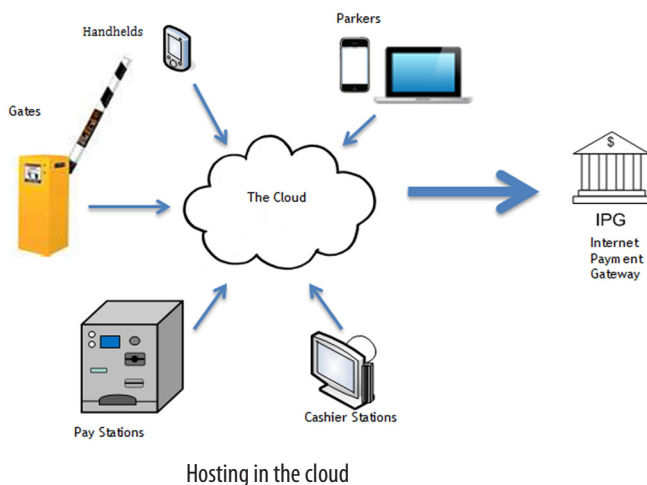


WHAT YOU NEED TO KNOW

PCI DSS, PA-DSS and PARKING IN THE CLOUD

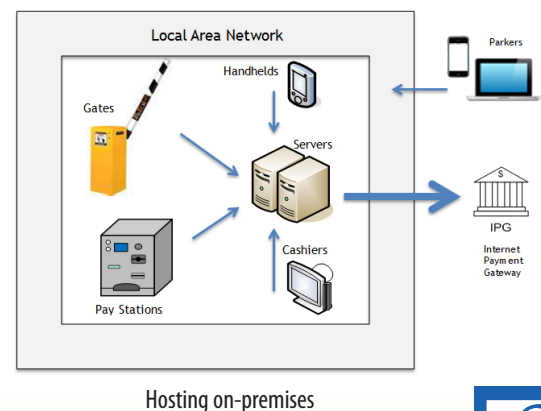
PCI DSS compliance is mandatory for any merchant that accepts credit card payments. So what are your options?

If your parking operation takes credit cards, PCI DSS compliance is a big factor in how you design and put together your parking system. You have two options when it comes to how your system is configured. At a high level, they are:



- 1. Hosting in the cloud:** the servers handling your parking data and cardholder information are in a separate, off-site location, not on your network. If the cloud environment fails to meet compliance guidelines, or if there is a failure or security breach in the cloud, it's your service provider's problem. If you plan to host in the cloud, make sure your parking system provider is PCI-DSS Level 1 compliant. A PCI-DSS Level 1 compliant provider will do the majority of the work required to meet the current compliance guidelines (PCI-DSS v2.0 effective July 1, 2012).

- 2. Hosting on-premises:** the servers handling your parking data, and cardholder information are part of your network and your organization's hosting environment. If your hosting environment fails to meet compliance guidelines, or if there is a network failure or security breach, you are responsible. If you plan hosting on-premises, make sure your parking system is PA-DSS validated, and then make sure your hosting environment meets the current compliance guidelines (PCI DSS v2.0 effective July 1, 2012).



THE VOCABULARY

PCI DSS, or Payment Card Industry Data Security Standard, is the global set of standards for business practices, network architecture, and other protective measures that merchants must uphold if they accept credit card payments. It's a continual process, and assessment occurs every year. PCI compliance is the responsibility of the merchant.

PA-DSS, or the Payment Card Industry Payment Application Data Security Standard, ensures that vendors develop secure payment applications that (1) don't store sensitive cardholder data and (2) support compliance with the PCI DSS. Providing PA-DSS validated payment applications is the responsibility of the vendor.

Qualified Security Assessors (QSA) are companies that assist organizations in reviewing the security of their payment transaction systems and have trained personnel and processes to assess and validate compliance with PCI DSS and PA-DSS.

Report of Compliance is a document produced by a QSA that verifies an organization's compliance with PCI DSS.

Compliance is assessed and validated—not certified.

Report of Validation is issued by a QSA after testing a payment application to validate that it meets the standards set out in PA-DSS.

In either case, in order to support compliance with PCI DSS, you'll need to secure physical access to equipment at your facilities, and you must establish and follow compliant business practices.

On-Premises vs. the Cloud

Here are the key differences in roles and responsibilities for PCI-DSS compliance between on-premises system and hosting in the cloud.

PCI DSS Requirements	Responsibility	
	On-Premises	Cloud Hosting
Build and maintain a secure network	Parking Operator	Vendor
Protect cardholder data	Parking Operator	Vendor
Maintain a vulnerability management program	Parking Operator	Vendor
Implement strong access control measures	Parking Operator	Vendor
Regularly monitor and test networks	Parking Operator	Vendor
Maintain an information security policy	Parking Operator	Vendor

When you **host in the cloud**, you shift much of the effort and responsibilities associated with maintaining a compliant hosting environment to your vendor. The advantages to this shift are myriad: economy of scale, reduced IT workload, extremely reliable uptime, dedicated systems monitoring, and perhaps most obviously, substantial cost savings.

Since maintaining your own hosting environment usually requires tens of thousands of dollars of initial capital expenses, and unforeseeable thousands more every few years to continue to uphold PCI DSS, moving to the cloud shifts a great deal of your computing costs from capital expenditures to lower, more predictable operating costs.

To date, T2 Systems is the only PCI DSS Level 1 PARCS provider. Use your smartphone to view the current list of PA-DSS validated applications and the list of PCI DSS Level 1 providers:

List of PCI PA DSS Validated Payment Applications:
<http://bit.ly/zzMmpf>

List of PCI DSS Level 1 Providers:
<http://bit.ly/wtweNi>



PCI DSS Level 1
Providers



PCI PA DSS Validated
Payment Applications

www.T2Systems.com

About T2 Systems

Since 1994, T2 Systems has delivered proven parking solutions that meet the ever changing needs of the parking industry. This commitment is evident in T2's quality products and services, thought leadership and strong customer relationships. With its broad range of technology-based solutions, T2 Systems is trusted by nearly 400 organizations in the US and Canada including universities, cities, towns, hospitals and airports. T2 Systems is headquartered in Indianapolis, Indiana and has virtual offices throughout the United States and Canada. For additional information about T2 Systems, Inc. products and services, visit www.T2Systems.com.

Think Technology. Think Solutions. Think T2.



Company Headquarters:
 8900 Keystone Crossing, Suite 700
 Indianapolis, IN 46240
 Tel. (800) 434.1502 Fax (317) 524.5501