

## eCommerce PGP key rotation FAQ

This document contains answers to several frequently asked questions about PGP key rotation for both the eCommerce production and test environments.

### Production environment

#### **Does it matter how I import these keys?**

For each environment, there is one file to import the new key and a second file to revoke the existing key. You must use your PGP tool to import these files into your PGP keyring.

To obtain the new key for the production environment, you must import the [VantiveCommerce2018Production.asc file](#). Next, to revoke the old key, import the [VantiveCommerce2017RevokedProductionPublicKey.asc file](#). Performing the steps in this order helps ensure your system trusts the new key because the new key is signed by the old key.

In the production environment, since the recipient email is the same for the new and old keys, you must revoke the old key to allow the use of the new key in all situations. Revoking the old key causes the failure of any subsequent attempts to use it to encrypt a file. Please be sure to update all application configuration changes to use the new key prior to revoking the old key.

If you wish to use a fingerprint to verify the authenticity of the key, please contact your Relationship Manager, Customer Service Team ([ecc@vantiv.com](mailto:ecc@vantiv.com)), or our First Line Technical Support group ([eCommerceSupport@vantiv.com](mailto:eCommerceSupport@vantiv.com)).

#### **Do I have to take any action so my production application identifies the new key used to encrypt production files?**

It depends upon how your application currently identifies the key used for encrypting batch files:

1. If your application uses a recipient email of [eCommerceSupport@vantiv.com](mailto:eCommerceSupport@vantiv.com) to identify the key, you only need to import the new key and expire/revoke the old key. Your application or configuration data does not need to change.
2. If your application refers to the key by a hex identifier, name, or UID, then you must change your application or configuration data to identify the new key based on the values below.

	Old Production Key	New Production Key
Recipient email	eCommerceSupport@vantiv.com	eCommerceSupport@vantiv.com
Key UID	Vantiv eCommerce 2017 Production Public Key (Vantiv Production Environment Key) <ecommercesupport@vantiv.com>	Vantiv eCommerce 2018 Production Public Key (Vantiv eCommerce Production Environment Key) <ecommercesupport@vantiv.com>
Key Hex identifier	pub 1024d/E7E5070A sub 2048g/49712254	pub 1024d/31ABA877 sub 2048g/443B77A0
Fingerprint	405E 9B85 F8FF 2DAA F0D5 DD73 00D9 8CD7 40B0 FD42	8D19 C80D A781 6B35 B059 5C4D 78AC B62F 31AB A877
Expires	2018-10-07	2019-11-07
File to Import or Expire	VantiveCommerce2017Production.asc	VantiveCommerce2018Production.asc

**Does the action have any impact on the public key that Worldpay uses to encrypt my response files?**

No the action will not have any impact on the public key that Worldpay uses encrypt response files.

## Test environment

**Does it matter how I keep these keys?**

For each environment, there is one file to import the new key and a second file to revoke the existing key. You must use your PGP tool to import these files into your PGP keyring.

To obtain the new key for your production environment, import file [VantiveCommerce2018TestPublicKey.asc](#). Next, to revoke the old key, you import the [VantiveCommerce2017RevokedTestPublicKey.asc](#) file. Performing the steps in this order helps ensure your system trusts the new key, because the new key is signed by the old key.

In the production environment, since the recipient email is the same for the new and old keys, you must revoke the old key to allow the use of the new key in all situations. Revoking the old key causes the failure of any subsequent attempts to use it to encrypt a file. Please be sure to update all application configuration changes to use the new key prior to revoking the old key.

If you wish to use a fingerprint to verify the authenticity of the key, please contact your Relationship Manager, Customer Service Team ([ecc@vantiv.com](mailto:ecc@vantiv.com)), or our First Line Technical Support group ([eCommerceSupport@vantiv.com](mailto:eCommerceSupport@vantiv.com)).

**Do I have to take any action on how my test application identifies the key to be used to encrypt files intended for the test environment?**

Yes. Determine how your test application identifies the key used for encrypting batch files and modify the application or configuration data to identify the new key based on the values below.

	Old Test Key	New Test Key
Recipient email	<a href="mailto:implementation@vantiv.com">implementation@vantiv.com</a>	<a href="mailto:implementation@vantiv.com">implementation@vantiv.com</a>
Key UID	Vantiv eCommerce 2017 Test Public Key (Vantiv eCommerce Merchant Test Environment Key) < <a href="mailto:implementation@vantiv.com">implementation@vantiv.com</a> >	Vantiv eCommerce 2018 Test Public Key (Vantiv eCommerce Merchant Test Environment Key) < <a href="mailto:implementation@vantiv.com">implementation@vantiv.com</a> >
Key Hex identifier	pub 1024D/7E25EB2C sub 2048g/49712254	pub 1024D/94276408 sub 2048g/5C78EF11
Fingerprint	4AEF F501 739F 45A2 7535 AC04 19D2 37DE 7E25 EB2C	15FB ACF4 7BFD 3BE3 8E10 16C3 7FB3 9925 9427 6408
Expires	2018-10-07	2019-11-07
File to Import or Expire	VantiveCommerce2017TestPublicKey.asc	VantiveCommerce2018TestPublicKey.asc

**Does this action have any impact on the public key that Worldpay uses to encrypt my response files?**

No. This action will not have any impact on the public key that Worldpay uses to encrypt response files.