Payment Security Solutions

Payment Tokenisation

Secure payment data storage and processing, while maintaining reliable, seamless transactions.
CYBERSOURCE PAYMENT TOKENISATION:
Securing Payment Data Storage

To enable secure payment data storage and processing, it is important to identify key business needs with regards to payment security management.

KEY BUSINESS NEEDS WITH REGARDS TO
Payment Security Management

Protect Your Brand
• Prevent damage to reputation by preventing breach of sensitive data.
• Stricter data breach disclosure requirements and penalties.

Scale and Evolve Reliably to Omni-Commerce
• Growth of multi-market expansion, and managing multiple customer channels and touch points without compromising on payment security.
• Reduce the complexity and challenges as business quickly grows.

Manage Costs
• Optimise payment security management and implementation costs whether it is in scaling existing systems, adding new channels or expanding into new markets.
• Prevent unnecessary losses due to payment data losses from your business environment.

Manage Your Business Effectively
• To continue to operate your business and service your customers with payment security management in place.
• Reduce scope of Payment Card Industry Data Security Standards (PCI DSS) compliance even as rate of accepted transactions increase.
WHAT IS
Tokenisation?

Tokenisation is the replacement of sensitive data with a unique identifier that cannot be mathematically reversed. In your business environment, tokens take the place of sensitive credit card data while the data is stored on CyberSource’s secure servers. There are multiple token formats generated using proprietary tokenisation algorithms to meet your business needs.

HOW DOES
Tokenisation Work?

To make a purchase on your website, the customer will enter their credit card information into the designated payment fields on the order page. These payment fields can also be hosted by CyberSource using its secure acceptance services.

1. When the customer hits the “Submit” button, the data is immediately encrypted and transmitted directly to CyberSource for processing, token generation and storing. Credit card information never enters your environment.

2. 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.

3. CyberSource returns the result to you but substitutes the PAN data with a uniquely generated token. You store the token, easily verified with the last four digits of the original PAN retained, in your Enterprise Resource Planning (ERP) system for future transactions or chargeback resolution on that account.
KEY BENEFITS OF
CyberSource Payment Tokenisation Services

Secure and Reliable

- Multiple layers of protection make cardholder data significantly more secure.
- Enables end-to-end security.
- CyberSource stores credit card information in their PCI-compliant secure servers.
- Using the token to replace the cardholder data within the merchant environment reduces PCI DSS scope.
- Tokens provide an added layer of security since they are not mathematically reversible.

Flexible and Simple to Integrate

- Easy implementation and maintenance, which enables IT to focus on broader business initiatives.
- Multiple token formats supported, including formats that fit legacy credit card data fields.
- Works with all CyberSource supported payment channels and processors.
- Supports multiple payment actions, including items such as authorisation, settlement, recurring billing, and refunds.
- Supports multiple checkout models, including standard and Simplified Checkout.
- Integrates easily with other CyberSource payment and fraud management solutions.
- PAN data is easily uploaded to CyberSource’s databases using CyberSource’s API or batch loading processes.

Improved Customer Experience

- Tokens with unique identifiers ensure that you retain control over your customer relationship management.
- Tokenisation format retains last four digits of original credit card number for easy reference.
- Visa and MasterCard Account Updater services (subject to regional coverage) automatically updates payment data for fewer payment failures.
- Facilitates Simplified Checkout.
HOW TOKENISATION CAN HELP ENABLE
Simplified Checkout

Tokenisation also plays an important part in streamlining the checkout process for repeat customers. Since the token stores a customer’s payment credentials, returning customers are not required to enter their payment information, address and other details for every purchase. Instead, they can check out with just one click.

After clicking the “Buy” button, they can be asked to verify the order and complete the transaction. This feature is particularly useful for recurring and subscription businesses, but can be a differentiator for other retailers as well. It rewards loyal customers by reducing friction and improving the checkout experience.

A Note on Tokenisation versus End-To-End Encryption

Tokenisation 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 all tokenisation solutions 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.

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.

Tokenisation – Using tokenisation, credit card data is completely replaced with a randomly generated number. There is no 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.
CyberSource can help you reduce the costs and complexities associated with payment security. You can better secure your environment, build consumer trust and better protect your brand by eliminating payment data storage, capture and exposure. You can accept and process payments without the risk of storing or handling sensitive customer payment details—we manage the data on your behalf in our secure data centres, reducing your PCI DSS compliance scope.

**Payment Tokenisation**
On-demand secure payment data storage in CyberSource’s PCI DSS-compliant data centres removes sensitive payment data from your network by exchanging that data for a payment token.

**Secure Acceptance – Web/Mobile**
CyberSource understands how important providing a seamless customer experience is to your business. Using our hosted payment acceptance, you can accept and process payment data without the data ever touching your network and without negatively impacting customer experience.

**Secure Acceptance – IVR/Call Centre**
Extend your multi-channel options by allowing your customers to pay by phone. CyberSource Secure IVR Payment offers the convenience of 24x7 customer service backed by a robust, PCI-compliant hosting environment outside your system.

**Secure ERP Payment**
The smart solution for organisations storing payment information in Oracle or Siebel systems. CyberSource Secure ERP Payment integrates with your enterprise deployment, reducing security risk and PCI DSS scope.
About

CyberSource Corporation

The World’s First eCommerce Payment Management Company

We’re more than a payment security solutions provider—we’re a payment management company. CyberSource provides a complete portfolio of services that simplify and automate payment operations. Customers use our CyberSource and Authorize.Net brand solutions to process online payments, streamline fraud management, and simplify payment security.
About CyberSource

CyberSource, a wholly-owned subsidiary of Visa Inc., is a payment management company. Over 400,000 businesses worldwide use CyberSource and Authorize.Net brand solutions to process online payments, streamline fraud management, and simplify payment security. The company is headquartered in Foster City, CA and maintains offices throughout the world, with regional headquarters in Singapore, Tokyo, Miami / Sao Paulo and Reading, U.K. CyberSource operates in Europe under agreement with Visa Europe. For more information, please visit http://www.cybersource.com/asiapacific

**NORTH AMERICA (US & CANADA)**

CyberSource Corporation HQ
Phone: 650-432-7350
Toll Free: 1-800-530-9095
Email: sales@cybersource.com
Website: www.cybersource.com

**EMEA (EUROPE, MIDDLE EAST & AFRICA)**

CyberSource EMEA
Phone: +44 (0)118 990 7300
Email: uk@cybersource.com
Website: www.cybersource.com/emea

CyberSource Visa Middle East FZ-LLC
Phone: +971 4 457 7200
Website: www.cybersource.com/mea

**LATIN AMERICA & CARIBBEAN**

CyberSource Miami
Phone: +1 (305) 328 1998
Email: lac@cybersource.com
Website: www.cybersource.com/lac

CyberSource Mexico
Phone: + (52-55) 5387 4185
Email: mexico@cybersource.com
Website: www.cybersource.com/mx

CyberSource Brazil
Phone: +55-11 2102-0088
Email: brasil@cybersource.com
Website: www.cybersource.com/brasil

**ASIA PACIFIC**

Asia Pacific CYBS Singapore Pte Ltd
Phone: 800-6363-083 (Singapore)
Phone: 1-800-816-575 (Malaysia)
Phone: 1-800-8-756-8388 (Philippines – Globe)
Phone: 1-800-10-802-7222 (Philippines – PLDT)
Email: ap_enquiries@cybersource.com
Website: www.cybersource.com/asiapacific

CyberSource KK (Japan)
Phone: +81 3 3548 9873
Email: sales@cybersource.co.jp
Website: www.cybersource.co.jp

CYBS Greater China
Phone: +86 21 6109 5141 / +86 21 6109 5100
Email: gc_enquiries@cybersource.com
Website: www.cybersource.com/cn

CyberSource Australia & New Zealand
Phone: 1-800-076-566 (Australia)
Phone: 0800-443-080 (New Zealand)
Email: anz_enquiries@cybersource.com
Website: www.cybersource.com/anz