



S2S Communications PCI –DSS Standard Adherence Mapping

PCI Data Security Adherence

The Payment Card Industry (PCI) published its most recent (Version 1.2) Data Security Standard on October 1, 2008. Corporations that acquire personal cardholder data and process this information through network and computing systems are required to comply with PCI mandates. The PCI-DSS standard consists of twelve (12) high-level requirements.

The S2S VPN solution utilizes customer premise-based hardware. Specifically, S2S will locate head-end VPN concentrators in one or more of the customer’s data centers side-by-side with other existing corporate network and computing assets. For purposes of this discussion, we will assume that those other assets have been configured and maintained in accordance with PCI standards. During the design and engineering phase of the project, S2S will work collaboratively with the customer’s IT Network and Security personnel to implement best practices with respect to firewalls and other access mechanisms in order to separate store from the general corporate network infrastructure. By doing so, we are able to confine exposure of personal information to those segments that are absolutely necessary and essential to the flow and storage of credit card data within the network and computing environment.

The table below sets forth statements of adherence mapped to the various requirements in the PCI-DSS Standard as applied in the context of S2S’s managed network solutions.

PCI -- DSS Standard Requirement	S2S Adherence Statements
1. Build and maintain a secure network	<ul style="list-style-type: none"> Define firewall and network segmentation policies and parameters per Customer requirements. Provide documentation of network and security design and configuration. Provide controlled access and logging to all associated network components. Note that S2S offers an optional event logging and reporting service with ability to generate reports in a PCI template format. Provide configuration management for all devices managed by S2S. Coordinate all configuration change management.
2. Do not use vendor-supplied defaults for system passwords and other security parameters	<ul style="list-style-type: none"> Device access credentials will be generated by S2S using strong password practices. Credentials are also cycled through certain change requests. Devices will be accessed using secure shell (SSH). 802.11 will utilize WPA credentials of bit length defined by customer and TKIP/AES 256-bit used for encryption dependent upon device capability. Network OS patches applied for medium and higher



S2S Communications PCI –DSS Standard Adherence Mapping

	published levels of security vulnerability.
3. Protect stored cardholder data	<ul style="list-style-type: none"> S2S solution does not store any cardholder personal data. This information is only transmitted across the VPN network between two or more customer internal networks.
4. Encrypt transmission of cardholder data across open, public networks	<ul style="list-style-type: none"> S2S will engineer the VPN network solution to provide IPSec strong encryption level (3DES, 256-bit AES) for local and wide area communications to and from VPN site, head-end and in-store devices.
5. Use and regularly update anti-virus software or programs	<ul style="list-style-type: none"> The S2S solution does not incorporate subscription based network AV scanning/quarantine or IPS services. It is assumed that the customer has implemented necessary measures on all associated workstations and core network infrastructure used to store and transfer cardholder data. S2S can optionally provide these subscription based security layered services utilizing Juniper VPN Unified Threat Management devices.
6. Develop and maintain secure systems and applications	<ul style="list-style-type: none"> S2S software components used in our solution, such as the customer portal, do not store or display cardholder information. S2S VPN network and device configurations will support any of the standard protocols and encryption methods required per the customer’s workstation and application environment.
7. Restrict access to cardholder data by business need to know	<ul style="list-style-type: none"> S2S enforces strong access credentials for all associated network devices and, furthermore, in our fully managed solution, these credentials are stored in credential management software such that only personnel directly engaged in configuration and operational management of the VPN network have access to these credentials. Device access credentials are generated for read-write and read-only privilege granularity based upon operation function, thus need to know. The S2S VPN network and associated components does not store cardholder data, thus access is only granted on a need to know basis for network elements that are used to transmit cardholder data.
8. Assign a unique ID to each person with computer access	<ul style="list-style-type: none"> This requirement generally refers to credential management associated with user access to a PC or workstation device that may have access or contain cardholder information. These systems are not used in the S2S solution, only access to network devices in which



S2S Communications PCI –DSS Standard Adherence Mapping

	cardholder data is not available.
9. Restrict physical access to cardholder data	<ul style="list-style-type: none"> • S2S network elements do not contain/store cardholder information. • S2S network elements are physically placed at the customer premise, both remote store locations and data center(s).
10. Track and monitor all access to network resources and cardholder data	<ul style="list-style-type: none"> • S2S offers an optional event logging/reporting service. Events, such as device access authentication, success/failure, firewall exceptions, etc. are captured from network elements and presented in a portal with dashboard and reporting views. • S2S has the ability to generate the above reports containing detailed audit trails in a PCI reporting template.
11. Regularly test security systems and processes	<ul style="list-style-type: none"> • S2S works collaboratively with the customer to participate and support any required periodic network layer and security testing practices and procedures.
12. Maintain a policy that addresses information security for employees and contractors	<ul style="list-style-type: none"> • Security vulnerabilities are continually assessed as published by product vendors used in the S2S VPN solution. OS patches are made based on severity of impact and per vendor recommendations (Juniper, Cisco, etc.). • All of our global network/security operations centers (GOCs) have comprehensive security and operational policies and practices that have been assessed and certified per SAS-70 type II and ISO 27001. They are also certified for ISO 20K for the latest ITIL best practices.