Mobile Payment Apps:

The Development Options

jelecos
Technology—Powered by People

Mobile devices seem to have become part of the human body. It's rare to see someone that doesn't have a smartphone or some kind of tablet in his or her hand. Why? It's largely because these devices make so many mundane, often time-consuming tasks much easier and faster — including making purchases. With what's been called "the Uberization of payments," people can use their mobile devices to buy anything from a car ride (as is the case with Uber) to a pizza as long as they have a credit card.

The increase in the number of "things" that can be purchased from mobile devices is, not surprisingly, driving demand for mobile applications that enable those financial transactions. Developing the apps is one thing, but because these involve transactions via credit cards there is also PCI DSS compliance to consider.
Any organization that accepts, transmits or stores any cardholder data, regardless of size or number of transactions, must comply with PCI DSS. So whether you are developing the mobile payment app internally or working with a third-party developer, PCI compliance is an essential consideration. However, a payment app is exempt from the requirements if it employs point-to-point encryption (P2PE) technology to prevent the mobile device from ever having access to cardholder information.

Where to Begin

Many organizations find the PCI DSS confusing because it doesn't provide hard, fast rules. Instead, they provide "guidelines" that are open to interpretation. Prior to beginning the development process for a mobile payment app, it's a good idea to review some of the resources the PCI Security Standards Council for assistance in understanding and implementing the requirements. For the most up-to-date resources from the PCI SCC, visit: https://www.pcisecuritystandards.org/document_library or you can check out Jelecos's resource page for more information on PCI compliance.

At-a-Glance Overview

So what are the PCI mobile payment guidelines? First, the guidelines contain three objectives for securing mobile payment transactions:

Prevent account data from being intercepted when entered into a mobile device.

If P2PE is not being used, developers must ensure that a secure transmission path exists between the device used to swipe or input card data and the mobile device.

Prevent account data from compromise while processed or stored within the mobile device.

Any account data stored temporarily on the device must be protected within a secure storage environment. Data retained on the device after transaction authorization must be protected with hashing, truncation or encryption combined with acceptable key management practices.

Prevent account data from interception upon transmission out of the mobile device.
When cardholder data is transmitted from the device to the next step in the authorization process, it must be protected with strong encryption, such as that provided by Secure Sockets Layer (SSL)/Transport Layer Security (TLS).

The guidelines also include 15 specific points for securely configuring a mobile device:

1. Prevent unauthorized logical device access.
2. Create server-side controls and report unauthorized access.
3. Prevent escalation of privileges.
4. Create the ability to remotely disable the payment application.
5. Detect theft or loss.
6. Harden supporting systems.
7. Prefer online transactions.
8. Conform to secure coding, engineering and testing.
9. Protect against known vulnerabilities.
10. Protect the mobile device from unauthorized applications.
11. Protect the mobile device from malware.
12. Protect the mobile device from unauthorized attachments.
13. Create instructional materials for implementation and use.
14. Support secure merchant receipts.
15. Provide an indication of secure state.

Your responsibility for meeting these requirements will depend on your organization's role in the development process. Appendix B in the PCI Data Security Standard (PCI DSS) Information Supplement: Third-Party Security Assurance contains a matrix with specific interpretations for device manufacturers, mobile operating system developers, application developers, merchants and mobile payment solution providers.

Mobile Payment App Options

If developing PCI-compliant mobile payment apps seems beyond what you want to take on in-house, there are options. Among them:

- **Existing apps**. You can opt for an existing PCI-compliant mobile point-of-sale apps such as Square. There's a small transaction fee involved, but you get funds deposited to your account in a day or two. Unfortunately, these kind of apps are offered under their own brand names, not yours, so you miss out on the branding side as well as giving up control over the app.

- **Mobile payment widgets.** Many gateways, such as Stripe and PayPal offer mobile-specific libraries that provide their own payment UI components. Card data is handled by their library, limiting your PCI compliance exposure and implementation effort. You do give up control of the user experience since you're using the gateway widget's look and feel.

- **Gateway API.** To provide a "custom" checkout experience and for greater control of the user experience than you get with mobile payment widgets, you can develop directly to the gateway's API. Integrating with an API depends on the client library support. The developer experience isn't always optimal. And while you get complete control of the user experience, you also get increased development complexity and gateway lock-in. Plus, you are now in scope for meeting PCI compliance.

- **Multi-gateway mobile access.** There are some companies whose apps use a common API on top of dozens of gateways to provide a consistent payment processing language to your app. Integrating from a mobile app requires the same attention to security as going to the gateway API directly. However, you get non-vendor specific card storage and processing paired with a modern, mobile-compatible API.

- **Outsource.** Depending on the vendor you choose, this could prove to be the most efficient, cost-effective and safest for ensuring your app is PCI compliant. The key is to make sure the company you work with is highly experienced in PCI-compliant app development. If the organization itself holds PCI certification, meaning that it employs the processes and controls to meet the PCI security requirements, you'll stand a much better chance of the apps it develops meeting many of the requirements as well.

The Jelecos Advantage

If outsourcing seems like your best option, Jelecos is among the companies to consider for the job. It stands out among its competitors, however, because of several key points:

- **Standards-based coding**. Jelecos' employs of a standards-based coding approach comprised of a number of security best practices (such as those outlined by Open Web Application Security Project (OWASP) and others). The app development team also codes specifically to prevent certain types of attacks — cross site scripting, SQL injection, and access control violations, among them — as required for PCI compliance. Third-party penetration tests are conducted to validate the apps.

- **Third-party and internal code reviews**. Code reviews are a PCI requirement. They are also an integral component of the software development process at Jelecos. That includes third-party code reviews and peer code reviews. Many development projects are validated using penetration testing as well as code review services such as Veracode.

- **In-depth PCI app development expertise**. Jelecos' developers have extensive experience in developing PCI-compliant apps. They also have in-depth knowledge of both PCI DSS and PA DSS requirements. In addition, Jelecos has a long list of customers to attest to the effectiveness and quality of those apps.

- **Qualified staff; staffing oversight**: In addition to their demonstrated expertise in PCI-compliant app development, Jelecos' developers undergo background checks and engage in frequent security awareness training. There is also segregation of duties, as required by PCI DSS, between personnel assigned to the development/test environments and those assigned to the production environment. This ensures that no single individual that has end-to-end administrative control of the system.

- **PCI certification**. Jelecos is one of the only service providers in the region with third-party PCI certifications in both infrastructure and app development.

Bottom line: Jelecos ensures that apps are built correctly from the ground up to meet PCI requirements so they don't have to be retrofitted to comply. Its use of custom libraries and reusable frameworks speeds up the process, and it employs mature development and release processes with all appropriate workflows and tollgates in place to ensure compliance. No changes in processes or infrastructure are required on your part.

In addition, all hiring processes, planning processes, architecture and development processes, operational processes, facility processes, and segmentation of roles/responsibilities are done with compliance in mind. Yet another key benefit is that Jelecos will map technical controls to your specific requirements, and respond to auditors' requests for documentation.

Jelecos is also flexible, and can work with you in whatever way best meets your needs. It can take you most of the way to full compliance, and then you can decide if you want to do external scans, pen tests, code reviews, etc. If you want the full menu of services to get you to full PCI compliance for your app, Jelecos can do everything necessary to ensure compliance with the version of PCI published during the development of the app (currently, v3.2)

Get Your PCI-compliant Mobile Payment App Now

To learn more about Jelecos' PCI-compliant mobile payment app development, contact:

402.955.0489

866.955.0489 TOLL FREE

sales@jelecos.com

jelecos
Technology—Powered by People