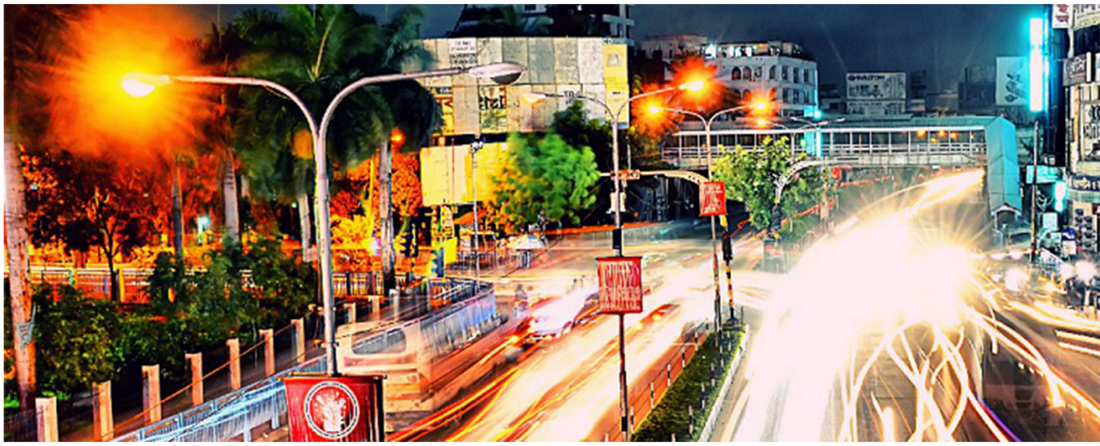
Creating and Using Security Keys

User Guide

cybersource
A Visa Solution



Restricted Rights Legends

Trademarks

Version: 21.01

Contents

Recent Revisions to This Document

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 also click **View All Keys** to go directly to the Key Management page, instead of using the navigation menu.

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.
    - **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.**

Message-Level Encryption Keys

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**.