Creating and Using Security Keys

Restricted Rights Legends

For Government or defense agencies: Use, duplication, or disclosure by the Government or defense agencies is subject to restrictions as set forth the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and in similar clauses in the FAR and NASA FAR Supplement.

For civilian agencies: Use, reproduction, or disclosure is subject to restrictions set forth in subparagraphs (a) through (d) of the Commercial Computer Software Restricted Rights clause at 52.227-19 and the limitations set forth in Cybersource Corporation's standard commercial agreement for this software. Unpublished rights reserved under the copyright laws of the United States.

Trademarks

Authorize.Net, eCheck.Net, and The Power of Payment are registered trademarks of Cybersource Corporation. Cybersource, Cybersource Payment Manager, Cybersource Risk Manager, Cybersource Decision Manager, and Cybersource Connect are trademarks and/or service marks of Cybersource Corporation. Visa, Visa International, Cybersource, the Visa logo, and the Cybersource logo are the registered trademarks of Visa International in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Version: 21.02
Contents

Recent Revisions to This Document.......................................................... 4
About This Guide....................................................................................... 5
Using the Dashboard................................................................................ 6
REST API Keys........................................................................................... 7
  Creating a REST API Key........................................................................ 7
Simple Order API Keys.............................................................................. 9
  Creating a Simple Order API Key.......................................................... 9
Secure Acceptance Keys.......................................................................... 10
  Creating a Secure Acceptance Key......................................................... 10
SOAP Toolkit Keys.................................................................................. 12
  Creating a SOAP Toolkit Key............................................................... 12
PGP Keys.................................................................................................. 13
  Creating PGP Keys................................................................................ 13
  Adding a PGP Key to Your Account....................................................... 14
  Business Center User Permissions....................................................... 14
    Granting User Permissions................................................................. 14
Message-Level Encryption Keys............................................................... 16
  Creating a Message-Level Encryption Key.......................................... 16
Using Meta Keys....................................................................................... 17
Searching for Keys and Filtering Results.................................................. 18
  Searching for Keys............................................................................... 18
  Filtering and Sorting Key Search Results............................................. 18
Deleting Keys............................................................................................ 19
Deactivating Keys..................................................................................... 20
Recent Revisions to This Document

Version 21.02

Added the following:

• Meta Keys (on page 17)
• Searching for Keys and Filtering Results (on page 18)
• Deactivating Keys (on page 20)
• Deleting Keys (on page 19)

Version 21.01

• Procedures were rewritten to reflect the more streamlined flow of the Cybersource Business Center Key Management page.

Version 18.01

• Updated the procedure for generating a Simple Order API security key.

Version 16.02

• Updated the Java browser plug-in version requirement.

Version 16.01

• Added the duration of the Simple Order security key.
About This Guide

This section describes the structure and content of this guide.

Audience and Purpose

This guide is written for application developers who want to use Cybersource services that require a security key, including API requests.

Related Documentation

Refer to the Support Center for complete technical documentation: http://www.cybersource.com/support_center/support_documentation

Customer Support

For support information about any service, visit the Support Center: http://www.cybersource.com/support
Using the Dashboard

When you log in to the Business Center, the dashboard appears. You can use the Expiring Keys dashboard to view any keys that will expire soon. You can click **View All Keys** to go directly to the Key Management page, or click **Generate new key** to create a new key.
REST API Keys

The Cybersource REST API uses public key cryptography to securely exchange information over the Internet. Before you can send requests for Cybersource services using the REST API, you must create a security key for your Cybersource merchant account on the Business Center.

The REST API supports two types of security key:

- Shared secret key for using HTTP Signature authentication
- P12 certificate for using JSON Web Token authentication

REST API keys expire after 3 years.

Security keys can be used to make any call, including payments. Treat your security keys as you would any secure password.

You must use separate keys for the test and production environments.

For more information about REST API authentication, see the Developer Center's Authentication section.

Creating a REST API Key

To create a REST API key:

1. Log in to the Business Center:
   - Test Environment: https://ebc2test.cybersource.com/ebc2
   - Production Environment: https://ebc2.cybersource.com/ebc2

2. On the left navigation panel, click the Payment Configuration icon.

3. Click Key Management.
   The Key Management page appears.

4. Click Generate Key.
   The Create Key page appears.

5. Select the type of REST key that you want, and click Generate Key.

6. Follow the sub-step below that corresponds to the key you selected.
• **REST Shared Secret:** copy the generated key to your clipboard by clicking the clipboard icon, or click **Download key** to download the shared secret. The first value is the key and the second value is the shared secret.

• **REST Certificate:** click **Download key** to download the certificate.
Simple Order API Keys

The Simple Order API uses public key cryptography to securely exchange information over the Internet. Before you can send requests for Cybersource services using the Simple Order API, you must go to the Business Center and create a security key for your Cybersource merchant account.

Simple Order API keys expire after 3 years.

Security keys can be used to make any call, including payments. Treat your security keys as you would any secure password.

You must use separate keys for the test and production environments.

Creating a Simple Order API Key

To create a Simple Order API key:

1. Log in to the Business Center.
   - Test Environment: https://ebc2test.cybersource.com/ebc2
   - Production Environment: https://ebc2.cybersource.com/ebc2
2. On the left navigation panel, click the Payment Configuration icon.
3. Click Key Management.
   The Key Management page appears.
4. Click Generate Key.
   The Create Key page appears.
5. Select Simple Order API and click Generate Key.
6. Click Download key to download the .p12 file.
Secure Acceptance Keys

The Cybersource Secure Acceptance API uses public key cryptography to securely exchange information over the Internet. Before you can send requests for Cybersource services using the Secure Acceptance, you must go to the Business Center and create a security key for your Cybersource merchant account.

Secure Acceptance keys expire after 2 years.

Security keys can be used to make any call, including payments. Treat your security keys as you would any secure password.

You must use separate keys for the test and production environments.

Creating a Secure Acceptance Key

To create a Secure Acceptance key:

1. Log in to the Business Center.
   • Test Environment: https://ebc2test.cybersource.com/ebc2
   • Production Environment: https://ebc2.cybersource.com/ebc2

2. On the left navigation panel, click the Payment Configuration icon.

3. Click Key Management
   The Key Management page appears.

4. Click Generate Key
   The Create Key page appears.

5. Select Secure Acceptance and click Generate Key.

6. Enter the required information:
   • Key Name: enter a name for this key.
   • Signature Version: select 1 from the drop-down menu.
   • Signature Method: select HMAC-SHA256 from the drop-down menu.
   • Security Profile: select a security profile from the drop-down menu.
7. Click **Generate Key**. You can copy the access key and secret key by clicking the clipboard icons, or click **Download key** to download a text file containing both keys.
SOAP Toolkit Keys

The Cybersource SOAP Toolkit uses public key cryptography to securely exchange information over the Internet. Before you can send requests for Cybersource services using the SOAP Toolkit, you must go to the Business Center and create a security key for your Cybersource merchant account.

SOAP Toolkit keys expire after 3 years.

Security keys can be used to make any call, including payments. Treat your security keys as you would any secure password.

You must use separate keys for the test and production environments.

Creating a SOAP Toolkit Key

To create a SOAP Toolkit key:

1. Log in to the Business Center.
   - Test Environment: https://ebc2test.cybersource.com/ebc2
   - Production Environment: https://ebc2.cybersource.com/ebc2

2. On the left navigation panel, click the Payment Configuration icon.

3. Click Key Management.
   The Key Management page appears.

4. Click Generate Key.
   The Create Key page appears.

5. Select SOAP Toolkit and click Generate Key.

6. You can copy the generated key to your clipboard by clicking the clipboard icon, or click Download key to download the key.
PGP Keys

Cybersource uses PGP encryption for Account Updater response files and Notice of Change (NOC) reports. For information about Account Updater, see the Account Updater User Guide. For information about NOC reports, see Electronic Check Services Using the Simple Order API.

A PGP public/private key pair enables you to use encryption to protect payment data. You exchange the public part of this key pair with Cybersource, which uses the public key to encrypt response files or NOC reports. You use the private part of the key pair to decrypt the response files or NOC reports. Only the private key can decrypt files that are encrypted with the public key.

PGP keys expire after 3 years.

Security keys can be used to make any call, including payments. Treat your security keys as you would any secure password.

You must use separate keys for the test and production environments.

Creating PGP Keys

You can use any OpenPGP-compliant software to generate PGP keys. The key you generate must be an RSA key. The following free OpenPGP solutions are available:

- Bouncy Castle
- GPG4WIN

Cybersource recommends that you do the following:

- Make the key at least 2048 bits long.
- Store the private key in an encrypted format to protect it from unauthorized use.
- Back up the private key in case of disaster.

Place the backup of the private key on removable media, and lock it in secure storage.

Cybersource does not receive a copy of your private key and cannot decrypt files that are encrypted with your public key. After you create a public/private key pair, add the public key to the Business Center as described in the next section.
Adding a PGP Key to Your Account

To add a PGP key to your account:

1. Log in to the Business Center.
   - Test Environment: https://ebc2test.cybersource.com/ebc2
   - Production Environment: https://ebc2.cybersource.com/ebc2

2. On the left navigation panel, click the **Payment Configuration** icon.

3. Click **Key Management**.
   The Key Management page appears.

4. Click **Generate Key**.
   The Create Key page appears.

5. Select **PGP** and click **Generate Key**.

6. Enter the ASCII string into the text field, and click **Create Key**.

Business Center User Permissions

A user account in the Business Center requires certain permissions to work with PGP keys and the Account Updater request files and reports.

Granting User Permissions

To grant user permissions:

1. Log in to the Business Center.

2. In the left navigation pane, choose **Account Management > Roles**.

3. Choose the role assigned to the user account that needs to work with PGP keys and click the **Edit** icon.

4. In the Role Editor, select the following permissions:
   
   a. Under Credit Card Account Updater Permissions, choose **View Status**. This option enables the user to view the status of uploaded Account Updater request files and NOC reports.

   b. Under Merchant Settings Permissions, choose **PGP Security Settings**. This option gives the user permission to upload, activate, and deactivate encryption keys.
c. Under Reporting Permissions, choose **Report Download**. This option gives the user permission to download Account Updater response files and NOC reports.

5. At the bottom of the Role Editor, click **Save**.
Before you can send requests for Cybersource services using message-level encryption, you must go to the Business Center and create a security key for your Cybersource merchant account.

Message-level encryption keys expire after 3 years.

Security keys can be used to make any call, including payments. Treat your security keys as you would any secure password.

You must use separate keys for the test and production environments.

Creating a Message-Level Encryption Key

To create a message-level encryption key:

1. Log in to the Business Center.
   • Test Environment: https://ebc2test.cybersource.com/ebc2
   • Production Environment: https://ebc2.cybersource.com/ebc2

2. On the left navigation panel, click the Payment Configuration icon.

3. Click Key Management.
   The Key Management page appears.

4. Click Generate Key.
   The Create Key page appears.

5. Select Message-Level Encryption and click Generate Key.

6. Enter the string into the text field, and click Create Key.
Using Meta Keys

When using a portfolio account, you have the option to create a meta key. A meta key is a key that you assign to more than one merchant account. To assign a key as a meta key:

1. During the Create Key procedure, select a key type and click Generate.

2. Choose one of the following:
   - To assign this key to all accounts in the current portfolio, choose All current and future Merchant IDs, click Create key, and continue to the Create Key page.
   - To assign this key to a specific merchant or group merchants, choose Custom Merchant ID selection, click Create key, and continue to Step 3.

3. Click + Add custom merchant ids. The Add Custom Merchant IDs page appears. By default, all merchant IDs are shown in the Merchant IDs table. To limit the list to a subset of merchant IDs, click + Add filter, select a search filter from the drop-down menu, and click Search.

4. Use the check boxes to select one or more merchant accounts, and click Submit. You are returned to the Key Generation page.

5. Click Create key. Continue to the Create Key page.
Searching for Keys and Filtering Results

When your account contains a large number of keys, it might be necessary to sort them using the search function and then filter the search results.

Search (on page 18)

Filter (on page 18)

Searching for Keys

You can search for keys by using the Search options.

1. Click the **Key Type** drop-down menu and select a key type (required).
2. Click the **Created At** drop-down menu and select a date range (required). To choose a custom date, select **Custom Date**. Choose the start date, end date, start time, and end time.
3. To add a custom search option, click **Add filter** and choose a filter from the drop-down menu. A new drop-down menu appears based on your choice, from which you can choose additional options.
4. Click **Search**.
   Results are displayed in the table below the search options. To reset the search, click **Reset Search**.

Filtering and Sorting Key Search Results

Large sets of search results can be sorted and filtered in the table of keys.

To sort the results of a column, click the column heading. Columns with alphanumeric data sort alphabetically from A-Z or Z-A. Columns with numbers will filter from greatest to smallest or smallest to greatest. The Delete column is not sortable.

To filter results within a column, enter a small amount of text in the **Filter** field. Only keys that match the filter text are returned. To reset the search, click **Reset Search**.
Deleting Keys

You can delete a key when you no longer need to use it for payment processing.

Keys become inactive after reaching the expiration date.

To delete security keys:

1. On the left navigation panel, click the payment configuration icon.
2. Click Key Management. The Key Management page appears.
3. In the table of keys, find the key that you want to delete, and click the Delete (>Delete) icon in the row for that key.
4. Click Yes.
Deactivating Keys

You can deactivate a key if you no longer need to use it. You can only deactivate MLE, PGP, or Secure Acceptance keys.

Keys become inactive after reaching the expiration date.

To deactivate security keys:

1. On the left navigation panel, click the Payment Configuration icon.

2. Click Key Management. The Key Management page appears.

3. Find the key in the table of keys, or search for one using the search filters, and click the link for that key in the Keys column. The Key Information page appears.

4. Click the Deactivate (.solve) icon.

5. Click Yes.