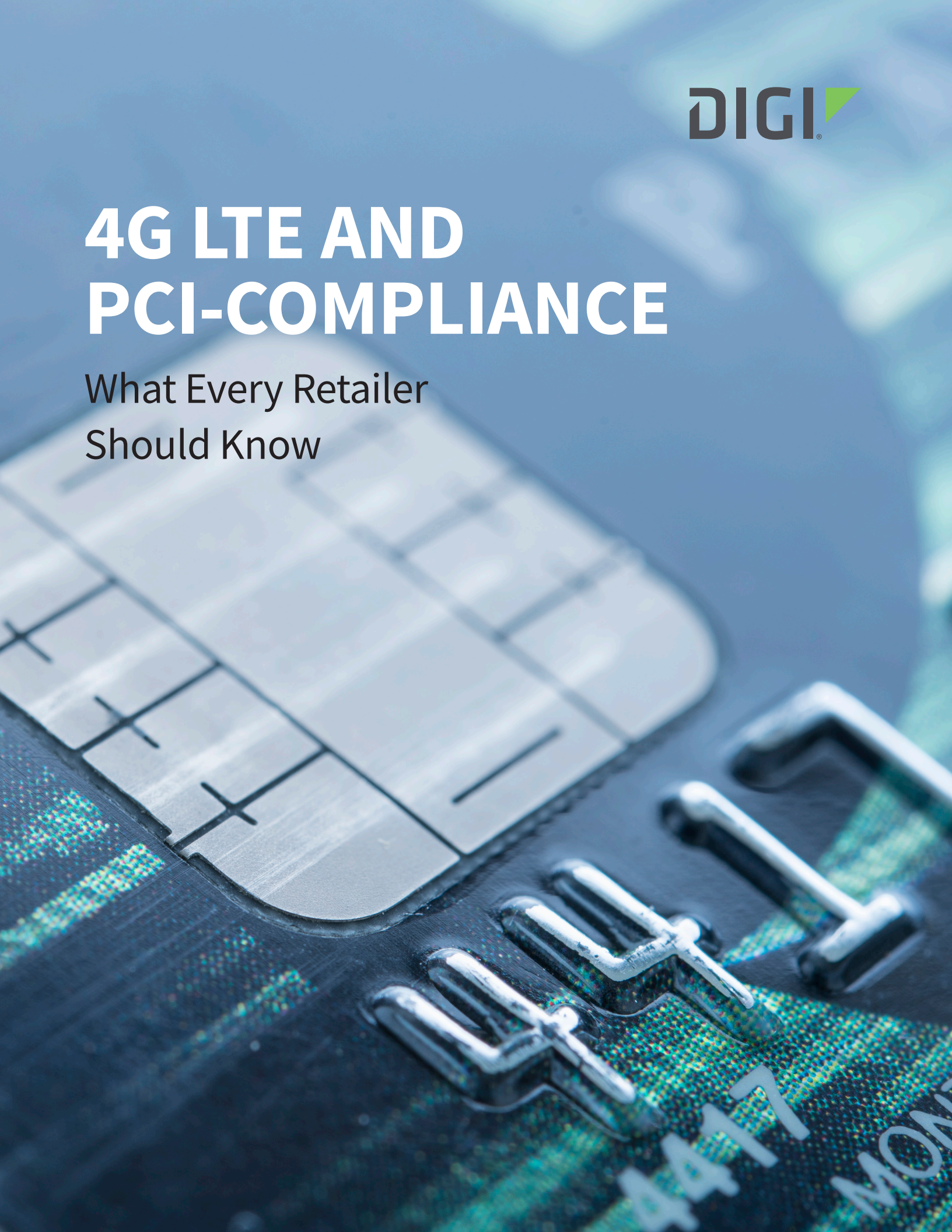
4G LTE AND PCI-COMPLIANCE

What Every Retailer Should Know



The Emerging Mandate For 4G LTE in Retail

Whether it's speed, efficiency, cost-effectiveness or quality, in the thin-margin world of retailing, it's essential to capitalize on every possible advantage to achieve and preserve profitability. In addition, businesses are at serious risk if they fail to implement rigorous security frameworks that also comply with stringent industry and regulatory standards. However, these regulations are saddling retailers with additional processes, cycles and costs that are hampering the retailer's mission. Nowhere is this truer than with the Payment Card Industry Data Security Standard (PCI DSS, or more frequently, simply PCI).

PCI is an industry standard that defines how retailers and other participants in the payment lifecycle must securely handle branded credit cards from major card issuers, such as MasterCard, Visa, American Express, Discover and others. The objective is to increase control and limit visibility of cardholder data to reduce fraud. That's an essential mandate for retailers – if only because consumers trust that every purchase and every transaction they make takes place on a foundation of privacy, safety and security.

The balance of this paper will provide background about LTE and some insights about how it can be utilized by M2M devices now and in the future.

From POS terminals and kiosks to ATMs and other connected devices, retailers are increasingly looking at the benefits of new 4G LTE networks, but need to ensure they transmit card data in ways that ensure PCI compliance.

In this white paper, Digi examines the issues surrounding 4G LTE and PCI compliance:

- The Advantages of 4G LTE
- Mythbusting: Cellular Connectivity in Retail
- Avoiding Common Security Mistakes
- Designing 4G LTE Networks for PCI Compliance

In 2013, 89 percent of companies were non-compliant. In 2014, 80 percent were. Are you in the 9 percent that moved into compliance -- or the 80 percent that are still noncompliant?

The Advantages of 4G LTE

The first generation of mobile technology developed from analog (1G) in 1981 to digital (2G) in 1992. By 2001, 3G multimedia support, spread spectrum transmission emerged and grew until the advent of 4G, which is an all-Internet Protocol (IP) packet-switched network that delivers mobile ultra-broadband (gigabit speed) access. With its greater speed and capacity, the 4G LTE wireless communications standard for voice and data continues to gain momentum in the U.S. and around the world. In the retail world, 4G LTE presents many attractive features that make it a compelling choice.

Reasons to Move from 3G to 4G

- Speed – Typical data rates are in the 1-50 Mbps range, instead of 0.5-5 Mbps. With peak data rates, speeds are measured in Gbps.
- Low Latency – 4G LTE offers latency of less than 100 ms, instead of 100-300 ms.
- Lower Frequency – Operating in the 700-750 MHz range, 4G LTE can cover larger service areas with better signal penetration (such as inside a shopping mall).
- More Bands – You can use aggregated bandwidth and higher throughput.

How 4G Outperforms VSAT

- Cost – VSAT is expensive to install (as much as $300-700 per installation) and also to maintain
- Environment Limitations – In dense urban environments, VSAT can be unfeasible. What's more, weather can degrade performance.
- Limited Bandwidth and Speed – VSAT doesn't always deliver the performance that retailers need.

The 4G Advantages over USB LTE Modems

- Unsuitability – USB modems are consumer-grade devices meant to be plugged into a single user's laptop or desktop. They're not designed for commercial applications.
- Theft-Prone – Retailers report losses of USB modems and the difficulties of replacing and deprovisioning the devices.
- Short Product Lifecycles – USB modems are often obsolete in months.

Mythbusting: Cellular Connectivity in Retail

Despite its many advantages, certain myths persist regarding the use of cellular connectivity in retail settings. Critics might assert, "Cellular is slow and unreliable." The fact is, however, 4G LTE doubles or triples communications capacity, and monitoring software can proactively manage connections to cell towers to reduce dropped connections. What's more, devices with dual SIMs can redirect network traffic for redundancy in the case of a failover event.

In the past, cellular connectivity has also faced criticism regarding its manageability. However, cell strategies are far easier to manage than USB modems distributed across the retail enterprise. More importantly, today's cellular routers embedded with 4G LTE modules are designed for distributed M2M applications that can be centrally managed over cloud-based or server-based SNMP network-management systems tools. Manageability is literally built-in. While most market- and technology-watchers agree that 4G LTE offers compelling advantages, a key question remains: How does it best fit into retailing?

At an entry level, 4G LTE provides an ideal platform for wireless backup, such as backing up POS transactions that are otherwise transmitted across a traditional terrestrial network. As the stability and popularity of wireless grow – earning retailers' trust – we see a move toward wireless as the primary connectivity conduit (particularly outside the U.S.). That translates into more flexibility and lower cost.

And, as retailers move beyond their brick-and-mortar locations and edge closer to their customers through line-busting kiosks or kiosks at airports, for instance, 4G LTE actually helps create entirely new customer points for the retailer.

Common Security Mistakes to Avoid

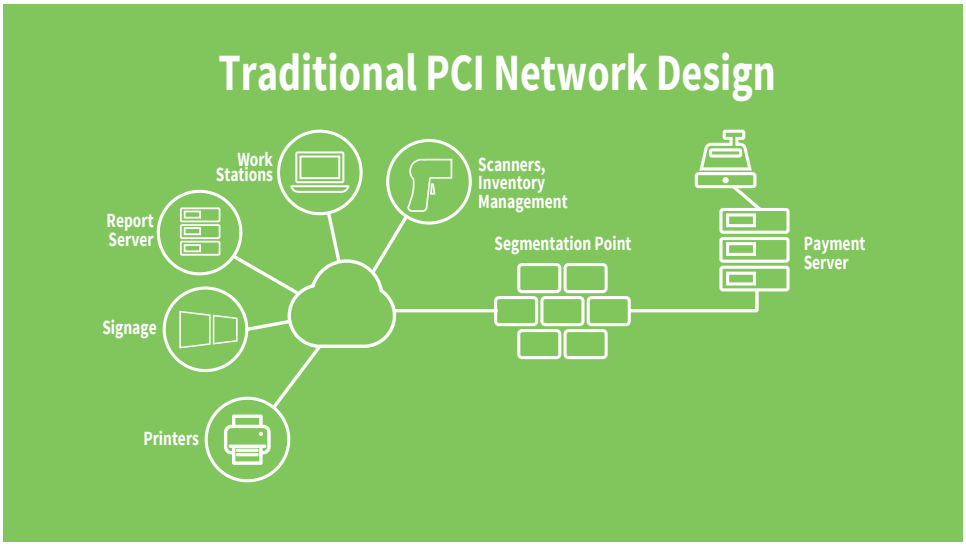
While wireless infrastructures offer many advantages for retailers, it's important to be mindful of easily avoidable security mistakes that can torpedo your ability to remain PCI compliant and pass the necessary PCI audits and certifications. Some of the more common missteps include:

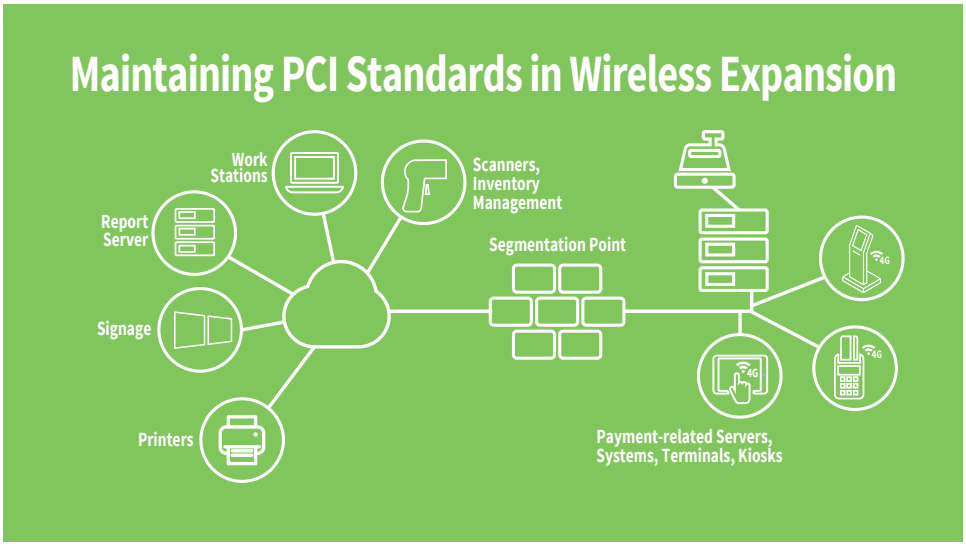
- **Unencrypted Card Transactions over the Public Internet** – It's inadvisable to send unencrypted credit card transactions over the public Internet. This is an easy mistake to make if a backup connection is configured to send data over a public cellular APN.
- **Passing Sensitive Information to an Untrusted Network** – This is a common mistake for many merchants – and it's usually an inadvertent one. For instance, in-store wireless networks often lack the segmentation of payment-related servers and systems, leaving them exposed to anyone lurking in or near the store.
- **Cloud-Based Payments Accessed through Public Internet** – Most cloud-resident payment systems and systems that manage devices are designed to prevent public access. However, if the access point itself is the public Internet, it creates an inviting target for hackers who can steal payment information.
- **Open Kiosks** – These systems provide content, coupons, pricing and POS information for a self-serve opportunity away from brick-and-mortar stores. However, if the payment information and process are not fully and carefully segregated, there is no PCI compliance – far too many vulnerabilities exist .
- **Improper Plans for Wireless Backups** – Since no network has 100-percent uptime (cables can get cut, networks can go down), many merchants use wireless as the failsafe backup network so they can continue to do business without disruption. Unfortunately, many retailers perform extensive planning to create a PCI-certified environment, only to open up a large number of vulnerabilities by attaching an open wireless environment that is a silver-plated invitation to hackers.

Even with the best-protected, properly certified systems, problems will occur. One need only reflect on high-profile penetrations at Target, The Home Depot, PF Chang's, Michaels and others to acknowledge that significant breaches can occur. Adding LTE to the mix, therefore, requires careful planning and protection.

A Network That's Designed for PCI Compliance

A carefully designed 4G LTE-based network can be ideally suited for retail – thanks to a favorable economic profile, excellent reliability, complete flexibility and near-universal coverage. But these networks also move sensitive credit card data on a continuous basis. And that means they're all subject to PCI compliance mandates that require merchants to process card information in a secure manner and in a secure environment.





The PCI Audit

In a PCI audit, the auditor examines your systems, scrutinizes your network, identifies vulnerabilities, and issues directives to improve your ability to prevent data from being compromised.

There are three types of audits, depending on your transaction volume.

- **A Qualified Security Assessor (QSA) guides you through an entire PCI audit**
- **An Approved Scanning Vendor (ASV) will test your endpoints to ensure they're not vulnerable**
- **A Self-Assessment Questionnaire (SAQ) is used by companies with smaller transaction smaller-volume companies**

The goal of a PCI network design is to segment any and every network element that has payment data (or other critical information) from anything else on the network – even if that requires the redundancy of separate routes and separate routers. It can even include separate transport carriers (not simply additional resold lines) that provide secure private routes, which are significantly harder to break into.

When you add 4G LTE technology to the network design, segmentation of cardholder data remains a crucial requirement, but there are now two different endpoints in the network that must maintain PCI compliance. That's accomplished in several key ways:

- Protecting Cardholder Data – Retailers must protect stored cardholder data and encrypt the transmissions of that data across open, public networks.
- Limiting Vulnerabilities – Merchants must protect their systems from malware exposure and regularly update antivirus software and programs. All systems and applications should be developed and maintained with security as a primary feature.
- Ensuring Strong Access Controls – Systems must identify and authenticate all users with access to system components.
- Validating Vendor Security Capabilities – It's easy to integrate security and even encryption features to a product. Merchants should insist on third-party audits and security testing (e.g., penetration testing). Ask vendors to show evidence of PCI security compliance. For 4G LTE network routers and software, for example, a PCI Attestation of Compliance indicates a vendor has passed rigorous third-party testing.

Conclusion

With speed, efficiency and cost-effectiveness, 4G LTE networks offer tremendous advantages to retail enterprises – if implemented properly. For the right level of security – and full PCI compliance – it's clear that a fully private network, with sufficient separation of payment-processing elements, is the only satisfactory choice. For more information on how Digi can help you achieve highly secure, PCI-compliant networks, visit www.digi.com.

Key Takeaways

- ✓ Offering new levels of speed, throughput, larger service areas, and centralized manageability, 4G LTE is an ideal technology for retail communication.
- ✓ 4G LTE connectivity provides excellent reliability and manageability that had been previously absent in other cellular technologies.
- ✓ PCI compliance is a non-negotiable requirement for retailers, regardless of network infrastructure.
- ✓ Expansion of the merchant network infrastructure to capitalize on the advantages of 4G LTE requires a careful focus on security and the design of the network to isolate payment-processing systems and data.

Contact a Digi expert and get started today

PH: 877-912-3444
www.digi.com

Digi International
9350 Excelsior Blvd.
Suite 700
Hopkins, MN 55343

Digi International - Germany
+49-89-540-428-0

Digi International - Japan
+81-3-5428-0261

Digi International - Singapore
+65-6213-5380

Digi International - China
+86-21-5049-2199

/digi.international @DigiDotCom /digi-international