Taking the complexity, cost and business change out of PCI compliant telephone payments.

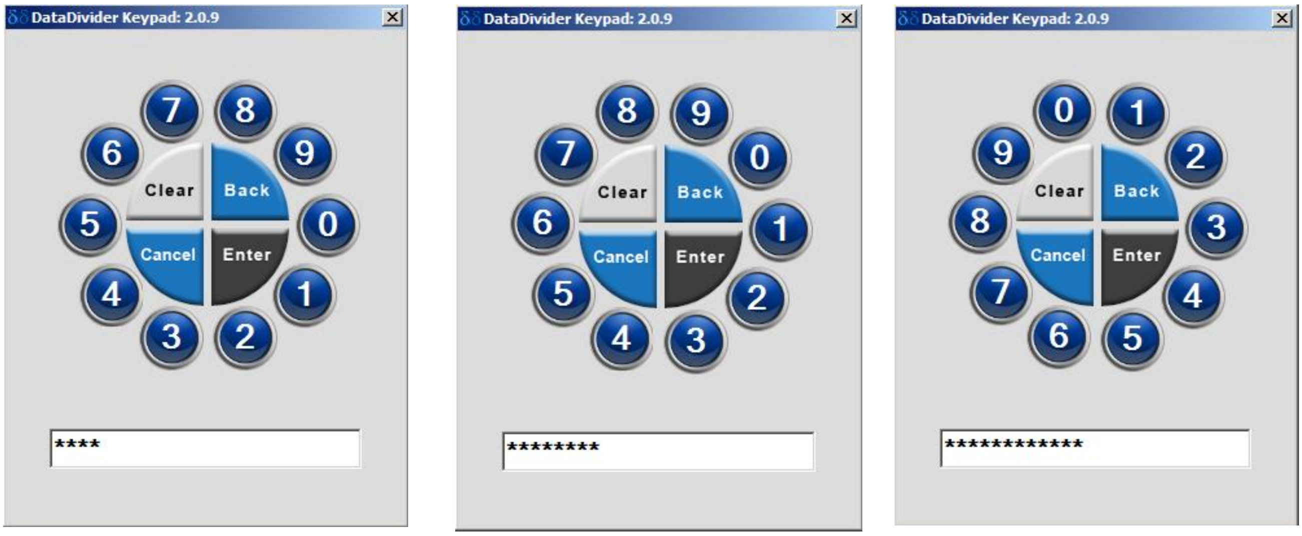
Call centers or back offices taking payments over the phone have proven to be the most challenging and expensive in satisfying PCI requirements. Most corporations have chosen to pause and resume their call recorders in order to ensure that their call recordings remain PCI DSS compliant. Some organizations have elected not to request the security code (CVV2) and to encrypt their call recordings again to meet PCI requirements (as the CVV2 cannot be stored post transaction, even if encrypted). Other organizations have gone so far as to not record calls, to avoid the PCI requirements. However, call recordings are the not the most difficult of PCI challenges for telephone payments. The real challenges lie in securing the desktops on which payments are taken and the network on which these workstations reside. A few organizations have chosen complex and often expensive DTMF tone masking solutions but these remain unpopular as they change the customer experience. Also, where these solutions are on premise, they add their own PCI zone and compliance requirements. Even cloud DTMF tone masking solutions can add additional call legs with associated call costs.

So how is it possible to dramatically address the cost of attaining PCI DSS compliance across desktops and their network taking payments? It takes some very innovative technology.

DataDivider's Virtual Keypad

The moment an employee types cardholder data into their workstation it brings the workstation into PCI DSS scope. This is even the case where the agent is using a payment processor's hosted payment page. The cardholder data has to traverse the local machine and the network before it hits the payment processor's hosted site. So how can cardholder data be captured without exposing it to the local workstation?

That is where DataDivider's patent pending Virtual Keypad comes into action. The Virtual Keypad, secured by DataDivider's Protected Zone, operates as a secure, isolated remote desktop application where mouse click coordinates cannot be reverse engineered back to the PAN (Primary Account Number). It is therefore impossible to reconstruct cardholder data from the local merchant machine. As the Virtual Keypad physically runs within DataDivider's PCI DSS Level 1 certified environment, the cardholder data is protected and out of merchant scope.



The Virtual Keypad initiates with the digit zero being randomly placed between 1^0 and 360^0. Following the mouse click entry each digit is masked. From the first 2 digits it is possible to determine the card format, 4-4-4-4 for MC and Visa, 4-6-5 for Amex and 4-6-4 for Diners Club.

Following the entry of each cluster of digits the Virtual Keypad rotates 1 or 2 digits clockwise or counter-clockwise. Most cardholders read their card number in clusters of digits following the card format. This makes entry simple for the call center agent.

Through the Virtual Keypad initiation and its rotation after each cluster of digits it is not possible to associate mouse clicks with card number digits. It is therefore impossible to reverse engineer mouse clicks back to the cardholder data.

Figure 1 - Virtual Keypad ensures mouse clicks cannot be reverse engineered to cardholder data

DataDivider's Protected Zone

DataDivider establishes a secure encrypted session within layered tunnels on a merchant's desktop to ensure that its Virtual Keypad cannot be compromised. Multi-factor authentication validates credentials, location and legitimate profile. The session is allocated a protected area of local memory. During the session if this memory is inappropriately tampered with, the session will block tampering or terminate with informative security alarms. Potentially harmful local functions within the secure session are disabled such as software keyboard logging, print screen and cut, copy and paste. A secure Remote Desktop Protocol (RDP) session is then established to the DataDivider PCI Level 1 Certified hosted environment. Within this session DataDivider's Virtual Keypad can operate such that it can capture sensitive cardholder data without exposing this data to the local environment. The DataDivider Protected Zone is extended beyond the local desktop by using DataDivider's Interceptor which avoids PAN data being exposed to downstream systems.

DataDivider's Interceptor

Having captured the PAN without bringing the merchant into scope, it is then critical to complete the payment transaction without ever exposing it to the merchant. This is a very simple task if the call center or back office is using the hosted payment page provided by their payment processor. DataDivider's Interceptor injects the PAN (masked from the agent) into the hosted payment page running remotely in the DataDivider PCI SaaS (Software as a Service) Level 1 certified environment. Access to the payment processor is restricted to the DataDivider hosted environment so that connection cannot be made directly from the merchant's local infrastructure. No cardholder data is exposed to the merchant's applications environment.

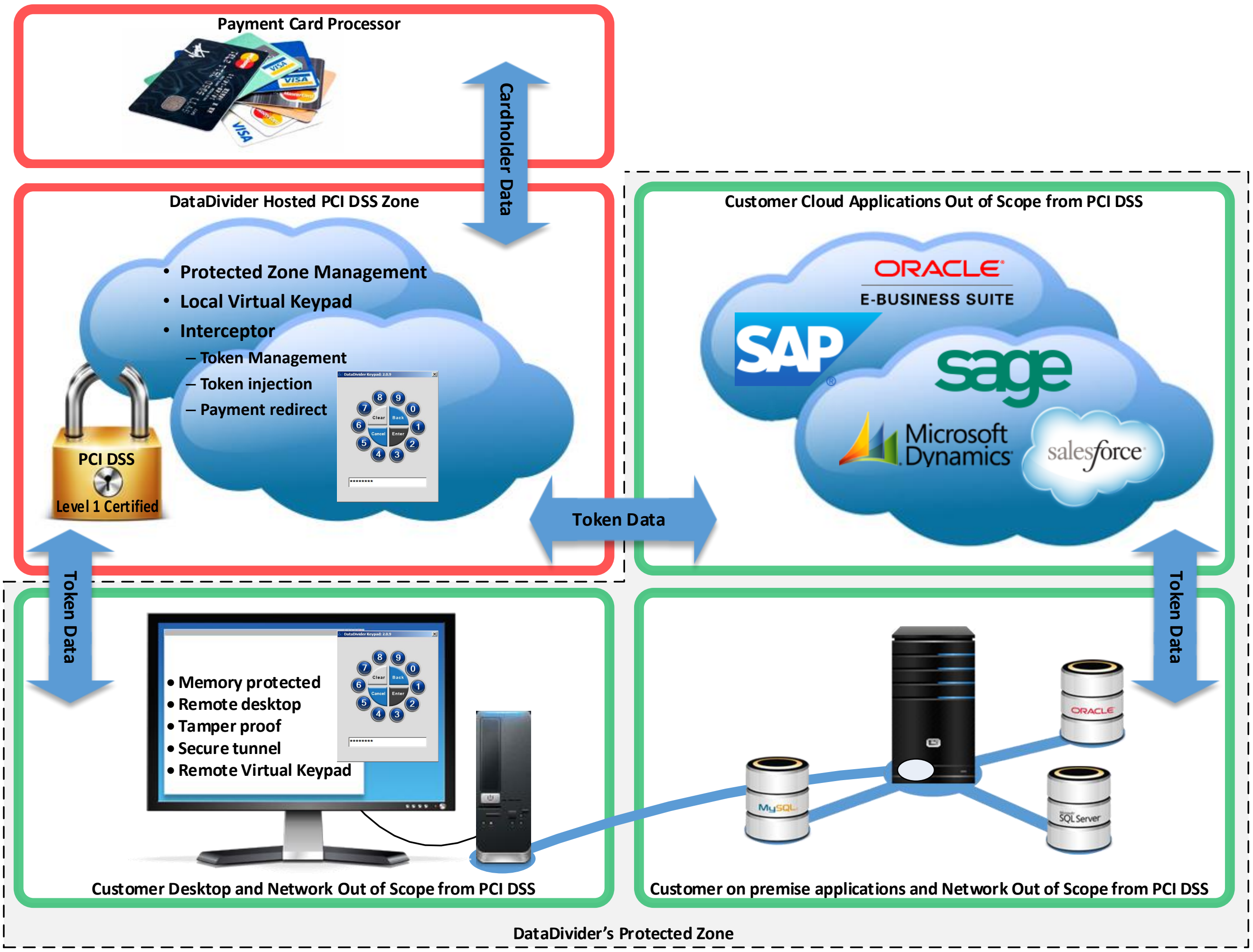


Figure 2 - DataDivider removing exposure from PCI DSS

For corporations who have embedded payment processing into their applications portfolio, Interceptor can still keep the desktop, network and application servers out of PCI DSS scope. In this scenario Interceptor has five key roles:

- Tokenizing the cardholder data
- Injecting the Token into the application payment screen
- Re-directing the payment processing to the hosted DataDivider Environment using an application adaptor
- Within DataDivider's hosted environment De-tokenizing to retrieve the original PAN
- Passing the payment transaction onward to the merchant's payment processor

A Token is simply a unique identifier for a PAN associated with a single merchant. If a fraudster should get hold of the Token it would not be of value and therefore is deemed out of scope from a PCI DSS perspective. DataDivider can provide its Tokens or merchants can use their own.

Within the Protected Zone, Interceptor injects the Token into the original PAN field within the payment application (the field is protected against any other data entry). Format preserved Tokens with the same last four digits as the PAN can be used so agents can refer back to a specific card. Tokens can also be provided that match all PAN rules so that the Token will pass through the payment application's validation controls e.g. a Luhn check.

The payment application would normally transmit the payment transaction to the merchant's chosen payment processor. Interceptor within the payment application re-directs the payment transaction to the hosted DataDivider environment. The Token is converted back into the PAN and the transaction is then passed through to the merchant's payment processor. Again there is no access to the payment processor from the merchant's local environment. Throughout this whole process the cardholder data is never exposed to the merchant's applications' architecture.

VOIP and Telephony Infrastructure

Analog calls are out of scope for PCI DSS, however, most call centers use VOIP and if cardholder data is shared on calls then the VOIP network is in scope for PCI. Most corporations will minimize their PCI costs by simply segregating their VOIP network and protecting it and their telephony switches with a firewall. This represents a small PCI footprint when compared with the corporation's desktops, network and back end servers. PCI costs can be reduced by up to 90% when just having to tackle these small areas.

Removing the headache and costs associated with Telephone Payments

Having left the call center to the final piece of the PCI jigsaw puzzle, many corporations have discovered this has become their Achilles' heel. Now, with DataDivider, it is possible to approach the PCI challenge for the Call Center in the same manner as for bricks and mortar and e-commerce by taking infrastructure out of scope for PCI controls. All this can be achieved without negatively impacting the customer journey.