



TECTIA CORPORATION

Achieving PCI DSS Compliance with Tectia® Solution

White Paper

May 2010

This document gives an overview of the Payment Card Industry (PCI) Data Security Standard related to the protection of cardholder data transferred over TCP/IP networks. An end-to-end communications security solution based on the robust and proven Tectia® Solution is introduced for strong encryption of file transfer, monitoring and access control in compliance with the PCI DSS security requirements.



PCI DATA SECURITY STANDARD

OVERVIEW

The major credit card associations have collaborated to create a single set of worldwide requirements, called the Payment Card Industry (PCI) Data Security Standard, for consumer data protection across the entire industry. The PCI Data Security Standard aligns the Visa and MasterCard data protection programs, streamlining requirements, compliance criteria, and validation processes. It addresses merchants' and acquirers' concerns of having to meet with more than one set of standards to accomplish a single goal. [1]

The PCI Data Security Standard defines a security framework with six areas of requirements that apply to all members, merchants, and service providers who store, process or transmit cardholder data.

Table 1 PCI Data Security Standard framework [2]

Payment Card Industry Data Security Standard
Build and Maintain a Secure Network (Requirements 1 - 2)
Protect Cardholder Data (Requirements 3 - 4)
Maintain a Vulnerability Management Program (Requirements 5 - 6)
Implement Strong Access Control Measures (Requirements 7 - 9)
Regularly Monitor and Test Networks (Requirements 10 - 11)
Maintain an Information Security Policy (Requirements 12)

The following two sections describe the key PCI requirement areas that can be achieved with a software solution.

TRANSMISSION SECURITY REQUIREMENTS

The PCI Data Security Standard defines twelve requirements, of which requirements 1, 2, 4 and 6 need special attention when implementing compliant transmission security measures.

Requirement 1: Establish firewall configuration standards

“1.2 Build a firewall configuration that denies all traffic from “untrusted” networks/hosts, except for: web protocols – HTTP (port 80) and Secure Sockets Layer (SSL) (typically port 443), system administration protocols (e.g. Secure Shell (SSH) or Virtual Private Network (VPN), or other protocols required by the business (e.g., for ISO 8583).”

1.2 requires implementing security protocols such as SSL, SSH, or IPSec when communicating with external, “untrusted” networks. It leaves some room for interpretation since the terms “untrusted” and “other protocols required by the business” are not clearly defined. However, by implementing the specific protocols mentioned in the requirement, organizations can ensure that they will pass requirement 1.2.

Requirement 2: Do not use vendor-supplied defaults and other security parameters.

“2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.”

Requirement 2.3 enforces the use of security protocols with strong encryption for administrating servers and other network resources. For example, unsecured legacy protocols such as Rlogin, Rsh, and Telnet cannot be used for server administration since they lack encryption. Again, organizations are on the safe side by implementing the specific protocols mentioned in the requirement.

Requirement 4: Encrypt transmission of cardholder and sensitive information across public networks.

Plaintext data is easy to eavesdrop and intercept in TCP/IP networks. Sensitive information is always exposed to third parties when transferred between systems using unencrypted connection protocols such as FTP (File Transfer Protocol).

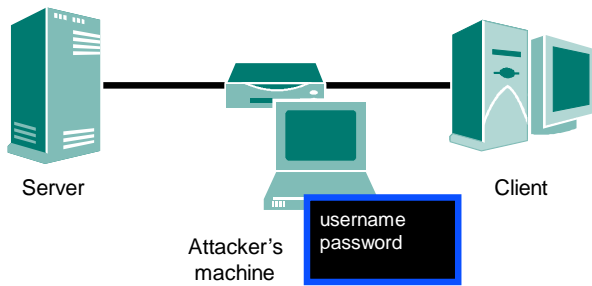


Figure 1 Plaintext data transfers are vulnerable against data eavesdropping

Requirement 4 of the PCI Security Standard specifically mandates the use of strong cryptography and encryption techniques (minimum 128-bit) to safeguard sensitive cardholder data in transit.

Requirement 6: Develop and maintain secure systems and applications.

“Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed via vendor security patches, and all systems should have current software patches to protect against exploitation by employees, external hackers, and viruses. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.” [2]

Deploying patches on time is of paramount importance especially in the case of security software. Running old versions with known vulnerabilities can risk the integrity of the transferred data, even when the transmission itself is encrypted.

When planning and implementing secure transmission security in your system, make sure that centralized and real-time software maintenance is in place.

ACCESS CONTROL AND MONITORING REQUIREMENTS

Of the twelve requirements in the PCI Data Security Standard, requirements 7, 8 and 10 need special attention when implementing compliant access control and monitoring measures using a software solution.

Requirement 7: Restrict access to cardholder data by business need-to-know

“To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. “Need to know” is when access rights are granted to only the least amount of data and privileges needed to perform a job.” [2]

One of the most effective ways to meet the “Need to know” principle is to ensure that the Role Based Access Control (RBAC) model is in use and that the access controls are automated to enable proactive control and security. To ensure the integrity and validity of the user and group privileges, the information should be stored and used in centrally managed fashion.

Requirement 8: Assign a unique ID to each person with computer access

“Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.” [2]

Strong user and service authentication is the core functionality and building block of a secure infrastructure. The PCI-DSS requirements enforce organizations to implement strong two-factor authentication for remote access by employees, administrators and third parties. When selecting the security solution, ensure that it scales to and can be easily deployed also to external partner and end-user environments.

Make also sure that the selected security solution meets all the user authentication and password management requirements stated in 8.5, such as “immediately revoke access for any terminated users”, or “enable accounts used by vendors for remote maintenance only during the time period needed”.

Requirement 10: Track and monitor all access to network resources and cardholder data.

“Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.” [2]

According to Gartner, most of the intrusions that result in significant financial losses are committed by insiders who often have legitimate access to the network [3]. It is extremely important that all the actions especially taken by any individual with root or administrative privileges (Requirement 10.2.2) are controlled and audited by a true third party using encrypted and tamper-proof audit trails.

Sometimes it is also possible for outsiders can gain access to employee credentials, for example due to weak password policies, and then use various methods to connect to internal systems. In either internal or external threads, reliable and centralized monitoring and control of encrypted connections is a critical requirement for a later determination of the true cause of the compromise.

TECTIA® - THE FASTEST TRACK TO ACHIEVE PCI COMPLIANCE





Tectia is the market maker in real-time information security for modern, networked organizations.

With the Tectia Solution you have the fastest track to real-time information security with respect to the PCI-DSS.

- Centralized environment monitoring allows real-time detection of system anomalies and threats. Fast deployment with no business disruptions (Customer case from retail industry: 75% faster than the competition; nearly 6,000 servers in 6 weeks)
- Connecting your people and business network securely to confidential data, connecting the right people, the right information, anytime, anywhere (Customer cases from automotive industry and retail industry)
- Automating real-time information security for low-risk, low-cost file transfer systems (Customer case from a European railway company)
- Enforcing your security controls with the strongest solutions, maintaining visibility and control of secure information flows (Customer cases from retail industry and space administration)
- Bridging the compliance gap, protecting operational integrity (Customer case from retail industry)
- Protecting your secrets and custodial data, maintaining customer loyalty and business goodwill, building your brand (Customer cases: 80% of the top 100 financial institutions).

This section explains how the Tectia Solution can help in complying with the key PCI Data Security Standard requirements related to cardholder data transmission.

PCI-DSS Compliance Area	#	PCI-DSS Requirements	Tectia Solution Support for PCI-DSS																	
Build and Maintain a Secure Network	1	Install and maintain a firewall configuration to protect cardholder data	1.1	1.2	1.3	1.4														
	2	Do not use vendor-supplied defaults for system passwords and other security parameters	2.1	2.2	2.3	2.4														
Protect Cardholder Data	3	Protect stored cardholder data	3.1	3.2	3.3	3.4	3.5	3.6												
	4	Encrypt transmission of cardholder data across open, public networks	4.1	4.2																
Maintain a Vulnerability Management Program	5	Use and regularly update anti-virus software	5.1	5.2																
	6	Develop and maintain secure systems and applications	6.1	6.2	6.3	6.4	6.5	6.6												
Implement Strong Access Control Measures	7	Restrict access to cardholder data by business need-to-know	7.1	7.2																
	8	Assign a unique ID to each person with computer access	8.1	8.2	8.3	8.4	8.5													
	9	Restrict physical access to cardholder data	9.1	9.2	9.3	9.4	9.5	9.6	9.7	9.8	9.9	9.10								
Regularly Monitor and Test Networks	10	Track and monitor all access to network resources and cardholder data	10.1	10.2	10.3	10.4	10.5	10.6	10.7											
	11	Regularly test security systems and processes	11.1	11.2	11.3	11.4	11.5													
Maintain an Information Security Policy	12	Maintain a policy that addresses information security	12.1	12.2	12.3	12.4	12.5	12.6	12.7	12.8	12.9									

-  PCI-DSS Compliance can be achieved fully with Software
-  PCI-DSS compliance cannot be achieved by software only
-  Supported fully by Tectia Solution
-  Supported partially by Tectia Solution

Requirements 1 and 2 explicitly specify Secure Shell as an accepted security protocol for use when connecting over untrusted networks and for all non-console system administration access. The Tectia Solution is based on the IETF-standard Secure Shell, and is developed and supported by the original developers of the protocol.

Requirement 3: Protect stored cardholder data.

Tectia MFT Portal provides a secure and easy-to-use web interface for external and internal data transfers, and allows enterprises to share a variety of different data types in a uniform way hiding all the background details from the end users. Tectia MFT Portal allows also limiting the storage retention time to that which is required for business, legal, and/or regulatory purposes (PCI-DSS 3.1). In addition, the Tectia solution protects cryptographic keys used for encryption of cardholder data against disclosure and misuse (PCI-DSS 3.5).

Requirement 4: Encrypt transmission of cardholder and sensitive information across public networks.

The Tectia Solution encrypts transmission of files, terminal connections, and application traffic over the TCP/IP networks, eliminating the possibility to eavesdrop cardholder data in transit. It fulfills the PCI Data Security requirements by supporting the industry-standard encryption algorithms, such as 3DES and AES without key size limitations.

The encryption libraries used by the Tectia Solution are FIPS 140-2 certified, which means that the cryptographic implementation has successfully undergone an extensive security evaluation by a trusted third party.

The Tectia Solution is available for all key enterprise platforms, and it provides secure cross-platform connectivity across heterogeneous environments

consisting of Windows, Unix, Linux, and IBM mainframes. The high-performance SSH G3 architecture and mainframe hardware acceleration enable strong encryption with minimum impact on system performance.

Tectia Solution secures transmission of cardholder data end-to-end and throughout cross-platform networks.

Requirement 5: Use and regularly update anti-virus software or programs.

Tectia MFT Events can be set to trigger automatic anti-virus check on local or remote files and folders, and to send alerts or perform post-processing operations (delete, copy, move, alert, etc) depending on the virus scan result. The Tectia Solution relies on third-party anti-virus software for performing the scans. As a real-life Tectia solution use case for achieving PCI-DSS compliance, Tectia MFT Events is being used with MFT Portal for virus scanning files transferred by partners to corporate networks.

Requirement 6: Develop and maintain secure systems and applications.

Tectia Manager provides centralized management to reduce total costs in large environments and to improve overall system security. The key Tectia Solution features and benefits related to the requirement 6 include the following:

- Rapid and reliable deployment of the latest Tectia Solution updates throughout multi-platform networks eliminates the possibility to exploit known vulnerabilities.
- Centralized environment monitoring allows real-time detection of system anomalies and threats.
- Centralized configuration management ensures that communications security measures stay consistent with the security policies at all times.
- Centralized host-key management eliminates manual error-prone processes and increases system trust and reliability.
- Tectia Corporation follows strict quality assurance processes with extensive code reviews and testing to minimize software vulnerabilities.

Requirement 7: Restrict access to cardholder data by business need-to-know.

With the Tectia solution you can fully utilize your centralized user database to ensure proper user and group access control, and that the privileges are assigned to individuals based on their job classification and function.

The transparent monitoring and access control capabilities of Tectia Guardian enable you to enforce automated and thorough access controls also for the encrypted connections.

Requirement 8: Assign a unique ID to each person with computer access.

All the components of the Tectia Solution Suite can be adapted to your existing authentication solution and processes to ensure smooth migration and minimal impact to processes and user experience.

With Tectia MobileID you can easily and cost-effectively activate strong two-factor authentication not only for your administrators and internal employees, but also for your business partners, external end users and other third parties, as described on the PCI DSS requirement 8.3.

To ensure the authentication and password requirements, the Tectia Solution can be used to audit, control, restrict and force access rules and management policies for end users as well as for un-attended systems.

Requirement 9: Restrict physical access to cardholder data.

Tectia is a software solution and does not provide physical access security.

Requirement 10: Track and monitor all access to network resources and cardholder data.

The Tectia solution enables centralized tracking, monitoring and archiving of secure remote administration and data exchange operations to network resources and cardholder data.

Tectia Guardian provides a transparent monitoring and control for encrypted remote administration and data exchange operations, and produces tamper-proof audit files for replay and search operations. The advanced monitoring, replay and search functionalities can also be used for graphical remote administration connections, such as remote Windows administration.

Tectia Guardian access control can be completely isolated from normal administration operations and privileges, which makes it a true third party for auditing operations and ensuring the integrity of the audit information.

Encrypted Secure Shell connections and secure file transfer operations can also be audited and tracked with Tectia Manager and MFT Auditor to gather a centralized audit database for statistics, troubleshooting and auditing.

Requirement 11: Regularly test security systems and processes.

Tectia Guardian allows integration to Intrusion Detection Systems (IDS), supporting also analysis of encrypted traffic (PCI-DSS 11.4).

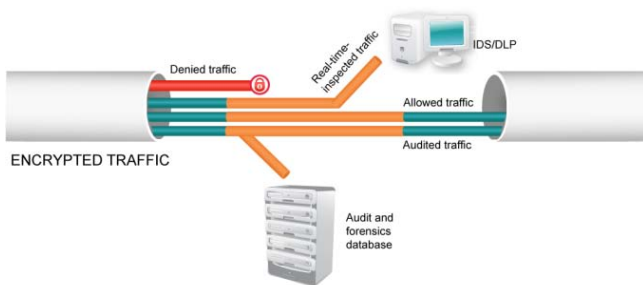


Figure 2. Tectia Guardian allows IDS for SSH, RDP, VNC, X11, Telnet and TN3270 protocols

Requirement 12: Maintain a policy that addresses information security for employees and contractors.

The Tectia Solution allows developing usage policies for critical employee-facing technologies such as remote-access authentication with two-factor authentication. With Tectia Mobile ID you can:

- Increase security for accessing critical systems with minimal effort from end users (PCI-DSS 12.3).
- Activate new users, partners, and ad-hoc accounts in minutes compared to days or weeks.

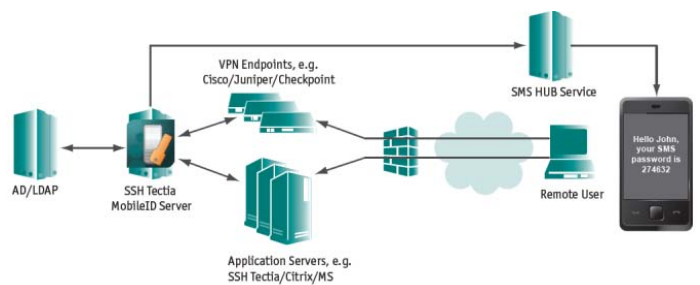


Figure 3. Tectia MobileID provides an additional layer of security by using two different methods to verify the user's identity.

EXAMPLE USE CASE

This section describes a use case where a retailer is using the Tectia Solution for securing file transfers and application connections between retail store servers and corporate back-office systems. Additional case studies of installations of Tectia Solution at leading U.S. and international retailers are described in [5].

RETAILER NETWORK AND CUSTOMER NEED

The retailer has deployed dedicated servers in some of the stores in order to streamline the integration of the local environment with the back-office system. These in-store servers handle all external connections between the store and the corporate data-centers over the TCP/IP-based retail network. The local servers are running common Windows, Linux, and Unix server operating systems.

Some of the local stores have point-of-sale (POS) equipment that directly connects to the back-end systems. These POS machines are running on the Windows operating system.

For marketing and customer history data collection, sensitive cardholder data is regularly transferred between the stores and a centralized IBM mainframe back-office system. While security measures are already in place for securing external credit card processing connections, the internal retail network is still running a variety of different transport protocols including plaintext FTP for transferring sensitive data.

Better cardholder data protection and compliance with the PCI transmission security requirements are among the key drivers for implementing comprehensive communications security solution in the retail store network.

TECTIA® SOLUTION

The retailer uses the Tectia Solution for ensuring confidentiality of all customer data when transmitted over the TCP/IP retail network. The data-in-transit is secured across cabled as well as wireless local area networks.

Cost-Effective Transmission Security

The Tectia Solution is available for all commonly used in-store server platforms including Windows, Unix, and Linux servers. The Tectia Solution allows seamless cross-platform connectivity between the store servers and the centralized IBM mainframe.

The Tectia Solution is an ideal solution for deploying cost-effective encryption and authentication of automated file transfers that contain sensitive cardholder data. Additionally, Tectia Client and Tectia Server provide a transparent application tunneling capability for the retailer, allowing easy tunneling of retail application connections without costly application-level modifications.

Tectia ConnectSecure is being used to quickly and cost-effectively protect the file transfers for the POS systems without modifications to infrastructure, scripts, or the POS applications.

Secure Server Administration

In addition to cardholder data protection, the Tectia Solution allows remote administration of all in-store servers. Through the secure terminal server and file transfer server capability, the retailer's system administrators are able to remotely and securely manage in-store servers over TCP/IP networks.

A Bonus: Centralized Management

As an additional benefit, the retailer is able to centrally manage and monitor secure communications in the network. Centralized Tectia Solution management helps the retailer to comply with the requirements 6 and 10 (secure system development and centralized network monitoring). The total cost of ownership is also reduced through automation of time-consuming administration tasks such as software maintenance.

CASE STUDIES OF DEPLOYED TECTIA SOLUTIONS

Case studies of how leading international retailers use the Tectia Solution to secure payment card data and other sensitive corporate data can be found on the Tectia web site at:

<http://www.ssh.com/resources/material/case/>.

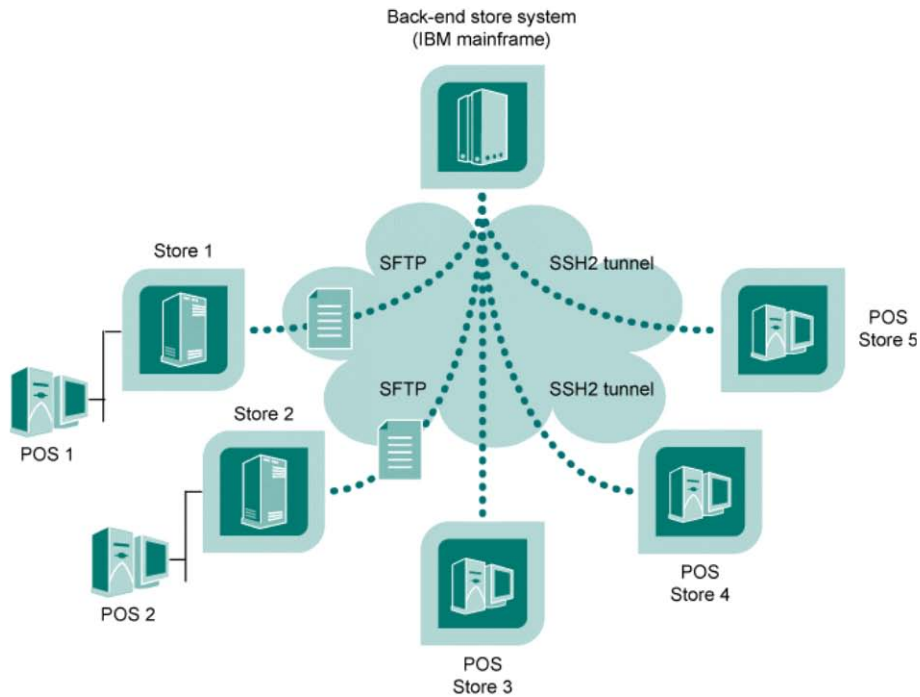


Figure 4 Example use case: securing a retail network with Tectia Solution

REFERENCES

[1] Visa Security Programs:

<http://corporate.visa.com/st/programs.jsp>

[2] PCI Data Security Standard specifications:

http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf

[3] Gartner website:

<http://www.gartner.com/>

[4] Tectia Solution brochure:

<http://www.ssh.com/resources/>

[5] Tectia Solution Case Studies:

<http://www.ssh.com/resources/material/cas>