Voltage security

Technical Brief

End-to-end Encryption for E-Commerce Payments using Voltage SecureData Web™

Introduction

Today, merchants accepting card-not-present payments on the web are concerned about three major issues affecting their business with respect to data security and the customer experience:

- The increasing cost and scope of PCI compliance
- The risk of a data breach and the fallout to their business and reputation
- Customer abandonment caused by sub-optimal user experience

The last seven years of published data breaches prove that the war against cybercrime is a never-ending struggle. Industries and government have mandated security standards for sensitive data. When cardholder information and credit card data is involved, the Payment Card Industry Data Security Standard (PCI DSS) applies. It is a set of guidelines that networks, software, and operational procedures must be assessed against and upgraded where necessary to stay in compliance.

Additionally, today's IT environment consists of a constantly shifting set of applications running on an evolving set of platforms. The lifecycle of sensitive data lifecycle is complex and extends beyond the container and application, sometimes even outside traditional enterprise IT departments into places like offsite backup services, cloud analytic systems, and outsourced service providers. All these make compliance an increasingly complex and costly task.

Traditional access control approaches don't protect the data. They act as barriers to prevent access to the applications. As e-commerce continues to grow, more and more payment data is collected by merchants. Consequently, wide-scale breaches continue to occur as data is stolen, traded and monetized. Because customer data is the new currency of business and no business can function without it, a data breach would bring about erosion of brand trust and high remediation costs[1]. This means that data protection today is a non-negotiable cost of doing business.

Lastly, with shopping cart and checkout abandonment rates above 75%[2], technologies which do not disrupt customer experience and build relationships ensure maximum completion. Page redirects or iframes served by Hosted Payment Solution websites, which sometimes fail on mobile devices, may reduce PCI scope but at the cost of customer experience. According to Forrester's analysis of buyer behavior, *"11% deemed the checkout process laborious or the Web site sluggish. These are noteworthy complaints, as they underline the importance of a streamlined site experience."*

[1] Verizon, Ponemon, Gartner and others estimate the cost of a breach at more than $200 per record. This does not take into account the drastic impact on shareholder value, brand reputation, and the career costs to executives and employees of affected organizations. Recent breaches in large organizations have remediation costs in the tens to hundreds of millions (http://www.zdnet.com/blog/btl/sonys-data-breach-costs-likely-to-scream-higher/49161)

[2] Understanding Shopping Cart Abandonment, Customers Are Often Unprepared To Buy And Stunned By Shipping Costs, Sucharita Mulpuru and Peter Hult, Forrester May 2010.

Mitigating Threats to Card Not Present Payment Data

To address the payment security landscape described above, merchants need a data-centric protection solution that truly achieves end-to-end security in order to mitigate risk of breach, reduce PCI scope without disrupting customer experience, and address the proliferation of devices and data.

Voltage Security has innovated again to provide a game-changing technology that embodies the above capabilities. Called Page-Integrated Encryption™ (PIE), it is an innovation available only in Voltage SecureData Web.

PIE builds upon a variation of the original Voltage Security Format-Preserving Encryption™ (FPE) technique which permits policy information to be embedded into the encrypted data field without impacting the required field size. For a merchant, this allows full access to first 6 and/or last 4 digits of the credit card information if needed for existing business processes while protecting the sensitive digits from the browser all the way to the payment processor.

The Advantages of Voltage SecureData Web

With Voltage SecureData Web, organizations can be assured of end-to-end protection of their customers' payment information:

- **Protects sensitive data end-to-end.** Payment data is no longer exposed to hackers on web server infrastructure, networks and other systems between the browser and the payment processor – it is encrypted right when the customer enters the data at the browser.
- **Eliminates PCI DSS** scope by removing merchant access to sensitive data in systems that do not need it, and without disrupting existing business processes. This can reduce compliance and implementation costs. Coalfire Systems, a leading independent PCI Qualified Security Assessor (QSA), validates that Voltage SecureData Web can eliminate merchant PCI DSS scope if properly implemented[3].
- **Enables a seamless user experience at its most critical point: the checkout.** Alternative approaches involving redirects or embedded iframes negatively impact the customer experience, and obscure the ability to track user behavior.
- **Preserves compatibility with all current browsers including mobile,** using standard browser features – no plugins or additional technical requirements beyond what major internet merchants use today.
- **Deploys effortlessly,** requiring as little as 3 lines of HTML code to add Voltage SecureData Web to a payment application.

Why SSL Isn't Enough

One of the unsolved problems in online web applications is restricting access to sensitive information to just the systems and functions that need it – thereby reducing PCI assessment scope and making it hard for hackers to find the data they are looking for.

SSL is a proven technology for data protection when data is in transit between systems. SSL provides a tunnel within which all data is protected from inspection. But the data is "in the clear" and unprotected before it enters the tunnel and after it leaves the tunnel. So, payment data submitted on a web page is secured by SSL while it is "on the wire", but as soon as it reaches the web server layer, it is unprotected.

[3] Coalfire Report: Voltage SecureData Web™ with Page-Integrated Encryption™ (PIE) Technology Security Review (http://www.voltage.com/pdf/Coalfire_Report_Voltage_SecureData_Web_with_PIE_Technology.pdf)

The other problem with SSL is that the data is obscured while in the SSL tunnel. For an application or load balancer to reference even non-sensitive data on a submitted page, the SSL tunnel must be terminated, leaving all of the data on the page exposed on this intermediate infrastructure.

Closing the Gaps in Protection – Voltage SecureData Web Deployment Scenarios

Consider an e-commerce application like the one outlined in Figures 1 and 2 below. The user is buying a gift, and provides a greeting message, a shipping method, and a payment card to be charged. That data travels from the user browser to the merchant's e-commerce application over an SSL tunnel. Without Voltage SecureData Web the data leaves the tunnel unprotected and is passed around the web application and back office systems in the clear. When the payment card data is sent to a payment processor, it enters a new SSL tunnel.

Figures 1 and 2 show exactly where PCI scope reduction can be achieved if Voltage SecureData Web is correctly implemented and assessed by a QSA. Figure 1 outlines a scenario where the merchant's payment processor or gateway is Voltage-enabled. In this case, the merchant environment has no ability to decrypt payment data, so credit card data is never exposed.

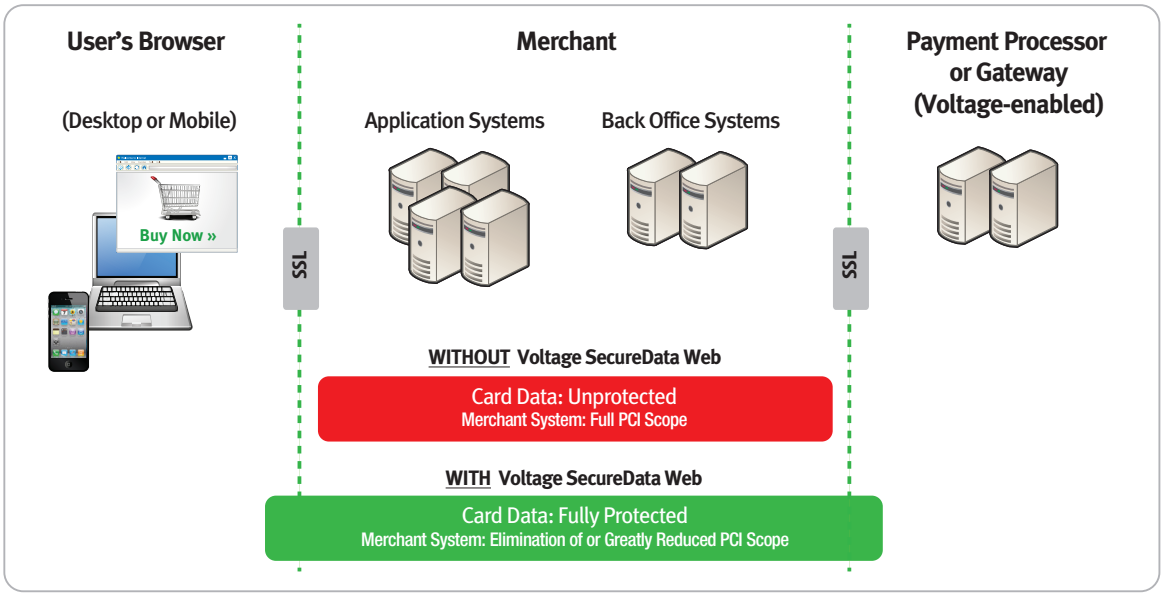

Figure 1. An e-commerce merchant using a Voltage-enabled payment processor

Figure 2 demonstrates another possible scenario, where a merchant implements Voltage SecureData Web back-end infrastructure, enabling an isolated part of the merchant's infrastructure to decrypt payment data and work with actual credit card numbers. In this example, the merchant can send the credit card data to any payment processor, whether or not they are Voltage SecureData Web-enabled. The figure shows where PCI scope reduction can be achieved in this second case.

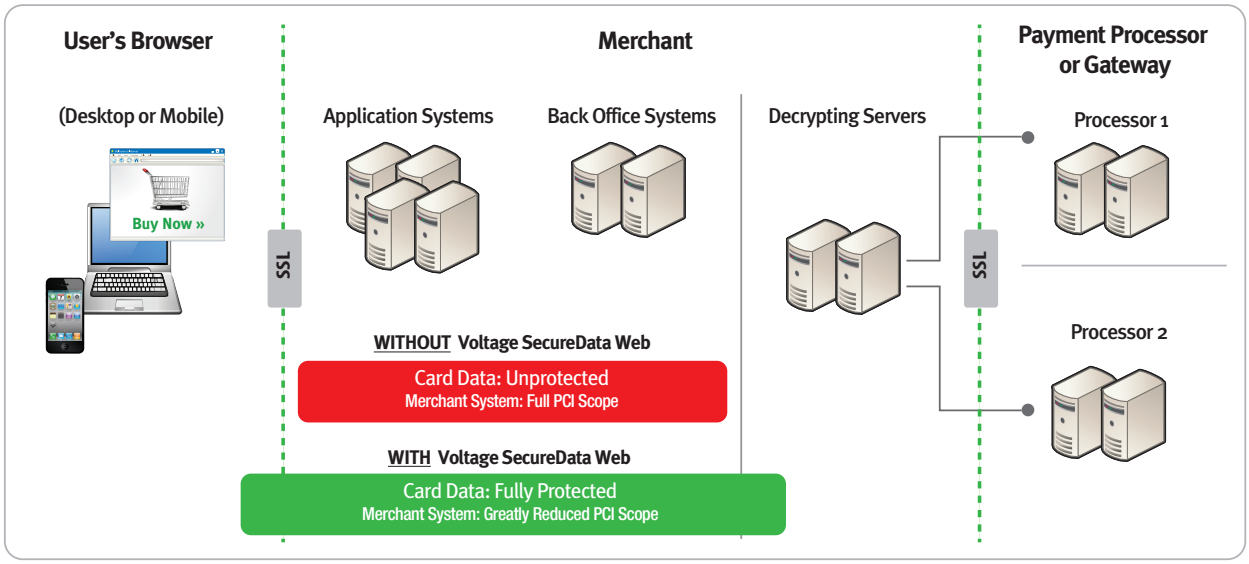

Figure 2. An e-commerce merchant using any payment processors

The PIE Technology Security Model

When encryption is deployed to protect data, the security of the data depends on the management of keys. Typically in most systems the same keys are used across different data elements. If a key is compromised, then any access to encrypted data elements provides access to all the original data. Voltage SecureData Web's PIE technology prevents this risk by using unique, randomly generated keys, which are different for every single transaction.

PIE technology is based on the following fundamental principles:

- PIE uses standard features in all browsers ensuring compatibility across desktop and mobile environments. The browsers must simply be capable of supporting SSL and JavaScript.
- Encryption takes place using one-time random keys per transaction.
- One-time key and key ID are dynamically provisioned to the browser from a trusted site (usually the payment processor) over SSL to ensure code integrity at the moment of encryption.
- Only the final recipient of the encrypted data – and nothing in between – can decrypt the data for the required business purpose – such as passing the cardholder details to the card brands.

While PIE technology provides a shield against data compromise at several points in the handling of the data, "man in the browser" attacks or PC malware may still affect a users's browser. In those cases PIE technology can significantly reduce the exposure of damage by limiting the compromise to just a single transaction instead of a pool of transactions or the entire system. The use of unique random keys per page load eliminates the possibility of any historical transactions being compromised.

What is Format-Preserving Encryption (FPE)?

Format-Preserving Encryption encrypts structured data like credit card numbers, social security numbers, and bank account numbers without changing the format, and thus the associated applications, databases and other systems, yet retaining the high level of security associated with FFX mode AES encryption. A variation of this technology allows the identity and access policy data to be embedded within the cipher text.

	 **Credit Card** 0012 3456 7890 0000	 **Tax ID** 000-00-0000	 **Bank Account** 122105278 724301068
FPE	0012 3423 3526 0000 0012 34Ax 3YPX 0000 (with embedded policy option)	982-28-7723	122110234 8273451068
AES	8JuYE62W%UWJaKS&D DFeruGa2345^WFLER	IJA&2924kUEF65%QAR oTuGDF2390^32KNqL	HIu97NMko2^Ku}o{35 RJ434DQNmnSDreK23

Voltage SecureData Web Implementation

The components that make up Voltage SecureData Web, marked with a “V” in Figure 3 below, are:

- **Voltage SecureData Web Front End Server** – serves static JavaScript FPE library, dynamic key and key ID
- **Voltage SecureData Key Management Server** – generates one-time keys
- **Voltage SecureData Payment Host SDK** – decrypts payment data in a backend host

The above components can all be scaled horizontally, by adding additional physical or virtual servers, for high throughput and redundancy – there is no single point of failure. All components are governed by a central management console, where administrators can set policies and audit usage.

The following diagram looks at how these components work together through the flow of a single transaction.

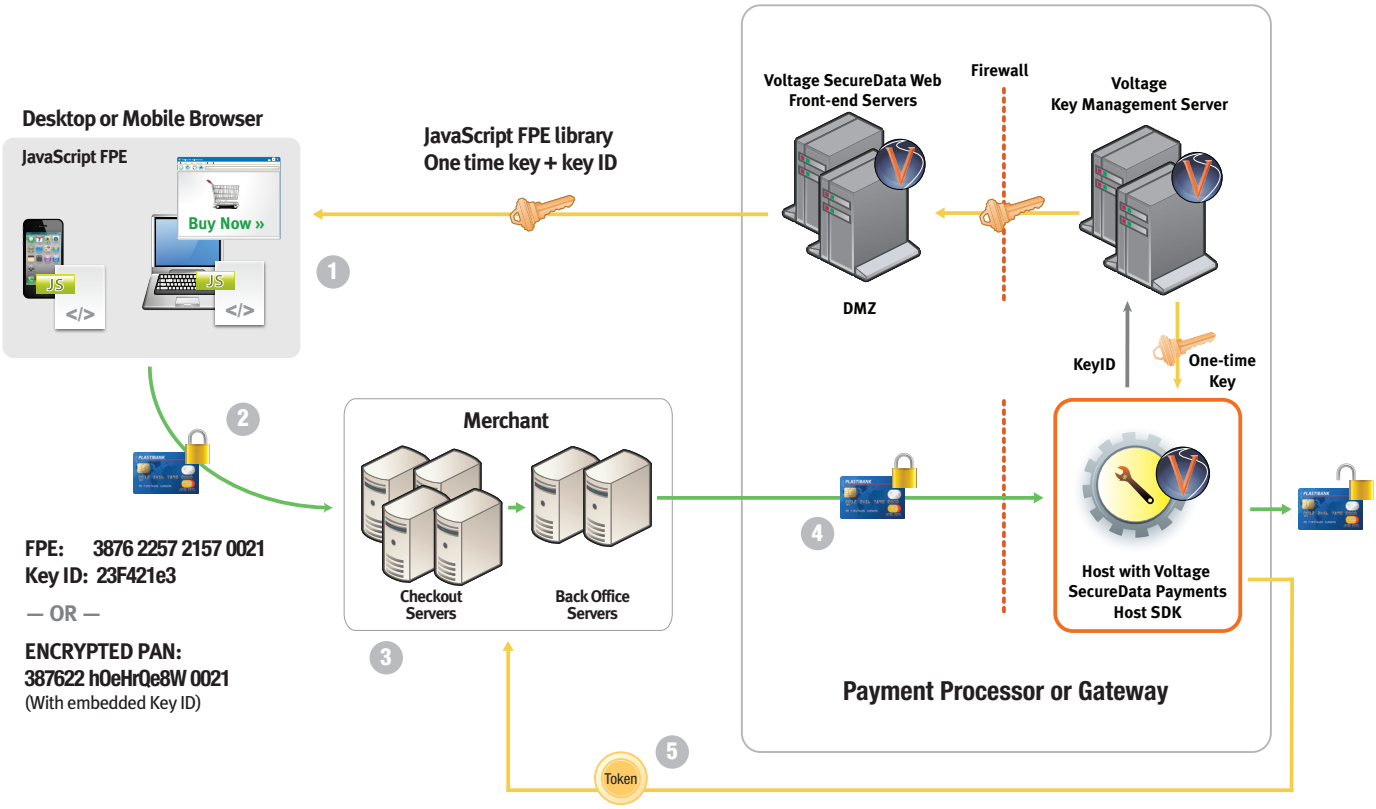

Figure 3. Voltage SecureData Card Not Present end-to-end protection for e-commerce

1. When the end user arrives at the checkout page, hosted in the Merchant server, a snippet of HTML, shown below, loads the static JavaScript FPE library from a Voltage SecureData Web Front End Server.

```
<script src= https://processor.com/.../getkey.js> </script>
<script src= https://processor.com/.../encryption.js> </script>
```

These lines load functions and data directly from the Processor's server into the user's web browser.

2. When the user submits sensitive data, such as a credit card number, the browser invokes the FPE functions to encrypt the sensitive parts of the data prior to submission to the merchant, using HTML code similar to this:

```
<input type=submit onsubmit = "encrypt(credit_card_number, cvv)">
```

3. The merchant's servers pass this encrypted data among its servers freely, confident that it is protected, as none of these servers have the ability to decrypt the data.

4. The merchant passes the protected data on to the processor, or in the alternate case shown in Figure 2, an isolated decrypting server at the merchant. There in the back-office, the **Voltage Key Management Server** and **Voltage SecureData Payments Host SDK** enable decryption of the original credit card and the payment is processed.

5. The processor can optionally return a token using Voltage SecureData Tokenization for final settlement or internal merchant processes previously using cardholder data.

The result: The data has traveled in protected form from capture to final processing, encrypted with a key that is used only for this single, individual transaction.

Conclusion

Voltage SecureData Web improves the security of e-commerce applications that handle sensitive data.Merchants and payment processors can mitigate risks and stay compliant by completely eliminating or significantly reducing PCI scope without disruptingexisting business processes or customer experience. Merchants can now devote time and resources to growing their businesses by providing uncompromised user experience during checkout, rather than battling threats to their data security. In the process, they can preserve their brand image and customer relationships.

All this is achieved with minimal software changes in the online application – a few lines of JavaScript in the front end, and little or no change to the back end. Voltage SecureData Web with PIE technology is essential whenever online data must be protected.

About Voltage Security

Voltage Security®, Inc., is the world leader in providing data-centric encryption and key management solutions for combating new and emerging security threats. Voltage customers represent a wide variety of industries including payments, financial, insurance, medical, e-commerce. Offerings include Voltage SecureMail™, Voltage SecureData™, Voltage SecureData Payments™, Voltage SecureData Web™, Voltage SecureFile™ and Voltage Cloud Services™. The company has been issued several patents based upon breakthrough research in mathematics and cryptographic systems. To learn more about Voltage customers please visit voltage.com/customers.