Hewlett Packard Enterprise

HPE SecureData Mobile

Protecting sensitive data in native mobile apps while safeguarding the data end-to-end

Key benefits of HPE SecureData Mobile

- Enables consumer confidence to safely interact with the business through mobile devices
- Simplifies PCI compliance and provides scope reduction
- Enables PII and PHI compliance
- Protect sensitive data at every level of the omni-channel and unified commerce experience
- Recognized format-preserving encryption standard (NIST SP800-38G)
- Developer friendly—simple, native libraries, easy to incorporate into iOS and Android apps
- HPE Stateless Key Management eliminates operational complexity

The challenge

With the increase in mobile applications, along with the recent surge in data breaches securing sensitive data in the mobile environment has become more important than ever. By year-end, mobile share of ecommerce transactions is forecasted to reach 40 percent globally.[1] Forrester states that mobile commerce transactions will have hit $115 billion USD in 2015 and increase to $142 billion USD this year.[2]

Sensitive cardholder information in mobile payment applications, as well as Personally Identifiable Information (PII) and Protected Health Information (PHI) in other mobile-based applications, should be protected end-to-end. The need to safeguard sensitive data in motion captured on mobile endpoints becomes critical to ensure end-to-end data protection.

Unique approach

HPE SecureData Mobile, a new addition to the HPE SecureData portfolio, provides security for sensitive data submitted through a mobile endpoint. HPE SecureData Mobile enables end-to-end sensitive data protection within native mobile iOS and Android applications through the entire enterprise data lifecycle and payment transaction flow. Data is secured from the point of capture to the trusted host.

[1] "Criteo, State of Mobile Commerce Report", Q3 2015. **criteo.com/resources/mobile-commerce-report/**

[2] "U.S. Mobile Phone and Tablet Commerce Forecast 2015 to 2020," Forrester Research, October 1, 2015.

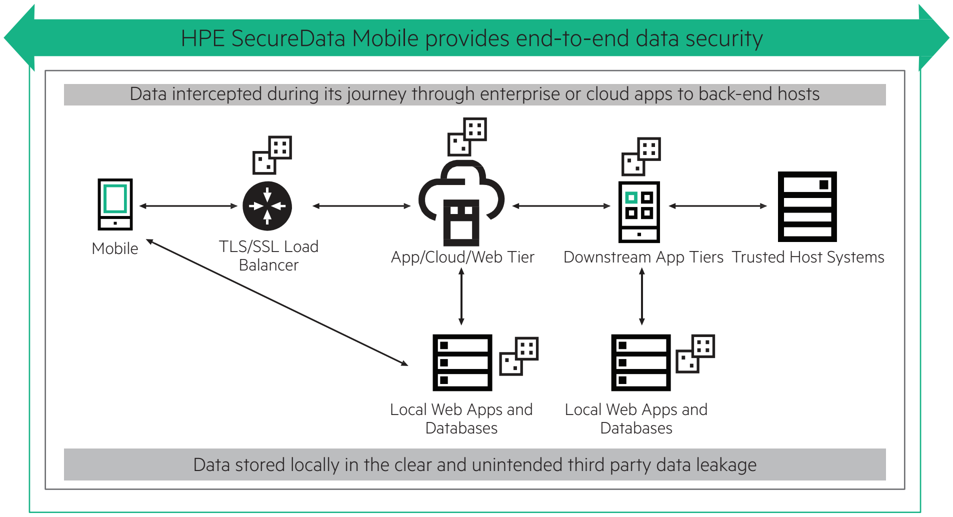
HPE SecureData Mobile provides end-to-end data security
Data intercepted during its journey through enterprise or cloud apps to back-end hosts
Mobile
TLS/SSL Load Balancer
App/Cloud/Web Tier
Downstream App Tiers
Trusted Host Systems
Local Web Apps and Databases
Local Web Apps and Databases
Data stored locally in the clear and unintended third party data leakage

Figure 1. Types of mobile app breaches–mitigate risks with HPE SecureData Mobile

HPE SecureData Mobile leverages HPE Format-Preserving Encryption (FPE) to provide data security for in-app mobile purchases. It encrypts sensitive customer information like PANs (credit card numbers) and the CVV/CVC (3 digit security code) when a customer makes a purchase through a merchant mobile application. The merchant environment has no access to PCI data in-the-clear or encryption keys since the PAN and CVV fields are encrypted in the mobile application before the data reaches the merchant's web services. Decryption happens at the host end so that transaction authorization may be completed. HPE SecureData Mobile simplifies compliance and reduces PCI audit scope.

HPE SecureData Mobile also provides data security for personal sensitive information like PII and PHI, and enables companies to meet PII and PHI compliance requirements. Sensitive PII and PHI information such as name, address, social security number, birthdate, health information and more is protected. In the healthcare industry, HIPAA and HITECH require and enforce the encryption of all PII and PHI data. Healthcare organizations can no longer afford to expose sensitive personal information in mobile environments, especially when more consumers are frequently using mobile apps to access test and lab reports, medical records, and billing services.

In the financial services industry, the combination of new state privacy regulations with consumer demand for faster, more convenient banking and mobile wallet services has also driven the need for companies to secure sensitive data in mobile applications. In a 2015 Forrester report, the findings show consumers are more willing than ever to walk away from the business if it fails to protect their data and privacy.[3] HPE SecureData Mobile protects sensitive PII and PHI personal data in the mobile applications by encrypting the data so that it may be used safely throughout its lifecycle. Since live data exposure is removed from insecure systems, compliance to privacy regulation is also streamlined. HPE SecureData Mobile safeguards sensitive data as it moves through the enterprise and beyond.

[3] Consumer privacy attitudes: A 2015 update, Forrester Research, Fatemeh Khatibloo's Blog, November 18, 2015.

With the growing popularity of digital shopping, the retail industry is rapidly embracing the omni-channel strategy that enables customers to have a seamless shopping experience regardless of the channel, whether online, mobile, or in store. Because of this multichannel approach, it is critical for retailers to reduce fraud and protect consumer data at every touch point to deliver a transformative and secure customer experience. Given the recent number of high-impact retail breaches, and the rapid increase in mobile wallets, payment applications, and other mobile-based applications, retailers need to increase the protection of PII and PHI data so that consumers may safely interact with the business through their mobile devices. HPE SecureData Mobile transparently secures the consumer's submission of sensitive data through mobile applications which gives retailers more control in the customer experience and how store associates interact with customers via mobile devices.

HPE SecureData Mobile Solution

HPE SecureData Mobile is a highly scalable, reliable and developer-friendly data protection solution that leverages HPE Format Preserving Encryption (FPE), a breakthrough technology. HPE FPE is a mode of AES, a recognized encryption standard by NIST (NIST SP800-38G). The result of a standards-based encryption scheme allows for encryption with minimal modifications to the existing applications. Because HPE FPE maintains the format of the data being encrypted, no database schema changes and minimal application changes are required.

HPE SecureData Mobile includes simple, native libraries to easily incorporate into native mobile applications. This enables the application code to retrieve a one-time-use cryptographic key for encrypting sensitive data. HPE SecureData Mobile supports two mobile client platforms, iOS and Android.

HPE SecureData Mobile also supports HPE Stateless Key Management architecture. HPE Stateless Key Management enables on-demand key generation and re-generation without the need for an ever-growing key store. The result is a system that can be infinitely scaled across distributed physical and logical locations for a low operational and infrastructure cost.

How it works

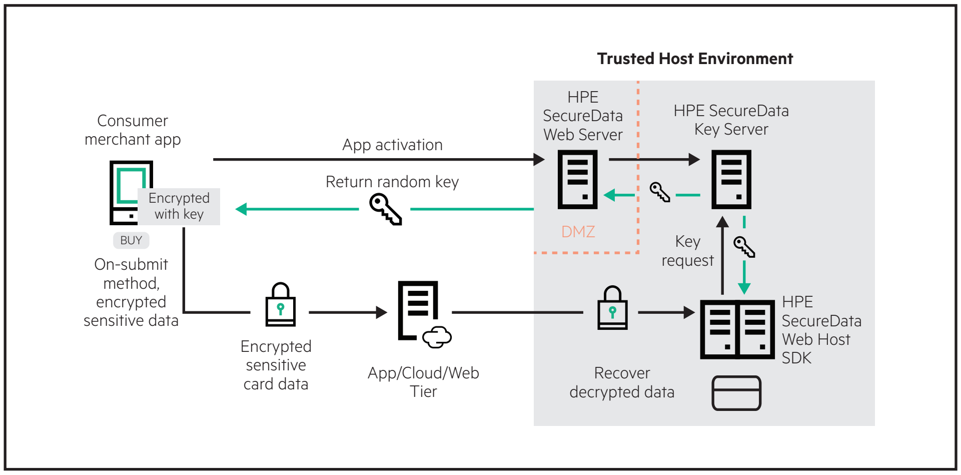

Figure 2. HPE SecureData Mobile Encryption

About HPE Security—Data Security

HPE Security—Data Security is a leader in data-centric security safeguarding data throughout its entire lifecycle—at rest, in motion, in use—across the cloud, on-premise and mobile environments with continuous protection.

About HPE Security

Hewlett Packard Enterprise is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from HPE Security ArcSight, HPE Security Fortify and HPE Security—Data Security, the HPE Security Intelligence Platform uniquely delivers the advanced correlation and analytics, application protection, and data security to protect today's hybrid IT infrastructure from sophisticated cyber threats.

Learn more at
voltage.com
hpe.com/software/datasecurity

Sign up for updates

★ Rate this document

Hewlett Packard
Enterprise

4AA6-4753ENW, April 2016, Rev. 1