Creating and Using Security Keys

May 2013

CyberSource®
the power of payment

CyberSource Corporation HQ | P.O. Box 8999 | San Francisco, CA 94128-8999 | Phone: 800-530-9095

CyberSource Contact Information

For general information about our company, products, and services, go to http://www.cybersource.com.

For sales questions about any CyberSource Service, email sales@cybersource.com or call 650-432-7350 or 888-330-2300 (toll free in the United States).

For support information about any CyberSource Service, visit the Support Center at http://www.cybersource.com/support.

Copyright

Restricted Rights Legends

Trademarks

Contents

Recent Revisions to This Document

Release	Changes
May 2013	Updated Simple Order API and SCMP API chapters to include 2048-bit keys and Copy Key functionality.
January 2013	First release of this document.

About This Guide

Audience and Scope

The audience for this guide is merchants or developers who want to create or update the security key for:

- Simple Order API
- SCMP API
- Account Updater
- Notice of Change (NOC) reports

Related Documents

- Simple Order API Client Developer Guides
- SCMP API Client Developer Guides
- *Credit Card Services Using the Simple Order API*
- *Credit Card Services Using the SCMP API*
- *Account Updater User Guide*
- *Electronic Check Services Using the Simple Order API*
- *Electronic Check Services Using the SCMP API*

Information About other Security Keys

For information about SOAP Toolkit security keys, see the *CyberSource Toolkits for Web Services Developer Guide*.

For information about Hosted Order Page security keys, see the *CyberSource Hosted Order Page User Guide*.

For information about Silent Order POST security keys, see the *Cybersource Silent Order POST User Guide*.

For information about Secure Acceptance Silent Order Post security keys, see the *Secure Acceptance Silent Order Post Development Guide*.

Conventions

Note

A *Note* contains helpful suggestions or references to material not contained in this document.

Important

An *Important* statement contains information essential to successfully completing a task or learning a concept.

CHAPTER 1

Simple Order API Security Keys

Generating Transaction Keys

The CyberSource 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 create a security key for your CyberSource merchant account on the Business Center.

Note The Business Center uses a Java applet to generate security keys. The Java applet requires version 1.4.1 or later of the Java browser plug-in. If the applet fails to load properly, CyberSource recommends that you install the latest version of your browser and try again.

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

To generate a security key:

Step 1 Log in to the Business Center.

Step 2 In the left navigation panel, choose **Account Management** > **Transaction Security Keys**.

Step 3 In the Transaction Security Keys window, click **Security Keys for the Simple Order API**.

Step 4 In the Security Keys for the Simple Order API window, click **2048-Bit Key**.

Note Clicking **2048-Bit Key** causes the Java applet on the Business Center web site to download 1.5 megabytes of executable code that is used to generate the certificate request in the next step. The download may take several minutes.

Step 5 In the New Security Key window, click **Generate Certificate Request**.
A warning message may appear.

Step 6 In the warning message window, verify that the certificate is signed by CyberSource, and click the appropriate option to dismiss the message.

While the new key is generated, messages appear in the Messages text box. Your browser then opens a Save As dialog box.

Step 7 In the Save As dialog box, navigate to a safe location for your key, which is named **<merchant ID>.p12**. Be sure to use separate locations for the test and production environments. Be careful not to overwrite a key in the wrong directory.

Important If you do not protect your security keys, the security of your CyberSource account may be compromised.

After you save the security key, the Messages text box in the New Security Key window displays the following messages:

```
Generating the certificate request. This may take several seconds.
Certificate request generated successfully.
Encoding the certificate request.
Certificate request encoded successfully.
Processing the certificate request. This may take several seconds.
Certificate request processed successfully.
Creating the key file contents.
Key file contents created successfully.
Please select a save location for your key file using the popup dialog.
Writing the key file to the filesystem.
Writing the key file to C:\Users\username\Documents\EBC_
test\username.p12.
Key file written to the filesystem successfully.
The password for the key file is your merchant id: <merchantid>.

The Certificate Manager has successfully completed all operations.
```

The last message indicates that the operation finished successfully.

Step 8 To verify that the key is active, go to the left navigation panel and choose **Transaction Security Keys**, and then click **Security Keys for the Simple Order API**.

The new key should be listed at the bottom of the table in the Security Keys for the Simple Order API window.

Verifying Serial Numbers

In the Business Center, you can view a list of the keys that you have generated. However, the keys are listed by their serial number, but not by their file name. If you are unsure which one of your keys is the active key that is recognized by CyberSource, you can view the serial numbers for your locally stored key files. Then you can match the locally stored keys with the information shown in the Business Center.

To import a key file and view its serial number in a Windows environment, follow these steps.

To import the key File:

Step 1 Find and double-click the key file.

The Certificate Import Wizard opens.

Step 2 Click **Next**.

The Wizard shows the path to the key file.

Step 3 Click **Next**.

Step 4 Type the password for the key file.

The password is the merchant ID that you used to log into the Business Center to generate the key.

Step 5 Clear all check boxes.

Step 6 Click **Next**.

Step 7 Ensure that the **Automatically select the certificate store based on the type of certificate** check box is checked.

Step 8 Click **Next**.

Step 9 Click **Finish**.

A warning appears.

Step 10 In the warning message dialog box, click **Yes**.

A success message appears.

Viewing the Serial Number

These instructions are written for Internet Explorer 9. Modify them as needed for your browser.

To view the serial number:

Step 1 Open Internet Explorer.

Step 2 Click the **Tools** icon in the upper right corner of the browser, and then click **Internet Options**.

Step 3 In the Internet Options window, click the **Content** tab.

Step 4 In the Certificates area of the window, click **Certificates**.

The Certificates window shows a list of the certificates that have been imported.

Step 5 Double-click the key file that you imported in the previous section.

The Certificate window for that file opens.

Step 6 Click the **Details** tab.

The window shows a list of fields and values, but the Serial Number field does not contain the correct serial number information. Instead, the Subject field contains the correct information.

Step 7 Click the **Subject** field.

The lower window displays the serial number for the key file.

Copying Keys

You can copy the key that you tested in the test environment to the live environment. The copied key will expire in the test environment after 30 days.

To copy keys from the test environment to the live environment:

Step 1 From the Security Keys for the Simple Order API page, check the box next to the keys that you want to copy.

Step 2 Click **Copy Keys**.

Step 3 Click **OK** in the warning screen that pops up.

Verify the keys in the Live Business Center.

CHAPTER 2

SCMP API Security Keys

Generating Transaction Keys

The CyberSource SCMP API uses public key cryptography to securely exchange information over the Internet. Before you can send transactions to CyberSource by using the SCMP API, you must log in to the Business Center to create and download the following transaction keys for your merchant account:

Table 1 SCMP Transaction Key Files

Files Name	Description
merchant_id.crt	Your public certificate file
merchant_id.pvt	Your private key file
CyberSource_SJC_US.crt	CyberSource server certificate file

Note The Business Center uses a Java applet to generate security keys. The Java applet requires version 1.4.1 or later of the Java browser plug-in. If the applet fails to load properly, CyberSource recommends that you download and install the latest version of your browser and try again.

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

To generate SCMP transaction keys in the business center:

Step 1 Log in to the Business Center, and in the left navigation pane, choose **Account Management > Transaction Security Keys**.

Step 2 In the Transaction Security Keys window, click **Security Keys for the SCMP API**.

Step 3 Click **2048-Bit Key**.
The New Security Key page displays.

Step 4 Click **Generate Certificate Request**.

While the new keys are generated, messages appear in the Messages text box. Your browser then opens a Save As dialog box.

Step 5 In the Save As dialog box, navigate to a safe location for your keys. Be sure to use separate locations for the test and production environments. Be careful not to overwrite a key in the wrong directory.

Important If you do not protect your security keys, the security of your CyberSource account may be compromised.

Specifying Transaction Key Locations

After you download your SCMP API transaction keys, you must specify the key directory location so that your client application can find them when you send transactions to the CyberSource server. The following table lists how to specify the key directory location for each type of SCMP API client application. For more information, see the *SCMP API Client Developer Guides*.

Table 2 Specifying Transaction Key Locations for the SCMP API Client Applications

SCMP API Client Type	Method to Specify Transaction Key Location
ASP	The client searches for the keys in ICSPATH\keys where ICSPATH is an environment variable that you must set. This applies to both Windows and UNIX. For additional options, see the documentation for your client.
C/C++	
.NET 2002, 2003	
Perl	
Java	Set the **ics.keysPath** property in the **ICSClient.props** file. For additional options, see the SCMP API Client for Java Developer Guide.

Copying Keys

You can copy the keys that you tested in the test environment to the live environment. The copied key will expire in the test environment after 30 days.

To copy keys from the test environment to the live environment:

Step 1 From the Security Keys for the SCMP API page, check the box next to the keys that you want to copy.

Step 2 Click **Copy Keys**.

Step 3 Click **OK** in the warning screen that pops up.

Verify the keys in the Live environment.

CHAPTER 3

PGP Security 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* and *Electronic Check Services Using the SCMP API*.

A PGP public/private key pair enables you to use encryption to protect credit card 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.

Creating a PGP Key Pair

You can use any OpenPGP-compliant software to generate PGP keys. The key you generate must be an RSA key. For software solutions, see http://www.pgp.com/, which is part of the Symantec encryption product group. Free OpenPGP solutions are also available:

- Bouncy Castle at http://www.bouncycastle.org/
- GPG4WIN at http://www.gpg4win.org/

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.

Important

Place the backup 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 Public Key to Your CyberSource Merchant Profile

Before you can decrypt a response file or NOC report, you must add the PGP public key that you created to your CyberSource merchant profile in the Business Center. Only the corresponding private key can decrypt files that are encrypted with the public key.

Important If you do not have administrative privileges, an administrator must grant you Business Center access as described in "Granting Business Center User Permissions," page 16.

To add the PGP public key to your merchant profile:

Step 1 Log in to the Business Center.

Step 2 In the navigation pane, choose **Account Management > PGP Security Settings**.

The PGP Security Settings page appears.

Step 3 Copy the ASCII string of the PGP key into the PGP Key Value field. Here is an example of an ASCII string for a PGP key:

```
mQENBEnUeKQBCADI97dqBLOmIehGIuNWr08deuj6ym+CdrJ/lcugVqv1Od7iypT+
pu8zU2mEFTXWMLmf363KU8yNhbR3iSn5DKwpT/XLQ/SmaKOMv/ZZ2KoHbz5zGdd/
5nA/yIS3YvcACq+ZPpYS0as4LpJ4B6dnDuLroxMNjI+cxdXvJ7Rzt4Rqg+ro1KD3
URxqMa0wQbxm8R07k6wsNV1EJuPJ9N5ogYuPKdGyJ3TPQxdQtiqsRFF/KeuwNPk5
BPeOKnSbc4GPyilno1AA3pwdLgw4HIZ3POWq6Zu5jGOJiub8C1qtBUI0Hend73jh
kQmLylz17C5NdjfpCZSsxhee36lGsOALM2pXABEBAAG0I2ljYV90ZXN0XzEgPGds
bG95ZEBjeWJlcnNvdXJjZS5jb20+iQE2BBMBAgAgBQJJ1HikAhsPBgsJCAcDAgQV
AggDBBYCAwECHgECF4AACgkQc8du5ok+OYj3PAf/d3zwP+cBaJUMp61foljMsCF6
JNpkCil9A3gkkf6Z2YgVhfH1OXf1JsN3jDOBEkt24um5HfhmhsDy+x4VAQyEuzcN
Mst5FQBfLUOsy1tTz+RgDGlKUtSsbzJ9puURfRiyN0pqWoHmR2mTJq8puziOSNj4
WAaBq9Jq8o1R35xvrKkle/JGT24jTSwFDGcLIwRxndnutlvaftbkirVrCpRs5Cj/
u4HDh/tXmRKmKrGKOEhn2l1uYX2aLsSJnnlGoY7W+wYsJImw4j3EOa0WtPA3mO41
SfCYIohI4gkPH4eC/IQcoMkZZ1kV+HiA1wIimWez/YuqSsmPBubELB9VzxMLLA==
=y2uP
```

Important

Do not copy the header and footer when you copy the string. Here is an example of a header:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 8.1 - not licensed for commercial use:
www.pgp.com
```

Here is an example of a footer:

```
-----END PGP PUBLIC KEY BLOCK-----
```

Step 4 Click **Add**.

Step 5 Refresh the screen to view your new key.

Step 6 Click the **Active** button next to your new key in the Existing Keys table.

Step 7 Click **Activate**.

Granting Business Center User Permissions

Step 1 Log in to the Business Center.

Step 2 In the navigation pane, choose **Account Management > User Administration**.

Step 3 Choose a user.

Step 4 In the User Update window, select the following permissions:

a Under Credit Card Account Updater Permissions, check **View Status**.

This option gives the user permission to view the status of uploaded Account Updater request files and NOC reports.

b Under Merchant Settings Permissions, check **PGP Security Settings**.

This option gives the user permission to upload, activate, and deactivate encryption keys.

c Under Reporting Permissions, check **Report Download**.

This option gives the user permission to download Account Updater response files and NOC reports.

Step 5 Click **Update**.