Stored Credentials

Overview

Verifone's Transactions with Stored Credentials feature allows merchants in selected regions to save, adjust and use cardholder's stored credentials for transactions in certain predefined ways.

How it works

Verifone transactions with stored credentials are currently available for merchants in certain regions. Feel free to reach out to your Sales representative to find out more.

> To use Verifone's Stored Credential feature, the Merchant Entity should be enabled for [Tokenization](#) with Verifone's proprietary Verifone Reuse Token.

Concepts

Term	Definition
Stored Credential	Information including but not limited to a card number or payment token, that is stored by Verifone on the merchant's behalf to process future transactions, such as recurring payments for the cardholder
Cardholder Initiated Transaction (CIT)	Any transaction where the cardholder is actively participating in, such as a Terminal in-store transaction, through an online checkout, or with a stored credential (a.k.a. Card on File, a.k.a. Credential on File, a.k.a. One-click Payment)
Card on File CIT, Credential on File CIT, or a One-click Payment	A Card Not Present Transaction initiated by the cardholder where the cardholder does not need to enter their complete card details. The transaction uses the payment credential previously stored by the cardholder to perform the transaction, such as a transaction using the cardholder's merchant profile.
Merchant Initiated Transaction (MIT)	Any transaction which is initiated by a merchant, without the cardholder actively participating. Such a transaction can be a follow-up transaction to a Cardholder Initiated Transaction (CIT), or the performing of a pre-agreed standing instruction from the cardholder for the provision of goods or services. • **Unscheduled Credential on File** is an MIT using a stored credential for a fixed or variable amount that does not occur on scheduled time intervals where the cardholder has previously provided consent to the merchant.

Term	Definition

Recurring Payments	Transactions done with stored credentials that occur at regular predefined intervals without continual cardholder consent or interaction. The cardholder gives consent for a given series of recurring payments with a merchant once, and the transactions with stored credentials occur until:
	
	• the predefined date term ends, or
	• the pre-agreed number of transactions are reached, or
	• the sum of the amount of all the transactions reaches a pre-agreed total value, or
	    ○ the merchant stops sending subsequent transactions, or
	    ○ until the cardholder revokes their consent (i.e., 'cancels' the recurring payments).

> To utilize the stored credentials feature, you should use a Merchant Site organization with an active Payment Provider Contract and a token scope assigned. Your user should be assigned to the Merchant Site organization to perform the API calls.

Functionality

Verifone's Transactions with Stored Credentials feature is available for the following:

- A Sale, Account Verification, Pre-authorization, or Final-authorization acting as an Initial Transaction (a.k.a Sign-up), where the request to store the cardholder's credentials is submitted to Verifone
- A Sale or Final-authorization acting as a Subsequent Transaction (a.k.a. Charge) where the request uses previously-stored cardholder's credentials is submitted to Verifone

Verifone offers Secure Token Management services; however, the management of stored credentials lifecycle is the responsibility of the merchant. This means that merchants need to manage the lifecycle of the stored credentials outside of the Verifone solution, including but not limited to:

- Sign up for cardholder contracts for storing credentials
- Show and manage the Terms and Conditions for storing credentials
- Obtain and manage the cardholder consent for storing credentials
- Schedule the recurring payments processed with stored credentials
    - Manage the number of recurring payments
    - Manage the sequence of recurring payments
    - Manage the frequency of recurring payments
    - Manage the end date of recurring payments
    - Manage the total transaction amount of recurring payments
    - Manage the transaction amount of individual recurring payments
- Handle Subscription Management activities
- Manage Account Updating activities

Sign-up Transactions functionality

Sign-up transactions are usually CITs. 3DS is mandatory under PSD2 for such transactions.

The merchant needs to create the flow that initiates and sends the transaction that acts as a Sign-up Transaction.

Within Verifone's Stored Credentials framework, the following combinations of stored credentials are possible:

	As a CIT	**As an MIT**
Sign-up Transaction	Processing Model: None Processing Model: Recurring Integration Path: HPP, iFrame, Payment Link, Server-to-Server Payment: Account Verification, Sale, Pre-Authorization, Final-Authorization	Processing Model: None Processing Model: Recurring Integration Path: Virtual Terminal Payment: Pre-Authorization *Note: Regional restrictions apply for MIT and MO/TO Sign-up Transactions*
Charge Transaction	Processing Model: Credential on File Processing Model: Recurring Integration Path: HPP, iFrame, Payment Link, Server-to-Server Payment: Sale, Final-Authorization	Processing Model: Unscheduled Credential on File Processing Model: Recurring Integration Path: Server-to-Server, Virtual Terminal Payment: Sale, Final-Authorization

Note: Regional and Acquirer differences influence the regulatory requirements and fields needed for Stored Credential Transactions.

It is possible to use an existing VF Reuse Token ID for a Sign-up Transaction, in a way that a VF Reuse Token ID created earlier can be used instead of Encrypted Cardholder Data in the transaction that acts as a Sign-up Transaction.

The Processing Model of the Sign-up Transaction determines the Processing Model of the Charge Transactions that can be done later:

- A Sign-up with a Recurring Processing Model can only be followed by a Charge with a Recurring Processing Model
- A Sign-up with a None Processing Model
  - can be followed by a Charge with a Credential on File Processing Model, if the Charge is a Cardholder Initiated Transaction, or
  - followed by a Charge with an Unscheduled Credential on File Processing Model, if the Charge is a Merchant Initiated Transaction

A Charge Transaction must always be referenced to a previous transaction which, depending on the Card Brand used, can either be the Sign-up Transaction, or the previous Charge Transaction.

Charge Transactions functionality

Depending on the Verifone Merchant integration and on how the transactions are submitted, there are four options for how references can be submitted for Charge Transactions.

#	Reference(s)
Option #1	Verifone Stored Credential Reference
Option #2	Verifone Stored Credential Reference Scheme Reference
Option #3	VF Reuse Token ID Scheme Reference
Option #4	VF Reuse Token ID

> Check if **Scheme Reference** is supported by your acquirer implementation by clicking our **Supported acquirers** page.

Charge Transactions can use either of the options interchangeably. Regional and Acquirer differences influence which option(s) can be submitted.

We recommend merchants to use the Verifone Stored Credential Reference for a Charge Transaction. As part of the Verifone Framework for stored credentials, Verifone provides a Verifone Stored Credential Reference after a successful transaction. By using the Verifone Stored Credential Reference, the Scheme Reference is also passed, as long as it exists.

If the merchants want to use Option #2, they need to submit both the Verifone Stored Credential Reference and the Scheme Reference value for a transaction with stored credentials. The Scheme Reference is the reference received from the Card Scheme after a successful transaction.

If the merchants want to use Option #3, they need to submit both the VF Reuse Token ID and the Scheme Reference value for a transaction with stored credentials. Some acquirers might require more References from the Signup than provided in this option. To read more about Verifone Tokens, please see the Verifone Tokenization documentation.

If the merchants want to use Option #4, they need to submit the VF Reuse Token ID for a transaction with stored credentials.

For Payment Cards that are dual-branded cards, the Charge Transaction must be done with the same Brand as was used for the Sign-up Transaction.

Usage

Checkout Service and Ecom Service

The sections below explain the Stored Credential Framework-specific fields that can be submitted via API calls as part of the Checkout Service (HPP, iFrame, Payment Link via API) and as part of the Ecom Service (Server-to-Server) Integration Types.

Stored Credential Transaction with a Card

There are two objects in the Create Checkout Request or in the Create Card Payment Request that relate to the Stored Credential Framework.

One object to be used for a Sign-up Transaction is the `token_preference` object, where the VF Reuse Token-related information can be found. For further details, please see the [Tokenization documentation](#).

The other object is the `stored_credential` object, which contains the fields needed to identify a transaction as a transaction with stored credentials. Please see the parameters contained in that object described in the table below.

Parameter		Description
`first_payment`		(Optional Boolean field in a Sign-up Transaction Request) It can be used to indicate if this Request is the first payment in a series of Stored Credentials Transactions. This field is only required in regions where Acquirers do not support 0-amount Account Verification Transactions, but require merchants to submit minor currency amount transactions as Sign-up Transactions. If the field is set to FALSE, it means that this transaction is just a Sign-up Transaction without a payment intent, meaning that this minor currency amount is not Captured. If the field is set to TRUE, it means that this transaction is a Sign-up Transaction and also a Payment, meaning that this amount is expected to be Captured.
`processing_model`		Defines the Stored Credential processing model to be used for this transaction
`processing_model_details`		Object gives the possibility for the merchant to provide the following details:
	(only in the Checkout Service) `consent_text`	(Optional field in a Sign-up Transaction Request) If sent, the text is displayed to the cardholder alongside a checkbox, to provide merchants a possibility to capture cardholder consent to store their credentials
	`processing_model`	Indicates which Stored Credential Processing Model, from Verifone's Stored Credentials Framework, should be used for this transaction

Parameter		Description
	current_payment_number	(Optional field in the Ecom Service in a Charge Transaction Request) It can be used to indicate what is the sequence number of this transaction in this Stored Credentials Transactions series. Some acquirers refer to this field as 'stndOrdrNo'.
	first_payment_amount	(Optional field in a Sign-up Transaction Request) Some acquirers require this field to be submitted to indicate what is the first payment amount in this Stored Credentials Transactions series
	merchant_signup_code	(Optional field) Some acquirers require this field to be submitted with the predefined signup code between the merchant and the acquirer
	payment_frequency	(Optional field in a Sign-up Transaction Request) Some acquirers require this field to be submitted to indicate what will be the frequency of transactions in this Stored Credentials Transactions series
	total_payment_amount	(Optional field in a Sign-up Transaction Request) Some acquirers require this field to be submitted to indicate what will be the sum transaction amount for all transactions in this Stored Credentials Transactions series
	total_payment_number	(Optional field in a Sign-up Transaction Request) Some acquirers require this field to be submitted to indicate what will be the count of transactions in this Stored Credentials Transactions series
stored_credential_type		Defines whether this transaction is a Sign-up or a Charge, and if it is a Charge, then the following fields can also be sent by the merchant:

Parameter		Description
	reference	The Verifone Stored Credential Reference of the Sign-up Transaction (field to be used to submit the reference as detailed in Option #1). The value to be populated here is what was received in the reference field of the stored_credential object as part of the Verifone response to a successful Sign-up Transaction.
	scheme_reference	The Scheme Reference value (field to be used to submit the reference as detailed in Option #2 or Option #3). The value to be populated here is what was received in the scheme_reference field after a successful transaction which, depending on the Card Brand used, can either be the Sign-up Transaction, or the previous Charge Transaction.

Stored Credential Transaction with a Token

If a merchant would like to use an existing VF Reuse Token ID for a Sign-up Transaction or would like to use Option #3 for a Charge Transaction, then there are two objects in the Create Checkout Request or in the Create Token Payment Request that relate to the Stored Credential Framework.

One object to be used for a Sign-up Transaction is the token_preference object, where the VF Reuse Token-related information can be found. For further details, please see the Tokenization documentation.

The other object is the stored_credential object, which contains the fields needed to identify a transaction as a Transaction with Stored Credentials. Please see the parameters which *differ* from the Stored Credentials specific fields already detailed in the section above described in the table below.

Parameter		Description
reuse_token		Instead of encrypted card details, for the TokenPaymentRequest Body Schema, the VF Reuse Token ID must be submitted
stored_credential_type		Defines whether this transaction is a Sign-up or a Charge, and if it is a Charge, then the following fields can also be sent by the merchant:
	reference	Should not be sent

Parameter		Description
	`scheme_reference`	Which is the Scheme Reference value (field to be used to submit the reference as detailed in Option #3). The value to be populated here is what was received in the `scheme_reference` field after a successful transaction, which, depending on the Card Brand used, can either be the Sign-up Transaction, or the previous Charge Transaction.

Virtual Terminal

The Virtual Terminal documentation explains the Stored Credential Framework-specific fields that can be submitted via UI as MO/TO transactions on the Virtual Terminal Integration Type.

Stored Credentials for Wallets (Apple Pay/ Google Pay)

Stored Credentials for Wallets are supported as long as the acquirer supports both Stored Credentials and Apple Pay/ Google Pay.

To perform a "Sign Up" Apple Pay/Google Pay transaction, the "Initiate a wallet payment using Google Pay or Apple Pay" API endpoint should be used.

To perform a "Charge" Apple Pay/ Google Pay transaction, an "Initiate a card payment" API call should be submitted and use a re-use token as well.

For more information related to wallets, please view Apple Pay and Google Pay pages.

Transactions with Stored Credentials on Verifone Central

It is possible to see Stored Credential-related details for transactions on Verifone Central. Transactions with Stored Credentials can be accessed in the same manner as any other kind of transaction. Through Verifone Central in the Transaction details tab, for every Transaction with Stored Credentials, you can see:

- Type of the transaction as 'Sign-up', or a 'Charge'
- Status of the transaction as 'Stored now'
- Stored Credential Model details of the transaction, as 'Recurring' or 'CIT CoF Payments'
- Reuse Token ID that was created or used for this transaction
- Scheme reference that was provided for this transaction

Stored Credential details

Type
Sign up

Status
Stored now

Model details
Recurring

Re-use Token ID
123e4567-e89b-12d3-a456-426614174000

Scheme reference
123e4567-e89b-12d3-a456-426614174000

You can filter for transactions by:

- Sign-up
- Charge

Use Cases

Processing Model	Transaction Type	Use Case description
Sign-up: Recurring Charge: Recurring	Sign-up: CIT Account Verification Charge: MIT Sale	This scenario can occur when a cardholder visits the merchant's website for the first time, creates an account, and adds the payment method on this account without purchasing any product. The cardholder agrees that the merchant will store their payment details for the use of a given Recurring Payment series (e.g., monthly fees of a gym membership). Any Charge Transactions part of this recurring payment will happen as Merchant Initiated Transactions.
Sign-up: Recurring Charge: Recurring	Sign-up: CIT Sale Charge: MIT Sale	This scenario can occur when a cardholder visits the merchant's website to start with recurring payments (e.g., agrees to pay monthly fees of a gym membership) and agrees that the merchant will store their payment details for future use. The specific use case describes a scenario where the first payment of the recurring payments is also the initial transaction of storing the payment credentials. The cardholder agrees that the merchant will store their payment details for the use of this Recurring Payment series. Any Charge Transactions part of this recurring payment will happen as Merchant Initiated Transactions.

Processing Model	Transaction Type	Use Case description
Sign-up: None Charge: Credential on File	Sign-up: CIT Account Verification Charge: CIT Sale	This scenario can occur when a cardholder visits the merchant's website for the first time, creates an account, and adds the payment method on this account without purchasing any product. The cardholder agrees that the merchant will store their payment details for future use. The next time the cardholder purchases something from the Merchant's website, the Merchant can prompt the use of the already stored credentials for the purchase. Usually, the Merchant shows the first and last digits of the card.
Sign-up: None Charge: Credential on File	Sign-up: CIT Sale Charge: CIT Sale	This scenario can occur when a cardholder visits the merchant's website for the first time to buy a product and agrees that the merchant will store their payment details (either via checking a box on the merchant website or checking a box on Verifone's Hosted Payment Page) for future use. The next time the cardholder visits the merchant's website, the merchant can prompt the use of the already stored credentials for the purchase. Usually, the merchant shows the first and last digits of the card.
Sign-up: None Charge: Unscheduled Credential on File	Sign-up: CIT Account Verification Charge: MIT Sale	This scenario can occur if a cardholder visits the merchant's website for the first time, creates an account, and saves their payment credentials without purchasing any product or service at this point. Later, the merchant offers a subscription product, where the yearly subscription fee can vary. The cardholder agrees that the merchant can use their stored credential for this given subscription product and that the merchant should deduct the fees periodically.

Processing Model	Transaction Type	Use Case description
Sign-up: None Charge: Unscheduled Credential on File	Sign-up: CIT Sale Charge: MIT Sale	This scenario can occur if a cardholder visits the merchant's website to buy a recurring product or service. During checkout, the cardholder agrees that the merchant can save and use their stored credential for future purchases in relation to this recurring product or service and that the merchant should deduct the costs periodically.
Sign-up: Unscheduled Credential on File Charge: Unscheduled Credential on File	Sign-up: CIT Sale Charge: MIT Sale	This scenario can occur if a cardholder visits the merchant's website to buy a recurring product or service. During this transaction the cardholder sign ups for unscheduled payments and during checkout agrees that the merchant can save and use their stored credential for future purchases in relation to this recurring product or service and that the merchant should deduct the costs periodically.
Sign-up: None Charge: Re-authorization	Sign-up: CIT Account Verification/ Pre-Authorization/ Authorization/ Sale Charge: MIT Pre-Authorization/ Authorization/ Sale	This scenario can occur when a cardholder reserves a product in advance, such that the shipment will be made later in the future. The order placement (Sign-up) consists of an account verification, with the payment being made when the product is shipped (Charge Re-authorization). Other scenarios: split shipments, stay hotels, car rentals, etc.