



Stored Credentials - A Guide

Requirements

Card brands have introduced a Cardholder Initiated (CIT) and Merchant Initiated (MIT) Transaction framework. Their aim in introducing CIT/MIT is to increase transaction transparency, which may result in higher authorisation rates and an improved cardholder experience.

Upcoming PSD2 regulations are linked to CIT/MIT, as Strong Customer Authentication (SCA) is required for European transactions from September 2019. Coding to MIT enables issuers identify transactions where the cardholder is not actively participating.

CIT/MIT framework overview

Cardholder Initiated (CIT)		A cardholder participates in the transaction	Used for storing credentials only or for storing and purchasing	Cardholder consent is provided
Merchant Initiated (MIT)		A cardholder does not participate in the transaction	Store credentials in place and used by the merchant to initiate a transaction	Cardholder consent in place

Points to note

- This framework applies to Visa and Mastercard methods of payments and enables a link between the initial CIT and any subsequent MITs
- The framework now also applies to American Express
- Framework applies to credentials (PAN or Payment token) stored by a merchant or its agent
- Existing arrangements (e.g. recurring transactions) can be transitioned to the framework without re-storing credentials
- Testing and certification is required
 - Merchants using a PSP should contact their PSP to determine testing and certification requirements
 - Merchants connecting directly to J.P Morgan should contact their relationship manager to request consulting support

Please see technical specifications available in our [Developer Center](#) for full details of the framework.

Framework transaction types

Transaction	Description	SCA
Recurring	Cardholder provides card details, agreeing to Stored Credential used for recurring subscription billing	✓
	Merchant uses Cardholder Stored Credential to process a recurring subscription billing transaction	Out of Scope
Credential on File	Cardholder provides card details, agreeing to Stored Credential to be used for future purchases with that merchant (CIT or MIT)	✓
	Cardholder buys on merchant website, choosing to pay with the stored credential on file	✓
Instalment	Cardholder provides card details, agreeing to store credentials for future use for a limited series of transactions, for example 3 monthly payments for a single purchase	✓
	Merchant uses Cardholder Stored Credential to process an instalment billing transaction	Out of Scope
Reauthorisation	To submit an authorisation for an amount where a delay in fulfilling the goods/service renders the original authorisation invalid (e.g. Split Shipments)	Out of Scope
Resubmission	To resubmit an authorisation for an amount previously declined, when the cardholder has already received the goods/service (prevalent with transit merchants)	Out of Scope
Incremental	To authorise a top up amount, in addition to the amount previously authorised (e.g. adding a tip to a previously authorised taxi fare amount)	Out of Scope
Delayed Charges	To submit an authorisation for a supplemental amount after the original transaction (e.g. hotel mini bar charge after payment already made for room stay)	Out of Scope
Unscheduled	Merchant uses Cardholder Stored Credential to process a transaction for a fixed or variable amount that does not occur on a scheduled or regularly occurring transaction date	Out of Scope
No Show	Cardholder pays a deposit amount and also agrees to guarantee payment for the full amount	✓
	Merchant initiates an authorisation for an amount that the cardholder has guaranteed to pay them (e.g. hotel no show)	Out of Scope

Transaction ID and the Stored Credential Flag are required in some scenarios - please see technical specifications for full details. "Out of Scope": Visa and Mastercard consider these to be out of scope, but could nonetheless be subject to change depending on confirmation by the EBA and other individual regulators. Merchants should therefore make their own independent decision.

Sample scenarios

Scenario	CIT/MIT Action
Storing credential for future use, but no goods purchased	CIT - Account verification with storing of credentials for future use
Storing credential for future use and purchasing goods at same time	CIT - Authorisation with storing of credential for future use
Using stored credentials to purchase goods	CIT - Authorisation using credentials stored for future use
Using a stored credential when wallet value falls below agreed limit	MIT - Authorisation using credentials stored for future use