

Payment Tokenization: Exposed

CyberSource Payment Security



Payment card data is extremely valuable not only to its owners but to merchants using it to process orders and hackers who seek to exploit it for their own gains. Keeping it safe and secure can be difficult and merchants will invest millions of dollars to place as many obstacles in front of it to keep out would-be cyber thieves. However, hackers have sharpened their skills and continue to be ruthless in their pursuit.

Merchants seeking to truly out-manuever hackers have adopted payment tokenization as a potential silver-bullet solution. In using tokenization, merchants completely move their customers' credit card information out of the environment. They no longer manage the storage, maintenance, or processing of that data, but task those duties to a third-party source, such as CyberSource.

Tokenization Defined

Simply, tokenization is the replacement of sensitive data with a unique identifier that cannot be mathematically reversed. In your environment, tokens take the place of sensitive credit card data. Typically, the token will retain the last four digits of the card as a means of accurately matching the token to the credit card owner. The remaining numbers are generated using proprietary tokenization algorithms.

How it Works

To make a purchase on your website, the customer will enter his credit card information into the designated payment fields on the order page. These payment fields will be hosted by CyberSource using either its hosted order page (HOP) or a silent order post (SOP)¹. When the customer hits the „submit“ button, the data is immediately encrypted and transmitted directly to CyberSource for storing, processing, and token generation. The credit card information never enters your environment.

The encrypted primary account number (PAN) is decrypted when it enters CyberSource's Level 1, PCI-compliant data vault, where it is securely stored. The payment data is then passed on to the processing channel (bank) and returned to CyberSource with an accepted or denied result.

CyberSource returns the result to you but substitutes the PAN data with a uniquely generated token. You store the token in their enterprise resource planning (ERP) system for future transactions or chargeback resolution on that account. Customer service representatives can easily verify customers as the custom token will retain the last four digits of the original PAN.

Benefits of Tokenization:

- Reduces PCI-DSS scope
- Renders credit card data meaningless to hackers
- Provides end-to-end security
- Not mathematically reversible
- Format fits legacy credit card data fields
- Retains last four digits of original credit card number
- Account Updater automatically updates payment data for fewer failures
- Chargebacks and payment reconciliation handled by CyberSource
- Works with existing systems or processor
- Supports multiple payment actions and checkout models
- Retains ability of customer service representatives to identify customers during an inquiry
- Low cost-per-transaction

¹For more information on CyberSource's HOP and SOP, please refer to CyberSource's "Hosted Order Page (HOP) Eliminates Handling of the Data" and "Streamline Sales Using Silent Order Post (SOP)" articles, available through your account manager.

CyberSource[®]
the power of payment

www.cybersource.com

Toll free: (888) 330-2300

Payment Tokenization: Exposed



Tokenization vs. End-to-end Encryption – Which is the preferred technology?

Tokenization and end-to-end encryption (E2EE) are often positioned as an either/or solution, but this is not the case. Encryption has many uses and will likely never be completely obsolete, and all tokenization solutions will incorporate some sort of encryption into its process. For instance, CyberSource encrypts PAN data as it is transmitted to its secure storage vault for processing. However, there are material differences between the two technologies that can impact a company's final decision as to which one to implement.

Encryption – Historically, encryption has been the standard for securing data and is used in virtually every company for many different reasons. In using E2EE for credit card data security, PAN data is converted into ciphertext using complex algorithms, which cannot be easily understood. A decryption key is required to translate the data back into a readable format. However, there are two primary drawbacks to this technology:

- Anyone who obtains the decryption key can easily access the sensitive and valuable credit card data.
- Hackers who obtain a series of encrypted data that was generated using the same algorithm can mathematically reverse it to de-code the data.

Tokenization – Using tokenization, credit card data is completely replaced with a randomly generated number. There is never a need to decrypt it or to call the real PAN back into the environment as the tokens can be used repeatedly, so hackers have nothing of value to steal. There are a few drawbacks to using tokenization:

- Tokenization does require the use of encryption for transmission of credit card data from the customer to the token vendor.
- There is no industry standard established for tokenization, although the PCI DSS Security Council has created a special interest group to construct a set of best practices for the technology.

Conclusion – While each technology has its place in payment security, tokenization is emerging as the primary solution for organizations seeking to mitigate the potential impact of a security breach as well as reduce their PCI scope and related costs.

Reliability, Flexibility, and Security with CyberSource Payment Tokenization

CyberSource's payment tokenization solution provides you with flexible options that will fit your specific needs. Tokenization can be used with or without a hosted payment acceptance option. It also works seamlessly with any existing system or processor.

Criteria	Tokenization	Encryption
PAN data displayed		X
Mathematically reversible		X
Reduces PCI scope	X	
Payment flexibility – refunds, chargebacks, etc.	X	
Rotation of keys required		X
End-to-end security	X	
Low-cost per transaction	X	
Format fits with legacy credit card fields	X	
Centrally managed	X	
Established security standards		X

If you have specialized requirements related to data sovereignty, legacy system formats, or PII tokenization CyberSource Global Services can provide a customized solution to meet your specific needs.

For merchants housing credit card data in on-premise databases, the PAN data is easily uploaded to CyberSource's storage vaults using CyberSource's API or batch loading processes. The payment tokenization solution is compatible with the Visa and MasterCard Account Updater service, where all payment information stored with CyberSource is automatically updated by participating banks, thereby reducing payment failures.

CyberSource's payment tokenization supports all payment actions and checkout models including one-time authorization, capture and settlement, recurring and subscription billing, credit and partial credit, split capture, re-authorization, and standard checkout. Included with the service is the management of chargebacks and payment reconciliation as well as support for online purchases, call center, kiosk, and IP-based POS systems