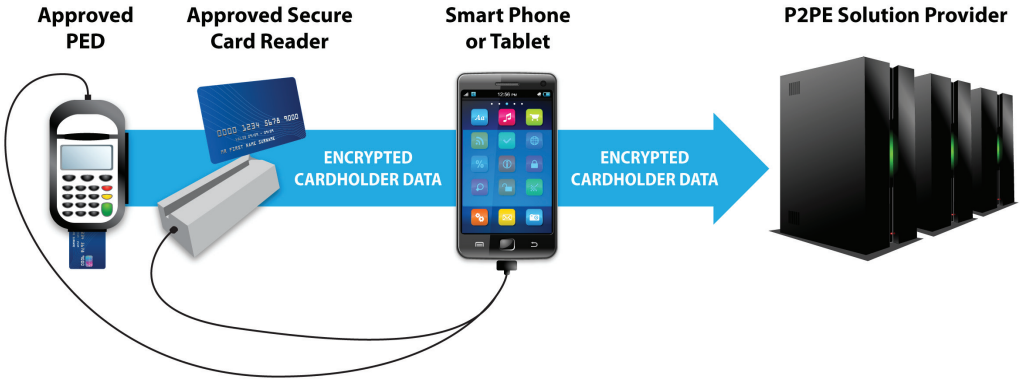
Accepting Mobile Payments with a Smartphone or Tablet



Many merchants seek innovative ways to engage customers and improve the shopping experience. The ever-expanding capabilities of mobile devices such as smart phones or tablets now includes payment acceptance. Along with the increased convenience at the Point of Sale, mobile payment acceptance can also bring new risks to the security of cardholder data. Securing account data at the point of capture is one way that you can actively help in controlling these risks. In 2012, validated Point-to-Point Encryption (P2PE) solutions will be listed on the PCI Council (PCI SSC) website. If you choose to accept mobile payments, these solutions may help you in your responsibilities under PCI DSS.

This *At a Glance* provides an example of a P2PE solution that leverages a mobile device's display and communication functions to secure mobile payments. Central to the example is the use of an approved hardware accessory in conjunction with a validated P2PE solution. Combining a validated P2PE solution with mobile devices such as phones or tablets helps to maintain data security throughout the payment lifecycle.

PROTECT CARDHOLDER DATA

The PCI Data Security Standard (PCI DSS) requires merchants to protect cardholder data. You must protect any payment card information, whether it is printed, processed, transmitted or stored.

For merchants interested in utilizing an off-the-shelf mobile payment acceptance solution:

Partner with a Provider of a Validated Solution

Validated P2PE solutions ensure that cardholder data is encrypted before it enters a mobile device. Using a validated and properly implemented P2PE solution greatly reduces the risk that a malicious person could intercept and use cardholder data.

Solution providers will often provide you with a card reader that works with your mobile device. Validated solution providers will have a list of approved card readers (also called Point of Interaction or POI) that have been tested to work securely with their solution. The solution provider is responsible for ensuring that any POI used with their solution has been validated as compliant with the appropriate PCI SSC security requirements, including the Secure Reading and Exchange of Data (SRED).

Your solution provider will also tell you how to safeguard your mobile payment acceptance system. This guidance is contained in a *P2PE Instruction Manual (PIM)*. Your acquirer or payment brand may ask you to complete a *P2PE Self-assessment Questionnaire* as part of your annual PCI DSS validation – including confirming that you are following the solution provider's PIM. You should coordinate with your acquirer or payment brand.

WHY SECURING MOBILE PAYMENTS IS IMPORTANT

- Current mobile devices have limited security safeguards for payment acceptance
- Responsibilities for security in the mobile infrastructure span multiple participants
- Protecting payment card data is required and protects all entities in the payment ecosystem
- Secure mobile acceptance supports consumer confidence

ENCRYPTION PRIMER

Cryptography is an important, information-security tool that can protect the confidentiality of data. It uses a secret called a key. Using the key, data is changed into what appears to be random data (a process called encryption). You need the key again to change the random data back into the original data (a process called decryption).

The key must be protected from unauthorized access or disclosure.

For merchants interested in building their own mobile acceptance solution:

Use an Approved Point of Interaction (POI) Device

Mobile devices are not necessarily designed to be secure input or storage devices for cardholder data. Your mobile payment solution thus requires additional technology, including encryption, to secure cardholder data acceptance. The first part of a secure mobile payment solution is an approved "point of interaction," which is the technical term for an approved PIN entry device (PED) or approved secure card reader (SCR) used to capture and encrypt cardholder data for a transaction. For example, the illustration above shows two options: one is a SCR used to swipe the magnetic stripe of a payment card; the other is an approved PED for reading a card and manually entering a PIN. All these devices have a single purpose: to safely capture and encrypt cardholder data. As and when devices become approved, they will be listed on the Council's website.

Comply with the PCI Data Security Standard

A major benefit of using a validated P2PE solution for mobile payment security is scope reduction. This means that a validated and properly implemented acceptance solution for processing your mobile payments may lessen the requirements for your annual merchant compliance with the PCI DSS. Scope reduction can dramatically reduce the cost and effort of compliance. You will still be responsible for compliance with PCI DSS requirements for merchant policies and procedures, for contractual agreements with your P2PE solution provider, for physical protection of payment assets, and for following the *P2PE Instruction Manual*.

About the PCI Security Standards Council

The PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements.

The Council's five founding global payment brands – American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. – have agreed to incorporate the PCI DSS as the technical requirements of each of their data security compliance programs. Each founding member also recognizes the QSAs, PA-QSAs and ASVs certified by the PCI Security Standards Council.