



Vindicia Technology Overview

<i>Introduction</i>	3
<i>Experience</i>	3
<i>Data Transfer</i>	4
<i>Security</i>	4
<i>Reliability and Scalability</i>	4
<i>Compliance</i>	5
<i>About Vindicia</i>	5

Introduction

Vindicia offers an integrated billing and fraud management solution which is packaged as two products: Vindicia CashBox™, which is a billing system for creating and managing recurring as well as one-time payments; and Vindicia ChargeGuard™, which provides fraud screening and chargeback management services that help merchants recover lost revenue and minimize false positives. While the specific requirements for each vary, each of these has a basic flow in which data from the merchant is transmitted to Vindicia, that data is processed by Vindicia, data is added from third-party sources, and additional information is optionally provided back from Vindicia. This document explains the experience of the Vindicia team and the core philosophies and technology decisions that drive Vindicia's implementation of this flow. After reading this document, you should have an understanding of how data moves from place to place, how it is secured once it gets there, what Vindicia does to ensure reliability, and, what third-party audits and certifications are available around Vindicia's technologies and services.



Vindicia, Merchant and Payment Processor Data Flow

Experience

Vindicia's principals have over 25 years of experience in security companies, including Network Associates (McAfee) and PGP, Inc. The Chief Technology Officer, responsible for all security designs, was on the core development team for PGP software, developed systems that processed check data for NCR, and ran a rebilling subscription service for eMusic, a public company that never had a security compromise.

As pioneers in the security and recurring/automatic billing space, our employees know how to solve these difficult issues. We've done it successfully before.

Data Transfer

Underlying everything we do is the secure transfer of data from the merchant to Vindicia. All data is transferred using the open-standard Simple Object Access Protocol (SOAP). Data about transactions and events are processed into SOAP objects, and encrypted and transferred using industry-standard 128-bit SSL encryption over the HTTPS protocol.

Generally speaking, data will be collected by the merchant, and a call will be made to a Vindicia-provided API library. That library handles the packaging of the environment-specific local object into a generic SOAP object, and the transport. Equally important, it also detects failure and caches data submission for future retransmission so that the merchant's application doesn't have to implement these details.

The Vindicia SOAP library is available on a wide variety of platforms and in all major languages, including C#, Windows ASP/COM, Java, Perl, PHP, and others. Our goal is to make the transfer of data from the merchant to Vindicia as easy, secure and reliable as possible.

Security

Vindicia takes every precaution when handling customer sensitive data whether in CashBox or ChargeGuard. When highly sensitive data does need to be sent, it's encrypted on the way with SSL. Upon receipt, it is immediately encrypted to a public key meeting the OpenPGP standard. The corresponding private key does not exist on that server; even in the unlikely event of a breach, no data would be retrievable. In addition, ChargeGuard doesn't send credit card data when reporting initial transactions; it sends an industry-standard SHA-1 hash, instead.

In transport, as previously discussed, all data is encrypted using SSL. But security is not just a feature you add-in: Vindicia's system has been designed with security as its foremost attribute from the beginning. Physical and digital access to all sensitive areas is tightly controlled and audited. All Vindicia systems are constantly monitored via intrusion detection systems (IDS) as well as other remote-sensing systems to detect any attempts at unauthorized access.

Vindicia's goal is, as much as possible, to not gather sensitive data in the first place. That's why ChargeGuard doesn't send credit card data when reporting initial transactions; it sends an industry-standard SHA-1 hash, instead. But, when highly sensitive data does need to be sent, it's encrypted on the way with SSL. Upon receipt, it is immediately encrypted to a public key meeting the OpenPGP standard. The corresponding private key does not exist on that server; even in the unlikely event of a breach, no data would be retrievable.

Reliability and Scalability

First and foremost, because data transmission occurs over network lines, all Vindicia protocols are designed to degrade in a reasonable fashion in the event of an outage. While Vindicia servers are co-located at dedicated, managed and access-controlled facilities and our infrastructure is physically and network redundant across geographic regions, connectivity issues can occur between a merchant and Vindicia that are out of our control. As a result, when a failure is detected, data is cached and reasonable error codes are returned where necessary, or data is transparently resent when services become available, if appropriate to the application.

All of Vindicia's web and SOAP services are provided via a standard load-balancer/web server model. Requests are brokered by redundant, simple load balancers, which hand requests off to

the actual servers. This is reliable, because, if a given server fails, others are available to handle requests. The system is, as well, scalable, because new servers may be added as load increases.

Connections are centrally monitored by Vindicia for transport time, and our default SOAP library automatically reports average times and failure rates to Vindicia on a daily basis. Using this data, we have occasionally notified merchants of connectivity problems they were not yet aware of. All real-time connections (e.g., a subscription registration event for CashBox) are guaranteed to process within our system in less a second, and our goal is less than 2.5 seconds end-to-end, although the specific connection option between the merchant and Vindicia will dictate the final performance parameters.

Compliance

Vindicia's services have been audited to be PCI Service Provider Level 1 Compliant, and we may provide the audit data upon request. We are also SAS-70 Type 2 audited and comply with the European Data Privacy Act. Vindicia's underlying cryptographic software has met the US Government's FIPS 140-2 Certification.

About Vindicia

Vindicia offers an integrated, on-demand billing and fraud management solution for online merchants. Vindicia CashBox™ is a best-of-breed billing system for creating and managing recurring payments and helps merchants improve customer retention and maximize profit. Vindicia ChargeGuard™ provides automated fraud screening and chargeback management services that enable merchants to recover lost revenue. A PCI Service Provider Level 1 company and SAS 70 Type 2 audited, Vindicia is a key payment management resource for some of the best-known brands on the Internet.