

X-Payments:Encryption keys

X-Payments user manual

1. X-Payments:General information
 - ◆ How It Works
 - ◆ Key features
2. What's New
 - ◆ What's New in X-Payments 3.1
 - ◆ What's New in X-Payments 3.0
3. System requirements
 - ◆ System requirements for X-Payments 3
 - ◆ System requirements for X-Payments 2.2
4. Installation
 - ◆ Installing X-Payments
 - ◆ Setting up file permissions for X-Payments
 - ◆ Getting started with X-Payments
5. Two-factor user authentication
 - ◆ Two-factor authentication (X-Payments 3)
 - ◆ Managing PIN codes (X-Payments 2.2 and earlier)
6. Configuring X-Payments
 - ◆ General settings
 - ◆ Online stores
 - ◆ Payment configurations
 - ◆ Encryption keys
 - ◆ 3D-Secure settings
 - ◆ KOUNT Antifraud screening
 - ◆ NoFraud fraud prevention
 - ◆ Signifyd fraud protection and chargeback prevention
 - ◆ Developer mode
7. Managing users
8. Customizing the interface
 - ◆ Customizing the interface (X-Payments 3)
 - ◆ Customizing the interface (X-Payments 2.2 and earlier)
9. Managing payments
10. Uninstalling X-Payments
11. Upgrading
12. Moving X-Payments from one host to another
13. Viewing X-Payments logs
14. FAQ
15. Troubleshooting
16. Glossary
17. Supported payment gateways
 - ◆ Payment gateways supported by X-Payments 3.1
 - ◆ Payment gateways supported by X-Payments 3.0
 - ◆ Payment gateways supported by X-Payments 2.2

X-Payments uses two types of encryption keys:

- "Store" encryption keys;
- Cardholder data encryption keys.

Contents

- 1 "Store" encryption keys
- 2 Cardholder data encryption keys
- 3 Cardholder data encryption key preferences
- 4 Viewing cardholder data encryption key status
- 5 (Re)generating cardholder data encryption keys
- 6 Re-encrypting stored cardholder data with new encryption keys
- 7 Removing outdated cardholder data encryption keys

"Store" encryption keys

Encryption keys of this type ensure the security of communication between X-Payments and the online stores connected to it. They are generated specifically for each online store that needs to be connected to X-Payments and can be found on the "'Store" encryption keys' page ('Online store details' page -> [View online store encryption keys](#) link). These keys must be stored securely and re-generated by X-Payments admin regularly, at least monthly. Information on the cryptographic algorithm employed to secure the communication between X-Payments and online stores is available here: [Public-key cryptography](#).

To re-generate "Store" encryption keys, use the **Re-generate keys** button on the "'Store" encryption keys' page:

"Demo store (lite interface)" encryption keys

[← Back to "Demo store \(lite interface\)" details](#)

To decrypt requests from the shopping cart X-Payments uses a pair of keys. The public key is stored on the shopping cart side and is included in the requests from the shopping cart to X-Payments. The private key is securely stored on the X-Payments side. The shopping cart request to X-Payments must contain the shopping cart ID and some request-specific information (request body), encrypted with the public key. X-Payments receives this request, identifies it by the shopping cart ID and uses an appropriate private key to decrypt the request body.

The responses, generated by X-Payments to requests of the shopping cart or callback requests to the shopping cart also require encryption. To decrypt requests from X-Payments, the shopping cart must use the private key and a password that is used to decrypt the private key. The private key and password must also be securely stored on the shopping cart side.

Make sure these keys cannot be accessed without authorization. Regenerate keys regularly, at least monthly.

Public key (Shopping cart → X-Payments) This key is used to encrypt data, sent to X-Payments from the shopping cart.

```
-----BEGIN CERTIFICATE-----
MIIEtjCCAzagAwIBAgIBADANBgkqhkiG9w0BAQQFADB8MQswCQYDVQQGEwJVUzEN
MAsGA1UECBMEbm9uZTENMAsGA1UEBxMEbm9uZTENMAsGA1UEChMEbm9uZTENMAsG
A1UECxMEbm9uZTENMAsGA1UEAxMEbm9uZTEIMCAGCSqGSIb3DQEJARYTdW5rYm93
bkBlcGFtcG9uZTENMAsGA1UEFw0xMjEwMTcwNTM0NTVaFw0xMzEwMTcwNTM0NTVaMHwx
```

[Re-generate keys](#)



For X-Cart stores, the new encryption codes need to be copied and pasted into the appropriate fields in the admin area of the X-Cart store (Payment Methods ? Credit Card ? X-Payments connector module settings). See [how to configure X-Cart Connector](#).

For Magento stores, the entire configuration bundle needs to be updated, i.e. copied from the Magento shop configuration page in the X-Payments admin backend, then pasted and deployed on the X-Payments configuration page in the Magento admin backend.

Cardholder data encryption keys

Encryption keys of this type ensure the security of cardholder data stored by X-Payments - when X-Payments is configured to store cardholder data.

If you are going to store cardholder data in X-Payments, after enabling the option **Store cardholder data** in [X-Payments General settings](#), you will need to have a set of cardholder data encryption keys generated for your X-Payments installation. Unlike "store" encryption keys, cardholder data encryption keys are not displayed anywhere within the X-Payments user interface, so you will not be able to see them. However, you will need to make sure these keys exist in the system and are re-generated regularly. This is really easy because you will have to "tell" X-Payments to generate a set of cardholder data encryption keys only for the very first time; after this, you will be able to configure X-Payments to re-generate the keys automatically once in a set period of time. Re-generation of cardholder data encryption keys will be done as a cron job (based on running cron.php). You will also have the ability to re-generate the keys at any time manually should it be needed. To make sure the keys are actually re-generated at expected times, you will be able to view the encryption key generation history for your X-Payments installation and to configure X-Payments to notify you about such events as upcoming expiration of current cardholder data encryption keys and successful generation of new encryption keys.

In the X-Payments back end, cardholder data encryption keys are managed using the 'Encryption keys' page (Settings -> Encryption keys).

On this page you can:

- Adjust your cardholder data encryption key preferences (key time-to-live, frequency of re-generation, notifications, etc);
- (Re)generate cardholder data encryption keys;
- Find out the current status of cardholder data encryption keys for your X-Payments installation;
- Re-encrypt stored cardholder data using new encryption keys;
- Delete outdated encryption keys.

Cardholder data encryption key preferences

The encryption key preferences for your X-Payments installation can be adjusted using the 'Cardholder data encryption keys' section:

Encryption key settings

Key time-to-live: days

Regenerate keys days prior to key expiration date

Notify days prior to the key expiration date

Send notifications on key generation to email

Save

- Key time-to-live (days): Enter the number of days for which cardholder data encryption keys will be valid. After the number of days specified here the keys will expire.
- Regenerate keys X days prior to key expiration date: Specify how many days before the expiration date you want the encryption keys to be automatically re-generated. This setting is needed so that you will still have time to re-generate your keys if your keys are not re-generated at expected time (for example, if cron fails).
- Notify Y days prior to the key expiration date: Specify how many days before the expiration of your cardholder data encryption keys you want to be notified about the upcoming key expiration.
- Notify on key generation: Specify whether you want to be notified when cardholder data encryption keys are re-generated.
- Send notifications to email: Enter the email address for cardholder data encryption keys expiration notifications. If you fail to provide an email address here, the notifications will only be displayed in the X-Payments Dashboard.

Viewing cardholder data encryption key status

Before any encryption keys have been generated, or after you have removed all active keys, the 'Encryption keys' page displays a message saying that you have no active keys:

If you already have cardholder data encryption keys in the system, the 'Encryption keys' page shows information about the currently stored keys:

For each set of keys the following information is available:

- time of creation;
- whether the keys were generated by admin or automatically;
- key status;
- time until when the keys will be valid / time when the keys expired;
- whether there is any stored cardholder data in the system that is encrypted using these keys (*Has encrypted data / Has no encrypted data*).

Possible key statuses:

- **Active**
- **Expired** (automatically replaced by new keys after their time-to-live had expired)
- **Canceled** (re-generated by admin before the expiration of their time-to-live period)

(Re)generating cardholder data encryption keys

One of the actions that need to be completed to enable X-Payments to store cardholder data is generate cardholder data encryption keys.

To generate new cardholder data encryption keys:

1. Go to the 'Encryption keys' page in the X-Payments back end (Settings -> Encryption keys).
2. Click the **Generate new keys** button.

A new set of cardholder data encryption keys will be generated. You will see a new record with information about the new set of keys added to the list on the 'Encryption keys' page. From this moment the new set of encryption keys will be used to encrypt any new data being saved in X-Payments.

Do not forget to copy the new encryption codes and paste them into X-Cart in the appropriate fields (Payment Methods ? Credit Card ? X-Payments connector module settings, see [how to configure X-Cart Connector!](#))

Re-encrypting stored cardholder data with new encryption keys

If you already had active cardholder data encryption keys in the system when you re-generated your keys, the status of those keys will be changed to "Canceled". Stored cardholder data that was encrypted using those keys will remain encrypted with those keys. Any data that will be saved *after* the re-generation of the keys will be encrypted using the new keys. To re-encrypt all stored data using your new keys, click the **Reencrypt data** button.

Note: The 'Reencrypt data' button is not displayed if there is no encrypted cardholder data.

Removing outdated cardholder data encryption keys

You can remove any cardholder data encryption keys you no longer need. Please note that removing a key set that has encrypted data will result in deleting the encrypted data. To remove a set of cardholder data encryption keys:

- X-Payments 2.0 and later: Click the **Delete** button opposite the set of keys you want to remove.


Cardholder data encryption keys

Generate new keys

Generated **Nov 1, 2013 08:40:38** by [admin](#) Active Delete

Valid until **Dec 1, 2013 08:40:38** (29 days left) Has no encrypted data

Confirm the deletion.

- X-Payments 1.0: Click the Delete icon  opposite the set of keys you want to remove.

Cardholder data encryption keys

Generate new keys

Generated **Nov 28, 2009 21:44:06** by [Administrator](#) ✓ active Delete

Valid until **Dec 28, 2009 23:59:59** (28 days left)

Confirm the deletion.



This article can be [downloaded as a PDF file](#)