

Payment Security Services: Frequently Asked Questions

CyberSource Payment Security



Payment Security practices are critical to keeping payment data safe and protected to ensure that your brand remains unblemished. The CyberSource solution secures your payment environment with less cost and complexity by eliminating payment data exposure through the capture, storage, and transmission process.

This document discusses frequently asked questions on the implementation and use of hosted payment acceptance, tokenization, order handling, and PCI DSS compliance in a merchant environment.

Hosted Payment Acceptance

Hosted Payment Acceptance allows you to accept and process payments without payment data entering your systems. CyberSource hosts the payment data fields so that data is captured and transmitted outside of your environment and directly to the payment network.

Q: What is the difference between a Hosted Payment Field and a Hosted Payment Page?

A: A Hosted Payment Field refers to fields on your site that capture payment data from a customer. These fields are hosted by CyberSource, a third party PCI DSS Level-1 compliant service provider, who captures, transmits, and processes the customer's payment data on your behalf. A Hosted Payment Page refers to a payment data entry page that is completely hosted by CyberSource. Customers are automatically directed to a page that is branded exactly like the rest of your site, but only the URL is different. The process is entirely transparent to the customer and you retain full control of the page's content.

Q: When using tokenization, does the URL of the payment page change from my online shopping cart site?

A: No. Tokenization of the data is performed on the back-end of the payment process, following the transmission of encrypted data to CyberSource's network. Payment data is captured on the payment data entry page of your site, keeping intact any online shopping cart data collection.

Q: What kind of software is required on my payment site to accept the Hosted Payment Acceptance?

A: To implement Hosted Payment Acceptance, you must be able to create web pages that will gather customer and order information for the services that you want to use and you must be able to process the reply information to fulfill the customer's order. This includes:

- Existence of basic shopping-cart software.
- In-house programming skills in ASP, PHP, Perl, JSP, ColdFusion v7 or higher, or ASP.net.
- ISP hosts product pages in one of the scripting languages mentioned above.
- A secure (SSL) order form.

CyberSource®
the power of payment

www.cybersource.com

Toll free: (888) 330-2300

Payment Security Services: Frequently Asked Questions



Tokenization

A format-preserving token is one in which the number of digits match those of the payment card that the token is masking.

Q: Does tokenization work with an existing ERP systems payment interface?

A: Tokenization can be integrated with existing ERP systems. Using a format-preserving token, you can substitute the token for the actual primary account number (PAN) since the format preserving token will pass a mod 10 check and contains the same number of digits as an actual payment card number.

Q: Are tokens the same length as credit cards?

A: Tokens can be created in any length or be alphanumeric in nature. However, format-preserving tokens can now be generated that contain the same number of digits as a payment card, allowing for seamless integration with existing ERP systems.

Q: Do token formats need to be updated regularly?

A: No. Once a token has been assigned to a transaction or a payment card, it is never updated or changed. However, the details stored along with the token such as billing address and card expiration date can be updated.

Q: Can a token be customized?

A: In addition to the ability to preserve the format of a payment card, a token can be generated so that it retains the last four digits of the payment card. Using this customization, customer service representatives are easily able to identify customers by matching the actual last four digits of the last payment card to that of the last four digits of the token retained in the database of record.

Q: If we already send all payment data from our checkout system to CyberSource, is tokenization still necessary?

A: Tokenization provides additional safeguards and features that enhance the storage of data by CyberSource. Tokenization adds an additional layer of security to your existing payment processing platform. Using tokenization, you are able to completely remove payment data from your environment and significantly reduce the impact that a data security breach could cause as cyber thieves would find only masked data upon intrusion.

Q: If I want to move to tokenization, is it my acquirer who enables this for me or do I go to the payment brands?

A: To move to a tokenization solution, you would contact a vendor providing tokenization services, such as CyberSource. CyberSource provides global payment processing services, working with the larger payment network, which includes the acquirer. Tokenization services would augment the security of your payment services and could simply be enabled on if the CyberSource payment processing platform is installed.

CyberSource®
the power of payment

www.cybersource.com

Toll free: (888) 330-2300

Payment Security Services: Frequently Asked Questions



Handling Orders with Tokenization

Q: How does a token work with orders that are delayed (holds due to obtaining funding, authorization, etc.)?

A: The payment processing with an acquirer uses the actual payment data, not a token. CyberSource converts the payment data into a token and stores the token in its system as well as provides the token back to you. For orders that are delayed due to issues in the authorization or obtainment phase are flagged in your system. CyberSource automatically retries the payment several times. It is not considered a failed payment until CyberSource has exhausted all possible retries. At this point, CyberSource will require your intervention and notify you of its status in a daily activity report.

Q: How does tokenization support “single-click” ordering with stored payment data for returning customers?

A: Once a token has been generated, it is a best practice, and within PCI-DSS rule, to store the expiration date and last four digits of the card in your database of record. When the customer is ready to use the single-click option, simply display the last four digits of their payment card and the expiration date so that you are able to identify the appropriate card. Upon check-out, simply append the token for that card to the submitted transaction rather than sending the full payment card number or requesting it from your customer.

Q: How does a chargeback process work with tokenization?

A: When your acquirer initiates a chargeback, you should be provided with a unique reference number that you can use to locate the transaction. Your acquirer should not use the credit card number in any chargeback communication as per PCI-DSS rules. If your acquirer is still using the credit card number in communications, you can outsource the handling of your chargebacks to a secure vendor.

Q: How are refunds handled using tokenization?

A: Refunds can be handled in one of two ways. First, you can perform a follow-on refund transaction linked to the original sale, essentially reversing the sale. Second, you can perform a stand-alone credit by passing in the refund amount with the token. The stand-alone refund will not be linked to the original sale.

Q: How does tokenization account for split orders?

A: Each payment instrument in a split-order would have its own token generated. You would need to associate all tokens with the same order and if a refund is needed, refund against the appropriate token.

Q: How is tokenization used in a recurring charge/billing or subscription situation?

A: You are not required to re-submit payment data for a future or recurring billing event. Using CyberSource's tokenization solutions, you set up the customer profile so as to generate given-period billing cycles (weekly, bi-weekly, monthly, bi-monthly, quarterly, twice annually, annually) and related dollar amounts. CyberSource will initiate these recurring transactions on your behalf. With the integration of Account Updater, payment data is automatically updated when it expires or changed (a card reissue when reported stolen, etc).

Q: If a customer has multiple credit cards, will they have multiple tokens?

A: Yes. A token is specific to a given payment card transaction, not to the payment card owner.

Q: Does CyberSource have relationships with local banks in most countries for payment processing?

A: CyberSource provides global payment processing services, transacting payments in over 190 countries and funds in 21 currencies.

CyberSource®
the power of payment

www.cybersource.com

Toll free: (888) 330-2300

Payment Security Services: Frequently Asked Questions



PCI DSS Compliance

Q: If I need the PAN retrieved from the token storage vault, does this bring my devices and systems back into PCI scope?

A: Yes. To reduce the scope of PCI DSS, you should reduce the payment data capture, storage, or transmission on your network. The moment that payment data is re-introduced into the network in any form those devices or systems are back within scope and must be audited.

Q: If I implement a tokenization solution, am I still required to comply with PCI DSS?

A: Yes. Tokenization has the ability to reduce the scope of PCI DSS significantly, thereby reducing time and money spent on securing the network environment on a day-to-day basis. However, according to the PCI DSS standard, every merchant must validate their compliance and maintain compliance at all times. Depending on your level and payment data interaction, the depth of the audit will vary. See the PCI DSS security Standards Council website for additional information on determining your company's audit requirements: <https://www.pcisecuritystandards.org/>.

Q: If I use tokenization, does this completely eliminate my back office from PCI scope?

A. Depending on the scope of implementation, tokenization can reduce /eliminate merchant back office services from the scope of PCI DSS. In order to completely remove it from scope, payment data cannot enter your back office operations in any way. Often back office staff can encounter payment data on their devices in instances of recurring billing and chargeback processing. To eliminate access to data requires that tokens are used at all times, that staff uses the tokens to identify customers, that full PAN data is never requested from the customer, and that staff never writes down the PAN data or enters it into their systems.

Q: If a breach occurs in a system using tokenization, how does it affect the merchant and the payment gateway/tokenization solution provider?

A: When a merchant using tokenization is breached, the cyber thief will only be able to access tokens rather than actual PAN data. As the tokens are specific to a customer/merchant combination and can only be used by the merchant for a specific customer or transaction, they are useless to the cyber thief. He cannot transact with the token nor use it as a unique identifier in any instance outside of the merchant environment. As the tokens hold no value to other criminals, the cyber thief would be unable to profit from stealing them. It is the equivalent of a bank robber penetrating a bank safe only to find that it is empty.

Additional PCI DSS compliance and audit questions should be addressed directly by the PCI DSS Security Council (www.pcisecuritystandards.org), such as:

- Where do you start if you want to become PCI compliant?
- How do you determine what level of PCI DSS you are required to comply with?
- If you use a system that uses tokenization, what PCI DSS survey do you need to complete?
- Are there any resources online that can aid in the completion of the PCI DSS Self-Assessment Questionnaire (SAQ)?
- For smaller businesses, is there another way to prove compliance besides a full PCI DSS audit?

Solution Implementation

CyberSource provides several different implementation options including:

- A hosted, self-managed payment management system
- Professional service team members to help design and implement
- Fully managed service implementation with business performance guarantees

CyberSource®
the power of payment

www.cybersource.com

Toll free: (888) 330-2300