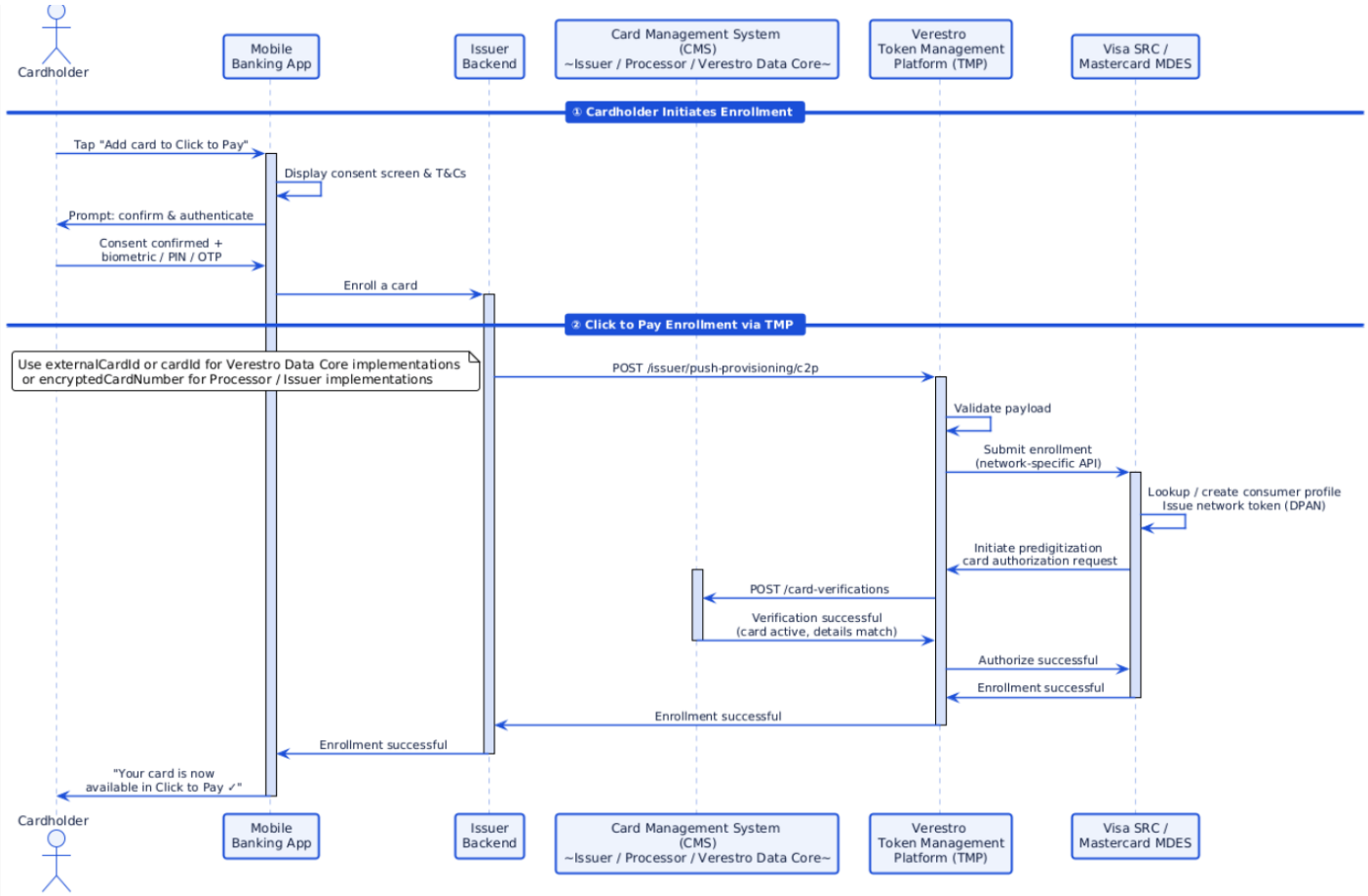
Identity Verification and Authentication Requirements

The SRC specification requires that a cardholder's identity be verified before their card is enrolled. This is the issuer's responsibility. The TMP carries the verified identity attributes in the enrollment request payload but does not perform identity verification itself.

- For user-initiated flows: The issuer's banking application must authenticate the cardholder (e.g., via app PIN, biometric, or step-up OTP) before submitting the enrollment API request. The authentication assurance level must meet the network's minimum requirement.
- For issuer-initiated async flows: The issuer must hold a record of prior consent. This is typically captured at card issuance via terms and conditions, an explicit opt-in campaign, or a standing mandate. Regulatory requirements (e.g., GDPR, PSD2) govern the validity of this prior consent.

How to Implement User Initiated Enrollment

Sequence diagram, happy path



API Documentation

API technical documentation can be found on: TMP API and Issuer API pages. Details may differ, depending on implementation approach, but core APIs are:

1. **TMP API:** POST /issuer/push-provisioning/c2p Issuer mobile app backend calls Verestro TMP to enroll a card to Click 2 pay.
2. **TMP API:** POST /issuer/push-provisioning/tokens/searches Issuer mobile app backend calls Verestro TMP to check existing token statuses and display or hide "Add to Click to Pay" button in mobile application for better user experience, base on the response. If the card has active Click to Pay token, user shouldn't be able to click "Add to Click to Pay" button.
3. **ISSUER API:** POST /card-verifications Verestro TMP will call Issuer/Processor Card Management System to verify card details and status during predigitization, after enrollment initiation.
4. **TMP API:** POST /issuer/v2/card-events Card Management System (issuer or processor) calls Verestro TMP to keep us synchronised with token status in MDES/VTS. TMP also performs token lifecycle actions in MDES/VTS, basing on this request.

Revision #3
Created 20 March 2026 14:53:18 by Ignacy Korytko

Updated 26 March 2026 15:56:49 by Ignacy Korytko