Payment Card Industry Data Security Standard (PCI DSS)

Organization Compliance with OmniAccess Stellar WLAN

White Paper
Alcatel-Lucent Enterprise Technology Compliance with PCI-DSS

Content

PCI DSS Definition

The Payment Card Industry Data Security Standard (PCI DSS) applies to companies of any size that accept credit card payments. PCI DSS is the worldwide Payment Card Industry Data Security Standard that has the prime goal to help businesses process card payments securely and reduce card fraud.

To put it in place, it is necessary to enforce tight control surrounding the storage, transmission and processing of cardholder data that businesses handle. PCI DSS is intended to protect sensitive cardholder data.

Specific guidelines to protect point-of-sale data over the wireless network, need secure infrastructure, implementation guidelines to keep the card payment transactions secure end to end.

The payment standard has twelve (12) high level requirements that can be resumed in six categories:

Build and Maintain a Secure Network

1- Install and maintain a firewall configuration to protect data
2- Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3- Protect stored data (use encryption)
4- Encrypt transmission of cardholder data and sensitive information across public net

Maintain a Vulnerability Management Program

5- Use and regularly update anti-virus software
6- Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7- Restrict access to data by business need-to-know
8- Assign a unique ID to each person with computer access
9- Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10- Track and monitor all access to network resources and cardholder data
11- Regularly test security systems and processes

Maintain an Information Security Policy

12- Maintain a policy that addresses Information Security

Alcatel-Lucent Enterprise PCI DSS certification strategy

Cybersecurity is a top priority for organizations, while they embrace the need for digital transformation. Digital transformation is enabling more connected and mobile devices on their networks, while increasing access to applications and data from beyond the network perimeter. As change accelerates, the old methods of network security can no longer keep up.

With these emerging challenges, the industry's approach to security cannot remain traditional. Organizations often implement security simply to tick the compliance boxes and don't consider changes due to digital transformation that impact security requirements.

Security needs to be an embedded part of the broader enterprise digital environment, to meet and exceed beyond the PCI DSS compliance adherence that organisations need to achieve.

Key aspects of layered network security technology should include:

- **Endpoint security** - To manage vulnerabilities for individual devices.

- **Trust management** - Organisations need a risk management approach that addresses the fact that users and resources can reside outside the network perimeter. One way to establish trust in such an environment is by understanding what constitutes normal and abnormal behaviour on the network. Artificial intelligence (AI) enabled tools for identity and authorisation management enable you to establish a normal baseline for behaviour on the network. These tools can evaluate each user and device and their application, security, and quality of service requirements to establish a normal baseline behaviour. Thereafter, AI can quickly identify any unusual events or actions and analytics that help determine why something has changed.

- **Identity management** - To authenticate users and control access. The solution should provide user authentication capabilities and fine-grained security policies that grant users just the right level of access to only the information they need.

- **Secure data exchange** - The use of encryption and secure file exchange protocols should safeguard data in motion. Encrypt network uplinks at the access, aggregation and network core & DC connections; this can be accomplished through the implementation of MACsec with MKA dynamic key assignments to maintain data integrity across the private network

- **A service defined architecture** - An automated network that is centrally managed can provide the speed required to keep up with digital transformation while enforcing the right security. Implement information and network security best practices framework to maintain the highest end-to-end network integrity guidelines via i) WLAN access that provide distributed intelligence, secure connectivity and mobility ii) Intelligent network of switches running dynamic and service defined network features such as automatic network provisioning for LACP, layer 3 services, auto SPB service provisioning for dynamic and high-performance network connectivity, etc.

- **Containerisation** - To prevent threats from jumping from one system to the next once a threat has gained access to the network, the solution should use containerisation and network segmentation to isolate individual systems. Implement Role based users & user group management by assigning PCI dependent devices & applications to be dynamically and securely assigned to network virtual containers via device profiling and fingerprinting features to further help maintain network integrity.

Strategy

Instead of implementing the minimum cybersecurity to achieve PCI DSS compliance, organizations should take the opportunity to develop a strategic security plan that manages risk in a manner that meets the demands of today's digital transformation context. They should:

- Think of regulatory compliance as a starting point. While many organizations start by doing the minimum necessary to comply with GDPR, PCI DSS, or other equivalent regulations outside of Europe, the organizations should think of regulatory compliance as a starting point for rethinking the way they're managing and governing data within their organizations and with their partners.

- Understand that security drives business value by ensuring business continuity. Organizations must avoid lost revenue that result from cyberattacks that take down IT systems or stolen information. Align security with your broader enterprise objectives and make it a part of your everyday business.

- Follow a security by design approach: Risk goes 'together with business workflows, which are constantly evolving along with technologies. The organizations must incorporate security into workflows from the start. Security needs to be a core business value and complement every business decision organizations make.

- Work with the ecosystem. Organizations no longer have a clear perimeter to defend. They need to work with the ecosystem to maintain cybersecurity.

Technology

Creating a secure connected ecosystem becomes paramount as organizations digitally transform their operations.

This ecosystem requires a layered approach that places the four core disciplines of security

- Identity management
- Vulnerability management
- Threat management
- Trust management

into a new dimension enabling scalability, velocity, intelligence and automation. See the technologies that applies to ALE OmniSwitches and OmniAccess Stellar WLAN solutions.

The Digital Age Networking Alcatel-Lucent Enterprise solution

- Alcatel-Lucent Enterprise Digital Age Networking is a multi-faceted approach to organization networks cybersecurity that provides security in depth for connected devices and applications through multiple layers of security.

Flexible connectivity through a Service Defined Network

- Our approach starts with a flexible, service defined network that makes it fast and easy to configure network and cybersecurity policies for the vast number of connected users, devices and applications that fuel digital transformation.

- In the past, IT has been a break-it/fix-it operation. IT would install new equipment, get it up and running, and manage the network using tedious manual processes. Digital Age Networking is a smart, automated network that makes it easy to connect users and devices to their specific applications in a secure manner. Built using Alcatel-Lucent Enterprise's Intelligent Fabric (iFab) technology, Digital Age Networking includes our homegrown Intelligent Fabric combined with industry-standard Shortest Path Bridging (SPB). Together, these technologies simplify the creation and

configuration of networks while enabling multipath routing and link aggregation to combine multiple network connections in parallel and thereby increase throughput and provide redundancy.

- With Alcatel-Lucent Enterprise's approach, IT defines network services, architecture, access policies and containers and the network builds itself out automatically. Once the network is architected, if anything is moved, changed or added, the network makes the necessary adjustments automatically and undetectably. For example, if a switch goes out of service, the network will automatically reroute around that switch.

- Using a service defined network, organizations benefit from automation that reduces manual configuration errors and helps them keep up with the accelerating rate of change within their organizations. Because automation eliminates manual work, IT becomes more of a business engine driver.

- Comprehensive access control through intelligent, automated policies

- Organizations can use Alcatel-Lucent Enterprise Digital Age Networking to define user access rules and policies that govern which applications and devices users can access and use and follow users wherever they go.

- Unified Policy Management capabilities enforce policies automatically every time a user connects, ensuring users have only the permitted access privileges. Once users log into the network with a PC/laptop/mobile device and their credentials are validated, they don't need to keep authenticating. They stay connected if the device is on and the system automatically enforces the policy for that user.

- Policies ensure that all users, inside or outside the organization, have access only to permitted areas and that these access controls are enforced consistently. They also simplify workflows while enforcing cybersecurity.

Reduced vulnerability with containerization and segmentation

- The ALE Digital Age Networking solution allows organizations to containerize each device, creating a virtual network segment for it to prevent any device from becoming a vector for attack. Containerization within the ALE Digital Age Network makes multiple virtual networks out of a single physical network, which is managed by a single management system.

- Containerization is simple for IT to implement. The ALE Digital Age Networking solution automatically discovers each device on the network.

When a device is plugged into the network, Alcatel-Lucent OmniVista® Network Management System, available on-premises or in the cloud, attempts to identify that device. If the management system doesn't have the device in its database, it will consult a cloud-based database of 17 million plus devices.

- Once the device is identified, the system will classify it, for example, Specific Laptop, Smartphone, etc. If that device is on the approved vendor list, it will be connected to the network. If not, then it won't be. The solution is then set up in a virtual container for the device, segmenting it from the rest of the network. If someone hacks into any networked device, that attacker will be unable to use that device to access the rest of the network.

Improved trust through artificial intelligence

- Once devices are connected, they must be continuously monitored to identify any threats and maintain trust. Alcatel-Lucent Enterprise's analytics and application visibility allow network administrators to see what's going on in the network by device. Analytics identify patterns for normal, expected network behaviour as well as any unusual patterns when they occur. We can look at the behaviour of applications at the edge of the network to decide whether to connect to that application as well as unusual behaviour in allowed applications.

- If an anomaly or unusual behaviour occurs on the device, the analytics will show that so the network security manager can intervene. Today the investigation must be performed manually, but Alcatel-Lucent Enterprise is working on automating the response using AI and ML.

Secure network equipment reduces vulnerabilities

Organizations today are aware of the need to secure IoT devices on the network. But they may fail to consider devices that form the foundation of the network, such as switches and Access Points.

Alcatel-Lucent Enterprise employs many technologies to reduce the threat from these devices. Our solutions:

- Harden the OS software to provide secure, diversified code.

- Send the OS software for third-party verification and validation to ensure it has no easy entry points or backdoors.

- Every time a switch is booted up, the memory is compiled and brought up in a different manner. Although switches function identically, no two have the same memory configuration internally. If someone were to break into one of our switches, they would be unable to access another switch the same way.

- Provide built-in distributed denial of service (DDoS) protection. Our CPU can detect unusual amounts of network traffic and automatically shut down the CPU if necessary.

- Complete multiple security certifications such as Common Criteria, JDIC and FIPS.

- Perform continual software upgrades.

- Secure connections for incoming and outgoing traffic

- For incoming traffic, our VPN capabilities provide an encrypted connection to the local network while end-to-end traffic is protected using the MACsec encryption (also known as IEEE 802.1AE) to protect information as it traverses the network.

Reporting

Alcatel-Lucent Enterprise reporting enables different personas to access information about the status, health and performance of the network, how applications are running, and user satisfaction. Using the ALE Unified Management tools, the capacity to monitor in real time and obtained a big number of reports based per example of traffic usage, client access or Top applications, will help in the improvement of costumer workflows and access to powerful information maintain the network in health.

How to use the Alcatel-Lucent Enterprise and OmniAccess Stellar WLAN solution in a PCI DSS certified organization?

General configurations

- Secure all segments of the network with strict policies and firewall at the enterprise perimeter
- Change default passwords and settings, and disable wireless transmission if connected via wired port

- Monitor wireless network and send events to a secured monitoring and logging device

- Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis

- Ensure wireless network use is included in information security policy and centrally provision wireless device access for consistent, simple compliance reporting

Maintain a hardware inventory

- Have always an up-to-date network documentation

- Maintain the last firmware with the last security features available in the equipment's
    - OmniVista 2500 or OmniVista Cirrus (on the cloud) ensures that all the visibility of the ALE equipment's (wired and Wireless) can be manage, monitored and secured from a single point (Unified Management):
- All the Configurations can be stored automatically, with a regular cadence, to improve secure configuration comparison, as well, a quick recover for the last correct one.
- The PALM component can ensure that you are use the last firmware, updated licences and maintain active maintenance contracts for all the infrastructure, avoiding have the network without the last security features available.
- UPAM NAC component, permits an integrated authentication with an integrated RADIUS, as well secure portals to receive GUESTs or BYOD, improving a consistent secure policy to all network (wired or Wireless), in the same tool. (Unified Management)

- Flow control and Analytics features, permits that you can obtain report documents that will help you to implement best secure practice decisions day by day, as well predict constrain traffic situation in the future.
- Unified policies can be created graphically, and be pushed consistently to the LAN and WLAN, ensuring the same level of security, if a user/device is connected by wired or wireless, improving mobility with the highest security.

Train and educate

- ALE certification curriculum complemented with our Knowledge Hub training webpage, offers the best preparation to the IT teams, to have the last knowledge in the ALE technologies and the best approach to secure the network with correct technics to avoid attacks and maintain the network in a healthy state.

Only authorized wireless technologies deployed in the organisation

- Identification of Interfering APs embed in OminiAccess Stellar WLAN solution
    - Useful to discover the surrounding wireless conditions, and based on that, provide instructions and tools to help administrators improve the quality of the wireless network.
    - Usually there are two types of foreign unknown APs having a negative effect on the wireless network:
        - Interfering APs
        - Rogue APs.

- Beyond potential RF interference it can cause, a **rogue AP** is considered as a security threat to the WLAN network.
    - Support definition of flexible policies to classify an AP as a Rogue AP
        - Unauthorized AP detected on LAN
        - Detect Valid SSID
        - Signal Strength Threshold
        - Detect Rogue SSID Keyword
        - Rogue OUI
        - …

- Attacks detection policies
    - AP Spoofing
    - AP Impersonation
    - Broadcast De-authentication

- Broadcast Disassociation
- Adhoc networks using a valid SSID
- Long SSID
- Adhoc Networks
- Wireless Bridge
- Null Probe Response
- Invalid Address Combination
- Reason Code Invalid of De-authentication
- Reason Code Invalid of Disassociation

- Client attacks detection policies
- Valid Station Misassociation
- Omerta Attack
- Unencrypted Valid Client
- 802.11 40Mhz Intolerance setting
- Active 802.11n Greenfield Mode
- DHCP Client ID
- DHCP Conflict
- DCHP Name Change
- Malformed Frame Association Request
- Sticky Client
- Detect Long SSID in Client detection
- Detect Reason Code Invalid
- …

Secure Management Access

- Enable SSH for in-band management to the wireless equipment

- Disable SNMP access to remote APs if possible. If not, change default SNMP passwords and use SNMPv3 with authentication and privacy enabled.

- Ensure that all default PSKs are changed. Enterprise mode is recommended.

- Synchronize all AP clocks with other network devices in the organization.

- Disable all unnecessary applications, ports, and protocols.

Strong wireless authentication

- OmniVista Management tool with a Radius server built-in
  - To adapt to local organization secure architecture, the RADIUS server can interface with an external authentication server (Radius, LDAP, Active Directory): FreeRadius, Microsoft NPS Radius Server, Microsoft AD, OpenLDAP…
  - MAC and 802.1x Authentication
  - EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-PEAP-MSCHAPv2, EAP-GTC
  - …

Strong cryptography for transmission of cardholder data

- Wi-Fi Protected Accessed (WPA3) encryption. Wired Equivalent Privacy (WEP) is not acceptable when transmitting cardholder data.
  - Supported in ALE OA Stellar WLAN:
    - WPA3 covered by the GCMP-256 (Galois/Counter Mode Protocol) of 256 bits
    - WPA2_AES, WPA2_TKIP, WPA_AES, WPA_TKIP, DYNAMIC_WEP, WPA_PSK_AES, WPA_PSK_TKIP, WPA_PSK_AES_TKIP, WPA2_PSK_AES, WPA2_PSK_TKIP, WPA3_PSK_SAE_AES, WPA3_SAE_AES.
    - …

Wireless Intrusion Detection and Prevention

- OmniAccess Stellar Access Points integrate wireless Intrusion Detection and Prevention (wIDS/wIPS) capabilities and reduce deployment and management costs by using Access Points to simultaneously serve clients and contain wireless threats.
  - There is no need for a costly overlay IDS with dedicated sensors.
  - Automatic threat mitigation protects the network from unauthorized clients or APs and attacks.
  - Protect the WLAN better than an overlay deployment by virtue of being able to analyse and correlate 802.11 frames inline.
  - It is possible to monitor the wireless radio spectrum for the presence of unsafe Access Points or unsafe clients, and countermeasures can be taken to mitigate the impact of foreign intrusions.

Physically segment unsecured wireless networks from secured networks

- When in the impossibility to separate completely the WLAN from the LAN by a firewall, The ALE technology Containers can do that job and create a complete secure separation of the WLAN traffic from the other traffic in secure pipes. Inside that wireless secure pipes, the traffic of users, devices or applications can be sub-segregated too, using this Alcatel-Lucent Enterprise containers technology.

Enforcement of wireless usage policies

- Each device or user that connects over our OmniAccess Stellar WLAN solution, will receive a specific policy, that is align with the role pre-stablished by the Organization Security Policy. The granularity cans start in rate limiting or QoS, and go to application control that each user or device is transmitting.

Conclusion

When you as an organization wants to go through a PCI DSS certification, you need to go further than the twelve (12) PCI DSS recommendations. Today cyberattacks are dynamic and with high level of adaptation. Digital transformation has profoundly changed organization cybersecurity requirements as the number of connected devices increases, the network perimeter disappears, and change continues to accelerate.

The Alcatel-Lucent Enterprise Digital Age Networking solution keeps your IT assets and data, secure in today's age of digital transformation. Through this solution you can closely control user access, reduce vulnerabilities, manage mobile and network devices, keep the inevitable breach from providing a vector for attack and communicate across the organization ecosystem from a position of trust, and you can ensure the integrity of the card payments data transmission or control access to them, when stored in a local datacenter.

Alcatel·Lucent Enterprise