CyberSource®

CyberSource Secure Acceptance

Businesses are striving to meet consumer expectations and increase checkout conversion rates by providing a fast, easy checkout experience. But at the same time, these businesses must maintain tight security for sensitive customer payment data—theft of that data could lead to lawsuits, fines, a damaged reputation, and erosion of customer loyalty.

Accept payments from any customer-owned device without handling sensitive payment information.

CyberSource Secure Acceptance

CyberSource can help your business meet consumer expectations and deliver a frictionless checkout experience while helping to protect sensitive data. CyberSource Secure Acceptance is a set of connection methods that allows you to accept payments from consumers without sensitive payment data entering your network. When implemented with CyberSource Tokenization, you can conduct all your payment processing functions without handling sensitive payment data, thus significantly reducing Payment Card Industry Data Security Standard (PCI DSS) compliance scope.

Secure Acceptance connections seamlessly integrate with a wide range of CyberSource solutions, including Payment Tokenization, Payer Authentication, Decision Manager, Visa Checkout, PayPal Express Checkout, and ACH processing.

Secure Acceptance Web/Mobile

CyberSource Secure Acceptance Web/Mobile is a fully outsourced hosted solution that passes payment data directly from the customer to secure CyberSource servers. With proper implementation of this solution, eCommerce businesses can qualify for PCI DSS Self-Assessment Questionnaire (SAQ A), which significantly reduces PCI DSS scope.

Secure Acceptance Web/Mobile can be implemented as a redirect solution, or embedded in an iframe on your site. The payment flow, as well as the look and feel, can be customized to match your website.

Secure Acceptance Web/Mobile also helps minimize development effort. You can add and configure payment acceptance methods such as PayPal, Visa Checkout, and electronic checks through the business center portal. Only one request is needed to execute multiple payment functions such as Rules-Based Payer Authentication, fraud screening, authorization, and capture.

KEY FEATURES

- ✓ **Mobile support:** Automatically detects the customer's screen resolution and renders appropriately on any device, from smartphones to desktop PCs.
- ✓ **Global coverage:** Includes out-of-the-box checkout templates in 28 languages,[1] covering 40+ countries.
- ✓ **Branding support:** Provides standardized forms that require no additional coding. You can incorporate your branding elements, and modify to match your look and feel.
- ✓ **Optimized for research and analysis:** Enables you to conduct analyses such as A/B testing. Since each order can be assigned a different profile, multiple segments and payment variables can be tested quickly and easily.
- ✓ **Payer Authentication support for major credit cards:** Supports Verified by Visa, MasterCard SecureCode, American Express SafeKey, and JCB J/Secure.
- ✓ **Support for multiple payment methods:** Supports Visa Checkout, electronic check (ACH), and PayPal Express Checkout without additional development effort.
- ✓ **Americans with Disabilities Act (ADA) compliance:** Complies with ADA guidelines.

Secure Acceptance Flexible Token API

CyberSource Secure Acceptance Flexible Token API is a partially outsourced solution that enables you to securely transmit card data from your customer directly to CyberSource and receive a token in exchange. Your customers' card numbers are encrypted on their own devices, inside a browser or native app, and sent directly to CyberSource. As a result, card data bypasses your systems, typically qualifying you for SAQ A-EP. On-device encryption helps protect your customers from attacks on network middleware—such as app accelerators, data loss prevention (DLP) solutions, and content delivery networks (CDNs)—and also from malicious hot spots.

Secure Acceptance Flexible Token API gives you complete control over the customer's payment experience, including the flow and user interface. The Flexible Token API—a JSON-based RESTful service—focuses on tokenizing card data. You can create separate calls (through additional development effort) for authorization/capture, Rules-Based Payer Authentication, Decision Manager, and other payment functions.

KEY FEATURES

- **Patent-pending double encryption:** Protection of the "pipe" and payload such that even if one level were to be compromised, the underlying card data would remain secure.
- **Complete control of the customer experience:** Allows you to gain full control of the design and customer experience without requiring compromise for security protection.
- **Total control over the payment experience:** Integrates with your existing checkout flow using a background AJAX request to tokenize the card. This token can be used for securely performing other CyberSource services.
- **Support for new, innovative payment experiences:** Secures in-app payment experiences and Internet of Things (IoT) solutions, plus any devices connected to the Internet.
- **Simple integration:** Consists of two small, RESTful APIs: a server-side request to create a public key, which can be used to encrypt the card number; and a client-side request to create a token from a card number that is optionally encrypted.

Which Secure Acceptance Option Is Right for You? At-a-Glance Comparison

	Secure Acceptance Web/Mobile	Secure Acceptance Flexible Token API
PCI DSS implications	Fully outsourced hosted solution. Could qualify you for PCI DSS Self-Assessment Questionnaire (SAQ A).	Partially outsourced hosted solution. Could help you qualify for PCI DSS Self-Assessment Questionnaire (SAQ A-EP).
User experience and checkout flow	Pages can be customized to mirror your branding. Checkout flow is predetermined.	You have complete control over the design and customer experience.
Platforms supported	Designed for web.	Works across web and native applications.
Payment processing impact	Payment services can be executed through the same call, minimizing development effort.	Additional development effort required for payment authorization, capture, and other services.
Deployment and configuration	Can be implemented as a redirect solution or embedded within an iframe. Payment preferences are configurable through the Business Center portal.	Uses a JSON-based RESTful service to obtain a token.
Integration method	Web redirect or iframe.	RESTful API.
Business requirements	Ideal for businesses wanting to minimize PCI DSS scope, access pre-built templates, and easily configure payment acceptance through the portal.	Ideal for businesses wanting to minimize PCI DSS scope while retaining total control of the user experience and payments process.

[1] *Languages supported: Arabic, Bahasa Indonesia, Bahasa Melayu (Malay), Chinese – Traditional , Chinese –Simplified, Catalan, Croatian, Czech, Danish, Dutch, English, French, Finnish, German, Greek, Hebrew, Hungarian, Italian, Japanese, Khmer, Korean, Polish, Lao, Norwegian, Portuguese (Brazilian), Russian, Slovak, Spanish, Swedish, Tagalog (Philippines), Thai , Turkish, Vietnamese.*

CONTACT US: t. **+1 888-330-2300** e. **sales@cybersource.com** w. **cybersource.com**

CyberSource is
a Visa solution VISA