PCI DSS 3.2 Requirements & Compliance of NewNet Secure Payment Transaction Systems

A REPORT FROM NEWNET COMMUNICATION TECHNOLOGIES, LLC

NewNet
SECURE TRANSACTIONS

NewNet & PCI Security Council

NewNet Communication Technologies, LLC, is a Participating Organization of PCI Security Standards Council. NewNet works with the Council to achieve and improve payment data security worldwide through the ongoing development of the PCI Security Standards, including the Payment Card Industry Data Security Standard (PCI DSS), PIN Transaction Security (PTS) requirements, Payment Application Data Security Standard (PA-DSS), PCI Point-to-Point Encryption (P2PE) requirements etc.

Endorsed by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc., the PCI Security Standards require merchants and service providers that store, process or transmit customer payment card data to adhere to information security controls and processes that ensure data protection. To enhance payment data security globally while embracing new technologies as they are developed, the Council relies on involvement of those across the payments processing chain, from merchants and service providers to payment device manufacturers and software developers, financial institutions and processors.

As a Participating Organization, NewNet adds its voice to the standards setting process and receive previews of drafts of standards and supporting materials in order to provide feedback to shape their final versions, as well as engage a growing community of more than 600 organizations united to improve payment security.

NewNet Payment Systems & Security

Security is handled with paramount importance on NewNet's payment transaction products and applications for all types of innovative mobile, broadband, dial transaction services. This involves the data security as well as the network security and barriers to prevent, deter and detect attempts to intrude. With applications having full know how of the transaction protocols and applying advanced methods of deep packet inspection and verification of transaction protocols and data, NewNet's products ensure that the mobile, broadband and dial transaction users and providers can be assured of the security of the transactions.

NewNet's AccessGuard 1000 (AG1000) and Total Control Secure Transaction Gateway (TC STG) employs a wide array of security, transaction user data safety and monetary loss avoidance procedures which make the best use of the industry standards and beyond the industry specifications including digital certificates, PIN numbers, SSL sessions, userid & passwords, multi-factor authentication, split key authentications, advanced cryptographic standards, longest key length encryptions, dynamic access controls, SSH access, multiple device verifications, real time reporting, transaction verifications on-the-fly, transaction value based verifications, end to end encryption, secondary data encryption, IPSec tunneling, multi-layer user approval requisitions, 2D barcode tokens, PKI procedures etc.

NewNet proposes and offers several advanced and enhanced Security Services for traditional and emerging payment models with the objective to make the security of transactions impenetrable and even push this to the extent of having no sensitive data being available in the vulnerable space for the attackers to target. As with traditional card payment transactions and even with mobile wallet or generic mobile based transactions the cardholder data is still transferred over the transport networks each time a transaction is made. While there are several security measures in place and compliance requirements available it would be most efficient if this data could be safely stored at secure data centers and not required to traverse cross country public networks. Several mechanisms including tokenization and similar one time usage security solutions together with end to end encryption methods are part of NewNet systems portfolio to address the security concerns of PCI.

These solution models offer several benefits including the following:

- Enables the payment transactions from traditional payment modes and emerging mobile devices
- Avoids the need to store credit/debit card data on POI devices, mobile devices etc
- Prevents the transfer of sensitive card data across public networks
- Leaves no card information with the merchant terminals
- Ensures that card data remains on secure databases and accessed over secure private networks

PCI DSS Requirements

1: Install and maintain a firewall configuration to protect cardholder data
2: Do not use vendor-supplied defaults for system passwords and other security parameters
3: Protect stored cardholder data
4: Encrypt transmission of cardholder data across open, public networks
5: Use and regularly update anti-virus software or programs
6: Develop and maintain secure systems and applications
7: Restrict access to cardholder data by business need to know
8 : Assign a unique ID to each person with computer access
9: Restrict physical access to cardholder data
10: Track and monitor all access to network resources and cardholder data
11: Regularly test security systems and processes.
12: Maintain a policy that addresses information security for all personnel.

NewNet Systems' PCI DSS Compliance Conformation

NewNet solutions of AG1000 and TC STG have been put through the rigor of strongest security validation procedure and are always in the endeavor to exceed the security requirements laid down by PCI DSS. Beyond meeting the requirements, it is NewNet's vision to elevate the security of transaction through the NewNet systems to have a cut above the rest in terms of absolute security combining our decades of experience in Networking, Security and Payment transactions.

NewNet's strong legacy in the field of networking, security and payment is unmatched in the industry with pioneering roles in these domains over the last 30 years in several incarnations and industry's direction defining stewardship in each of these areas. NewNet's payment products have expanded from this strong legacy and remarkable inheritance in the respective fields of TCP/IP Networking, Payment transaction systems and Security solutions (with the earliest Ethernet systems, the first X.25 payment solutions for Mainframe systems and one of the earliest Security Solutions in the industry) into a confluence of inimitable product and technology capabilities with incomparable mastery and excellence.

AG1000 and TC STG systems are target built for transaction routing process with unique and exclusive purpose to support the secure payment transaction switching and routing functions only. These systems use industry grade servers with proprietary hardware boards for modem traffic handling, cryptographic processing and high security key storage functions. The system Hardware and Operating System has a strict enforcement setting for all aspects of security of data, network, user access; and external threats mitigation and physical risk handling.

AG1000 and TC STG uses industry proven carrier grade servers equipped with an array of measures to Harden the systems for proofing these to use in payment transaction environments. The applications on these Servers are custom design for secure payment transaction aggregation, switching and routing only. PCI DSS compliance measure covers the defense against external attacks, virus threats, physical security intrusion etc. Physical ports are rendered inaccessible, barring the network accessing interfaces for TCP/IP or PSTN with full security for the sessions over these. Non-transaction application related users, services, ports, binaries etc are summarily blocked. Apart from the HW and OS security measures, the payment transaction handling application on the NewNet systems are further audited and verified for full compliance with PCI DSS requirements.

1. Install and maintain a firewall configuration to protect cardholder data

AG1000 & TC STG do not store card holder data and allows strict security for the data in transit by enforcing the data to be encrypted and handled within internal firewall rules while working with external firewall systems

2. Don't use vendor-supplied defaults for system passwords or other security parameters

Strict password policy enforced as per the standards for system remote access as well as console port access. Configuration access is provided over IPsec for Common Element Manager and AG1000 / TC STG secure communication. OS is hardened as per CIS benchmarking standards.

3. Protect stored cardholder data

Cardholder data is not stored on AG1000 & TC STG. Data is only routed through the system with high security and strong encryption without any storage.

4. Encrypt transmission of cardholder data across open, public networks

Encryption procedures with SSL/TLS, IPSec, SSH, SCP, HTTPS, DUKPT with 3DES/AES etc are utilized with public networks. Beyond the HW controls, the Operating System is hardened for exclusive usage in payment transaction environment. Application is target built for payment transaction switching and routing function with excessive security and compliance measures in place as per PCI DSS requirements. Key storage utilizes FIPS 140-2 Certified HSM modules offering the latest and most advanced security mechanism in the industry.

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

Facilitates antivirus systems to be scan folders, files and directories as wished by the security administrators with periodic updates.

6. Develop and maintain secure systems and applications

Follow the industry standard secure coding guidelines for software design, development, test, upgrade and maintenance processes. The physical structure of the system has tamper evident stickers which will deter attempts to physically open the box by unauthorized users other than by NewNet's designated personnel.

7. Restrict access to cardholder data by business need to know

No card information stored on the systems and while in transit the card data is in the encrypted form at all times with absolute protection from user access. AG 1000 and TC STG system uses Certificates for identification and authentication; remote and local user access is restricted by strong password policies; the TCP/IP interfaces are protected by packet filtering rules.

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

Stringent user access administration process is enforced to ensure multiple users with unique & distinct user ids for purposes of system management, operations, monitoring etc. Multi-level and multi factor authentication process provided for additional security. AG1000 and TC STG system HW restricts physical network access to system via GigE ports for TCP/IP networks, T1/E1 ports for PSTN networks or through console ports only. Console access is password protected and restricted by strict access control measures and stringent timeout mechanisms for inactivity detection and session closure.

9. Restrict physical access to cardholder data

Cardholder data not retained on the AG1000 / TC STG at any time and transferred over encrypted sessions with no physical access to users. HW encryption mechanism is on-board the system and provides security for the data accesses through the system.

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

All event occurring on the system including application user access events, system management events, user read/write events are logged. User access is completely restricted and log are retained for forensic purposes which can be can be viewed only by user with administrative privilege

11. Regularly test security systems and processes

Facilitates customer's security process to run tests on security controls for identifying any environmental changes and detect any changes occurring in the system including file structures, log files, system files etc.

12. Maintain a policy that addresses information security for all personnel

Supports the strict enforcement of the information security policy by establishing measures for enhanced controls for security of system access, network connectivity, and data safety while transit on the AG1000/TC STG systems.

The fundamental security policy is a deny-all mode with selective restricted access for applications and authorized users on need-to-access basis only. On these systems each and every resource access is denied by default, and permissions are applied on need basis that gives each user element or service element of the system only the access required to function within its defined boundary. If a service or user subsequently tries to access or modify a file or resource not necessary for it to function, then access is denied, the action is logged and even application may be halted requiring administrative intervention.

DSS Compliance Matrix

PCI DSS Requirements	AG1000/TC STG Compliance Status
1. Install and maintain a firewall configuration to protect cardholder data	Conformant
2. Don't use vendor-supplied defaults for system passwords or other security parameters	Compliant
3. Protect stored cardholder data	Compliant
4. Encrypt transmission of cardholder data across open, public networks	Compliant
5. Use and regularly update anti-virus software or programs	Conformant
6. Develop and maintain secure systems and applications	Compliant
7. Restrict access to cardholder data by business need to know	Compliant
8. Assign a unique ID to each person with computer access	Compliant
9. Restrict physical access to cardholder data	Compliant
10. Track and monitor all access to network resources and cardholder data	Compliant
11. Regularly test security systems and processes.	Conformant
12. Maintain a policy that addresses information security for all personnel.	Conformant

Specific requirements of PCI are applicable to AG1000 and TC STG directly and those are completely complied with the requirements the systems are fully compliant. Few requirements are generic to Datacenter environment and have dependencies on additional systems in the environment apart from AG1000 and TC STG themselves. For these requirements as well, NewNet systems are completely conformant which indicates that AG and TC STG systems offer the necessary provisions by itself to comply with the requirement and facilitates the overall Datacenter environment to be compliant.

System Security Summary

AG1000 and TC STG systems being custom application built specifically for transaction aggregation, switching, routing and transport function; the Linux OS version (CentOS 6.4) utilized is tailored to meet this with the required security needs for payment transaction handling.

The system supports and performs the following from a secure operations perspective of the Operating System:

- Enables and supports only the application specific users
- Uses secure means of remote access and secure file transfers
- Follows the password policies for secure systems
- Avoids usage of unwanted services
- Allows only those ports which are needed for transaction routing and related functions
- Logs all transaction application related actions on the system
- Maintains a fixed file structure

The security measures on the NewNet systems not only make the deployed networks compliant with the security standards requirements of PCI DSS, but also promotes a comprehensive security culture by means of the security sensitized procedures employed for handling the payment systems through the management tools and the restrictive measures for user access thus providing a fully secure system for the customers.

About NewNet Communication Technologies, LLC

NewNet Communication Technologies, LLC is a global provider of innovative solutions for next generation mobile technology. For over 25 years, NewNet has enabled global operators and equipment manufacturers to rapidly develop and deploy cutting edge, revenue generating solutions needed to build, grow and improve global communications.

NewNet specializes in Mobile Messaging, Secure Transaction Transport, Interactive Voice Response, Real Time Charging and Rating, Wireless Broadband and Network Optimization solutions that have reached millions of end users in over 90 countries.

720 East Butterfield Road. Suite 250
Lombard, IL 60148

+1 224-795-5200

www.newnet.com

traxcominfo@newnet.com

NewNet
SECURE TRANSACTIONS