digicert®
Your Success is Built on Trust™

March 2009

White Paper

This white paper demonstrates how DigiCert's cost-effective SSL certificate solutions meet your organization's PCI encryption needs.

Encryption for PCI Compliance

DigiCert's Solution for End-to-End Encryption

"Encrypted data does not usually give rise to claims of data breach. Most often, data is stolen when it is unencrypted and transmitted in clear text—not when it is protected by encryption."

Benjamin T. Wilson JD, CISSP

Lessons Learned from T.J. Maxx and Others

In early 2007, TJX Companies, Inc. (owner of T.J. Maxx, Marshalls, HomeGoods and A.J. Wright in the United States, Winners and HomeSense in Canada, and T.K. Maxx in Europe) announced it had suffered unauthorized intrusions into a portion of its computer system that processed and stored data related to customer transactions. Immediately thereafter, as thousands of credit cards had been compromised, numerous consumers and their banks filed suit in various state and federal jurisdictions in the United States, as well as in Canada and the U.K., asserting claims against TJX related to the intrusions. Visa fined TJX's card processor $880,000 for the breach, and costs to TJX have been estimated at over $200 million to date.

While TJX Companies has been able to remain in business, the incident highlighted the fact that a single breach of credit card security can have serious repercussions on a business' bottom line. Failure to adequately secure credit card data can not only cause a loss of customer trust and brand loyalty, but may also result in serious penalties under PCI-DSS – including being stripped of the privilege to accept credit and debit card payments.

Yet even compliance with the Payment Card Industry Data Security Standard (PCI-DSS) is not enough. For instance, PCI-DSS does not explicitly require that credit card data be encrypted during transmission over *internal* networks. Thus, PCI-DSS validation and/or compliance failed to prevent the theft of credit card data from Heartland Payment Systems in 2008.

A similar fate befell Hannaford Brothers, where data was illegally accessed from their computer systems during internal card verifications. Interestingly, national and local laws related to consumer data protection, privacy, identity theft and data security require the absolute protection of this data during the course of business operations. Adherence to those laws would presumably have thwarted those data breaches.

Given these stories, consumers have begun to ask, "Is it safe to do business with this merchant? Is my credit card information safe?" Card-issuing banks are likewise concerned, since security breaches by merchants and data processors can cost millions of dollars in credit card replacement and account monitoring.

Legal Facts

For a chronology of data breaches, check out: http://www.privacyrights.org/ar/ChronDataBreaches.htm

Over forty U.S. states have data breach notification laws: http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm

Massachusetts' 201 CMR 17.04(3): *Standards for The Protection of Personal Information of Residents of the Commonwealth* is just one example of state laws requiring the encryption of card holder data.

PCI Compliance

PCI & Encryption

Background
In December 2004, several credit card companies (American Express, Discover, Japan Credit Bureau, MasterCard and Visa)—members of the Payment Card Industry Security Standards Council—released the Payment Card Industry Data Security Standard or PCI-DSS. The PCI-DSS defines regulations to meet six Control Objectives:

1. Build and Maintain a Secure Network
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

Controls and Requirements
The PCI-DSS outlines 12 requirements designed to help meet the Control Objectives. Under the "Protect Cardholder Data" objective, this includes Requirement 3 - "Protect stored cardholder data" - and Requirement 4-- ***"Encrypt transmission of cardholder data across open, public networks."*** While most people recognize the need to encrypt sensitive information "during transmission over networks that are easily accessed by malicious individuals" – as specified by the standard - few recognize the importance of encrypting information sent between back-end systems. Data that is neither stored nor in transmission across open, public networks is vulnerable.

As learned through the experiences of Heartland Payment Systems and Hannaford Brothers, it is not good enough to simply encrypt credit card data in the transmission between consumer and merchant. Stored data (i.e., Primary Account Numbers) must be encrypted. (Section 3.4 requires, at a minimum, that PAN be rendered unreadable anywhere it is stored.) Subsequent retransmissions of the data must be conducted over SSL/TLS connections to ensure that credit card data is secure. In other words, end-to-end encryption should be implemented to avoid liability. In fact, these pending lawsuits allege negligence in failing to properly encrypt data.

Section 4.1 Requires Strong Encryption

Section 4.1.a of the PCI-DSS requires ASVs and QSAs to verify that:

- **strong (at least 128-bit) encryption** (e.g., SSLv.3/TLSv.1.0)* is used wherever cardholder data is transmitted or received over open, public networks;
- **HTTPS appears as a part of the browser** Universal Record Locator (URL), and that no cardholder data is required when HTTPS does not appear in the URL; and
- **only trusted SSL/TLS certificates** are accepted.

Section 4.1.1.a contains similar requirements for wireless networks transmitting cardholder data or connected to cardholder environments.

Data must be rendered unreadable using strong cryptography--Triple-DES 128-bit or AES 256-bit. ASVs must check SSL version, certificate validity, authenticity, and matching server name.

* Anything less than v3.0 of SSL is considered non-compliant (unless SSL 2.0 or older is enabled only for an initial handshake to identify that the browser needs to be updated).

PCI Facts

The PCI-SSC web site is: https://www.pcisecuritystandards.org/

The most current version of the PCI-DSS (v. 1.2) became effective December 2008.

Secure Sockets Layer protocol (or its successor, Transport Layer Security protocol) authenticates web pages and encrypts the data submitted through them.

The first Control Objective of the PCI-DSS --"Build and Maintain a Secure Network"-- is met in part with Requirement 1, which requires maintenance of firewalls to protect cardholder data.

Firewalls control the traffic flow into and out of a company's network. They can also block the transmission of credit card data to unintended destinations.

Section 1.1 of PCI-DSS specifies that certain protocols, such as Secure Sockets Layer (SSL), may pass through the firewall without special justification or documentation.

State Laws & Encryption

Controls and Requirements beyond PCI

Most state laws either require encryption of credit card data or at least provide a safe harbor if data is encrypted. Following California's enactments of SB 1386 and AB 1950, approximately 40 other states have adopted laws that require the protection of sensitive personal information, including credit card numbers.

Merchants are also liable when they capture credit card information in online, card-not-present environments. Below in Figure 1 is a diagram of the external data flows typically requiring SSL/TLS encryption.

No cardholder data should be transmitted unless "HTTPS" appears in the URL.

Whenever a cardholder is asked for his or her information, a secure SSL/TLS session should already be in place. Failure to implement SSL/TLS in this fashion may result in man-in-the-middle attacks that allow a malicious third party to intercept cardholder data.

DigiCert Certificates Offer End-to-End Solutions

DigiCert offers Extended Validation (EV) certificates that provide a greater degree of online confidence.

EV Certificates provide additional trust by consumers and cardholders because they activate a green address bar in web browsers whenever an SSL session is established with a merchant's or issuing bank's EV-validated site.

Beyond the initial customer experience, encryption on back-end systems is equally important, as illustrated in Figure 1.

As cardholder data is sent through payment gateways and credit card interchanges and between acquiring and issuing banks, encryption protects it in case it is intercepted.

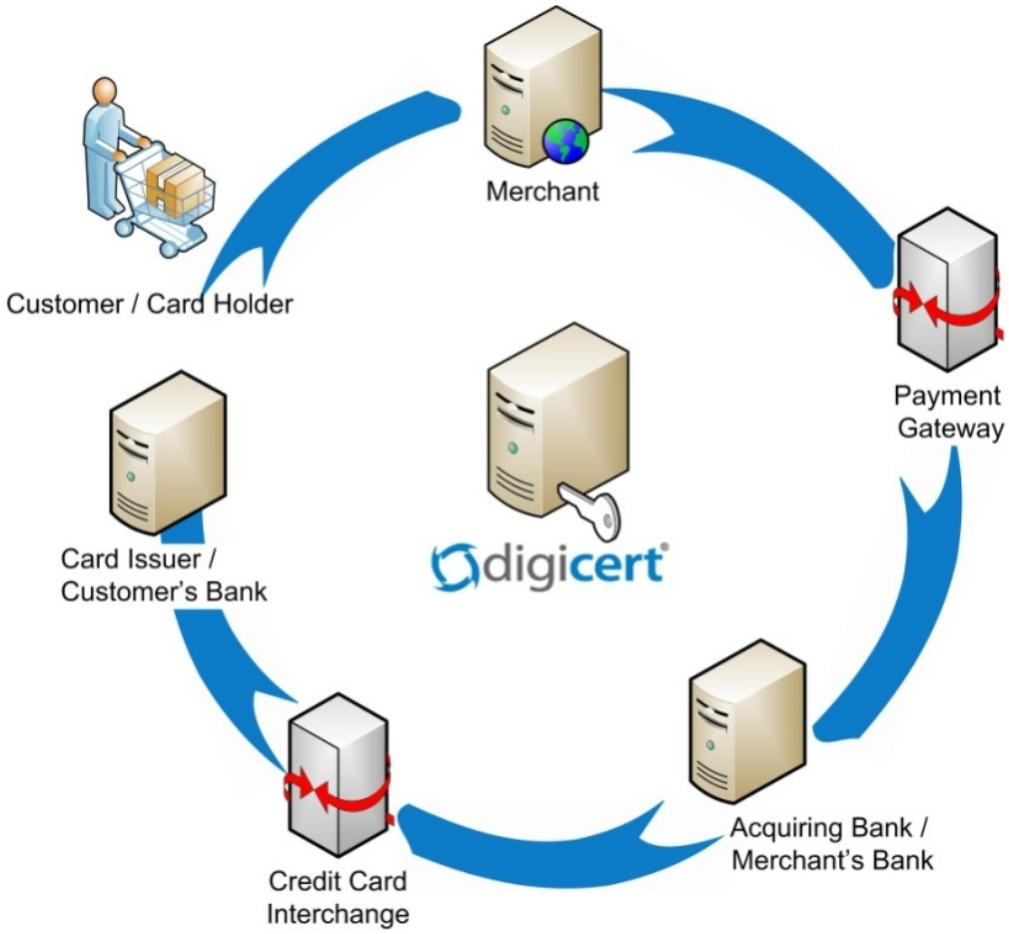

Figure 1.

PCI Facts

PCI Requirement 2 includes section 2.3—"Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS [for the] encryption of all passwords during transmission and storage on all system components…"

According to the PCI-DSS Security Audit Procedures, "All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees' Internet-based access through desktop browsers, or employees' e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems." (PCI-DSS Security Audit Proc., v. 1.1 at p. 9.)

When accessing web sites secured with SSL/TLS, users should make sure that "https" is part of the URL and that the correct address appears in the address bar.

DigiCert and PCI

DigiCert's certificates facilitate encrypted communications among servers and devices with internal and external IP addresses and private names. DigiCert's SSL/TLS certificates include both server and client authentication in the enhanced key usage extension, which means the payment processing network can be configured with certificates to encrypt data transmitted along all points in the processing cycle—see Figure 1.

Conclusion

Failure to encrypt credit card data can result in fines and civil damages in the millions of dollars. PCI and applicable laws require the encryption of cardholder data through the use of SSL/TLS certificates. Such certificates must be issued by a trusted provider. DigiCert is such a trusted provider because its root certificates are embedded as trust anchors in browser software published by Microsoft, Mozilla, Apple, and other browser vendors.

Certificates issued by DigiCert facilitate the encryption of cardholder data during network transmission. DigiCert offers a variety of SSL certificate solutions for the encryption of credit card transmissions including single server / single client, Wildcard, Unified Communications (multiple subject alternative names or SANs), IP-address-only and EV certificates. DigiCert also offers 24x7 support for these payment card encryption solutions.

Practical Tips

Microsoft's Internet Information Server accepts SSL v. 2.0 by default, which will make your site non-compliant. To change this default setting, see: http://technet.microsoft.com/en-us/library/cc755203.aspx

Apache's default SSLv.2 setting can also be changed with the following:
SSLCipherSuite HIGH:+MEDIUM:!SSLv2:!EXP:!ADH:!aNULL:!eNULL:!NULL
See also http://httpd.apache.org/docs/2.0/mod/mod_ssl.html

If your server supports or allows SSL 2.0 or bit rates below 128-bit, you will fail your PCI audit. Check your server's encryption settings by using http://www.serversniff.net/content.php?do=ssl.

PCI Facts

PCI Compliant Ciphers include:

- AES-SHA 128 bit
- DES-CBC3-SHA 168 bit
- RC4-SHA 128 bit
- RC4-MD5 128 bit

Each credit card company still maintains its own security standards program:

http://www.visa.com/cisp/

http://www.mastercard.com/us/sdp/

www.americanexpress.com/datasecurity/

http://www.discovernetwork.com/fraudsecurity/disc.html

http://www.jcb-global.com/english/jdsp

DigiCert, Inc.
355 South 520 West
Canopy Building II
Lindon, UT 84042
+1-800-896-7973 ph
+1-866-842-0223 fax
www.digicert.com

DigiCert, Inc. <http://www.digicert.com/> is a leading provider of enterprise-grade, high-assurance, 256-bit SSL Certificates trusted by many national and state governments, educational and medical institutions, and Fortune 500 companies around the world. DigiCert's commitment to innovation and value provides clients with peace of mind backed by a 100% money-back guarantee and live 24-hour phone, chat and email support, along with intuitive GUI certificate management. Located in Lindon, Utah, DigiCert is a WebTrust Certified Certificate Authority and a member of the CA/Browser Forum, the W3C Consortium, and the Authentication and Online Trust Alliance.

A Unified Communications certificate from DigiCert can secure servers with up to 150 subject alternative names (SANs).

Feedback? Whitepaper Suggestions? We want to know! Send an email to newsletter@digicert.com