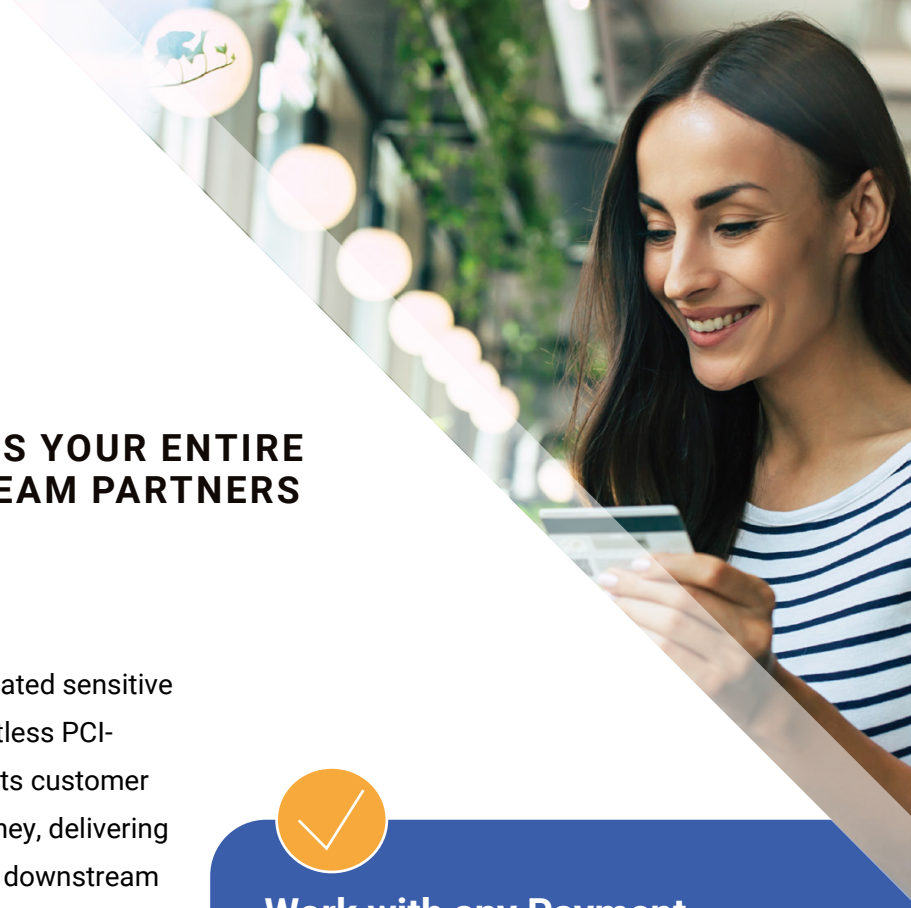
Bluefin®



DRIVE PCI COMPLIANCE ACROSS YOUR ENTIRE ORGANIZATION AND DOWNSTREAM PARTNERS

ShieldConex®

For any business processing payments and associated sensitive data including PII and PHI, ShieldConex is the vaultless PCI-compliant shared tokenization solution that protects customer payment data throughout the entire customer journey, delivering the benefits of PCI DSS scope reduction across all downstream channels and trusted third parties. With ShieldConex, you can tokenize field-specific data to share with trusted partners and across all downstream channels.

ShieldConex positions you to work with multiple acquirers, decouples your data security token solution from your acquirer, and provides enhanced flexibility and leverage over your current token provider.

Work with any Payment Processor, anytime

For Enterprise/Tier 1 retailers implementing a multi-processor strategy, the ShieldConex® Proxy Service is the tokenization and data anonymization service that minimizes the PCI and PII footprint while avoiding long-term processor lock in.

It is the only solution for tokenization and P2PE protected EMV payments that delivers true processor independence.

SECURITY FEATURES

Compliance: Tokenize PAN (primary account number) data and associated PII/PHI data so you maintain compliance for regulations governing the handling of sensitive data

Cloud-Based and easy to manage: web portal simplifies tokenization template creation plus detailed tokenization and detokenization metrics

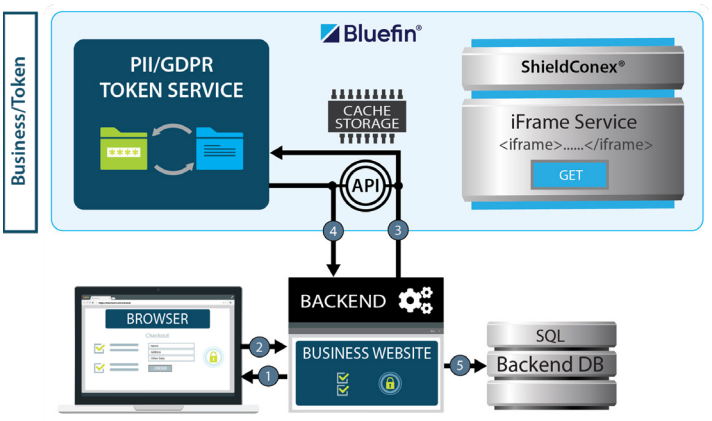
Risk mitigation: Devalue sensitive data and reduce the security attack surface

Validated P2PE: Secure transactions and protect your brand from a costly card data breach

How ShieldConex® Works – API Tokenization Method

Can be used with any platform, system or coding language that can call a REST API.

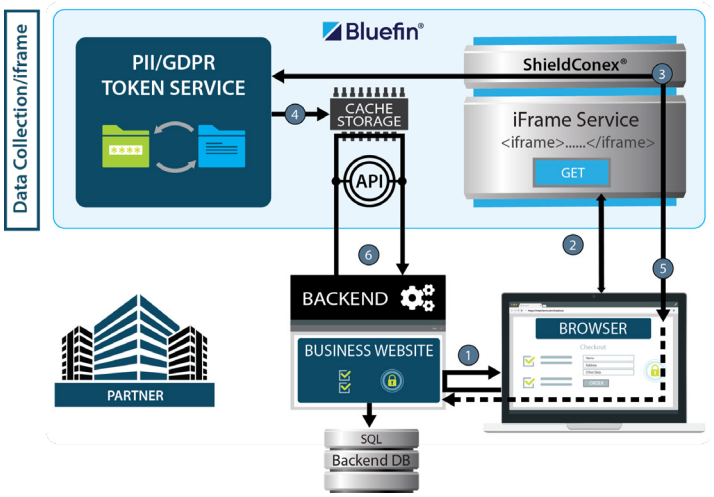
1. The consumer connects to a business website or other enterprise application and more.
2. Sensitive data is entered into the web page or application, and user submits this to the Backend Server service over TLS 1.2 or higher.
3. A backend server function makes the API call to ShieldConex over TLS 1.2 to tokenize the sensitive data.
4. The tokenized data and Bluefin ID (BFID) are returned to the backend server function that called the API.
5. The backend server saves the BFID and tokenized data to a backend database.



How ShieldConex® Works – iFrame Tokenization Method

The iFrame Method is popular for supporting existing payment applications, virtual terminals, user profile pages, etc.

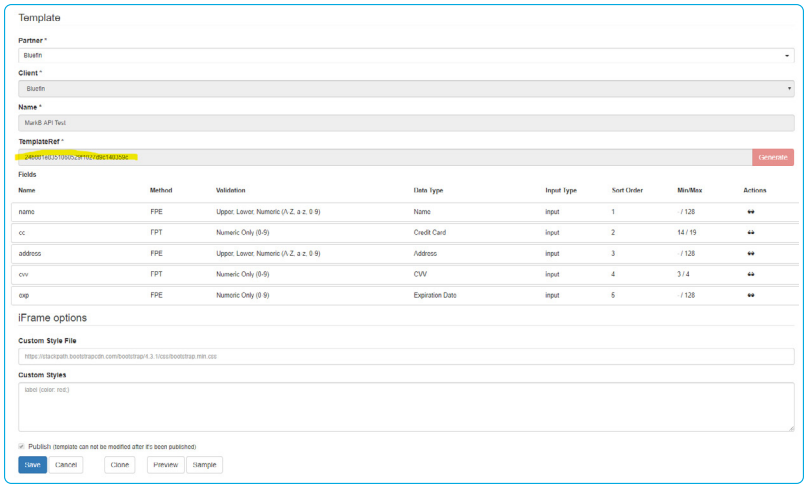
1. Consumer's browser connects to the business website. The page is loaded into the consumer's browser.
2. Code in the page calls ShieldConex. iFrame is returned to the browser.
3. As sensitive data is entered into the iFrame, AJAX elements send sensitive data to the ShieldConex service over TLS 1.2
4. Sensitive data is tokenized and cached in ShieldConex for later retrieval.
5. A Bluefin ID (BFID) is returned to the browser. The ShieldConex iframe passes the BFID to the parent page.
6. The backend server process calls the ShieldConex APIs with the BFID and proper authentication credentials to retrieve the tokens cached by ShieldConex and saves the BFID and tokenized data to a backend database.



Simple Administration with ShieldConex® Manager

Our web-based administration portal is where users can:

- Set security parameters for the data that requires tokenization.
- View detailed reporting on all tokenization and detokenization activity.
- Manage users and user roles for an organization.
- Tokenize and detokenize data directly via ShieldConex's Virtual Terminal without having to use the ShieldConex APIs.



Bluefin®