Secure Card Capture Key

Overview

Verifone provides multiple options to integrate to the eCommerce services: Checkout as a Hosted Payments Page (HPP), Checkout as an iFrame, and your own payment forms to capture card data.

For all solutions, both Verifone and you (as a merchant) need to send the card or other sensitive data in a secure way. To encrypt card details or other sensitive data, Verifone gives you the possibility to generate a private-public key pair, called **Secure Card Capture Key**.

Availability

Available to all merchants integrating with Verifone's eCommerce services.

Mandatory on accounts that are using the v2 card capture method and flow as the API cannot be used without a Secure Card Capture Key.

Secure Card Capture Key

A Secure Card Capture Key consists of:

- a public key, accessible to you to use for encryption
- a private key, only accessible to Verifone, to use for decryption
- a public key alias, to allow Verifone to match the Secure Card Capture Key to be used for decryption when a Transaction is processed.

At least one Secure Card Capture Key needs to be generated for the Organization for which encrypted card details will be needed (typically, this means the Organization with which card payments will be done).

To start accepting eCommerce card payments, you must create a public key for Secure Card Capture. The public key for Secure Card Capture ensures any card details are encrypted in the browser, so that information can be safely passed from you (merchant) to Verifone.

> The public key for the Secure Card Capture can be created only by a merchant with an Admin role, or by a Verifone Admin on behalf of the merchant.

Cardholder encryption card API parameters

The cardholder data encrypted using the Verifone provided public key. This needs to be provided in base64 encoded format.

The data to encrypt is a JSON with possible tags being cardNumber, sequenceNumber, cardholderName, startMonth, startYear, expiryMonth, expiryYear, cvv. This should be a single JSON line and should not contain any spaces.

Additionally, a tag called captureTime must be presenting indicating the time the card was captured in UTC in format RFC 3339, section 5.6. eg. 2019-08-24T14:15:22Z. Encrypted card is valid for only 15 minutes.

Parameter name	Required/Optional	Description

cardNumber	Required	Primary account number (PAN), the card identifier found on payment cards. Numeric value with no spaces or separators allowed between the digits.
sequenceNumber	Optional	The sequence number is the field which can uniquely identify a card. When two or more cards have the same card number, this field helps to make the distinction between the cards.
expiryMonth	Required	Numeric value with length 2. e.g., March -> 03
expiryYear	Required	Numeric value with length 4, e.g., 2028 -> 2028
cvv	Optional	Numeric value with length 3 or 4
cardholderName	Optional	<= 30 characters, the card holder name as it appears on the card
startMonth	Optional	Numeric value representing the month when the card was issued
startYear	Optional	Numeric value representing the year when card was issued
captureTime	-	The time the card was captured in UTC in format RFC 3339, section 5.6. eg. 2019-08-24T14:15:22Z.

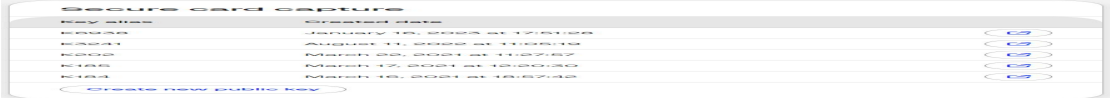
Generate a Secure Card Capture Key

You can generate a Secure Card Capture Key if you have a Merchant Admin role, either via Verifone Central or via API.

Generate a Secure Card Capture Key via Verifone Central

Follow these steps to generate a Secure Card Capture Key via Verifone Central.

1. Log in to your Verifone Central account.
2. Navigate to **Administration** → **Organization Company and Sites**, and select the required organization.
3. Scroll down to the bottom of the page to see the **Secure Card Capture** area.
4. Click on the **Create new public key** button.



Generate a Secure Card Capture Key via API

Follow these steps to generate a Secure Card Capture Key via API.

1. Authenticate as a Merchant Admin user and make sure this role is linked to the Organization for which you want to generate a Secure Card Capture Key.
2. Send the Generate Key Pair POST call.

There is no limit on how many Secure Card Capture Keys an Organization can have.

The public key and public key alias

The public key and the public key alias of a Secure Card Capture can be viewed anytime either via Verifone Central or via API.

View a public key via Verifone Central

Follow these steps to view a public key for Secure Card Capture via Verifone Central.

1. Navigate to *Administration -> Organization Company and Sites.*
2. Select the Organization for which to view the Secure Card Capture Key(s).
3. Scroll down to the bottom of the page to see the **Secure Card Capture** section where all the available Secure Card Capture Key(s) are displayed.

View a public key via API

1. Authenticate as a Merchant Admin user and make sure this role is linked to the Organization for which you want to view the Secure Card Capture Key(s).
2. Send the List Key Pair GET call.
3. Send the Deactivate Key Pair call to deactivate the linked Secure Card Capture Key(s).

Any commercially available encryption tools can be used to encrypt card details with the Verifone Secure Card Capture Key. Verifone uses openpgpjs NPMJS's JS Library on client for the cryptography of the encrypted Card data to be encrypted by the merchant prior to connecting to Verifone's GSC. The actual cryptography itself is Elliptic Key Cryptography, achieving the same level of security as OAEP, but with much smaller key sizes and hence requiring less computing power.

Once this is done, you can start performing integration tests. By using the API Keys you created, you can authenticate with our Checkout API or eCommerce API.