Advisory Notice – Apple Pay™ with Contactless Smartcard Readers
November 20, 2014

This notice provides an overview of the experience that occurs when an iPhone® 6 or iPhone® 6 Plus enabled with Apple Pay™ is presented to a reader.

Summary

An iPhone® 6 or iPhone® 6 Plus enabled with the Apple Pay™ application will launch the Apple Pay™ user interface when presented to some physical access and logical access readers. The launch of the Apple Pay™ user interface is not an indication of communication between the reader and the phone. The phone sends no meaningful information to the reader when the Apple Pay™ application launches. HID readers cannot interpret or send any credit card number, bank details, or other personal identifying information. Despite appearance, this device behavior does not reflect a compromise of privacy or security.

Further, this issue has no impact on the performance of the iPhone® 6 when used as a credential for physical access control with HID Mobile Access®. At this time there is no reasonable way to avoid this behavior during an HID Mobile Access® "Tap" transaction, apart from disabling the Apple Pay™ application. Apple® representatives are aware of the issue.

Issue Detail

On October 20, 2014, Apple® officially released iOS version 8.1 which optionally enables iPhone® 6 and iPhone® 6 Plus devices to use the Apple Pay™ application for financial transactions at select merchants. To initiate a financial transaction at a supporting retailer, the device owner must present his/her iPhone® 6 to a contactless payment terminal. The Apple Pay™ application will launch and the user will be prompted to authorize the transaction by presenting fingerprint verification on the embedded sensor.

As shown in the image below, an iPhone® 6 or iPhone® 6 Plus enabled with Apple Pay™ launches the application when presented to a contactless smartcard reader. The experience occurs with any contactless smartcard reader. Reader brands from HID Global that excite this behavior in iPhone® include iCLASS®, multiCLASS®, iCLASS SE®, multiCLASS SE®, pivCLASS®, SmartID®, and OMNIKEY®.

Additionally, legacy reader models with a configuration that allows the output of a random ISO14443 UID (also referred to as a "card serial number") will send the random UID to the access control system when an iPhone® 6 owner presents the phone and validates identity with biometric. This would most likely be presented at an access control workstation or audit log as an "invalid card format" or "access denied" event.

Root Cause

Apple Pay™ uses NFC (Near Field Communication) to process payment transactions. NFC leverages the 13.56MHz frequency and communication protocols that have been standardized by the contactless smartcard industry over the past 20 years.

It is possible for an NFC-enabled device to distinguish between a legitimate payment terminal authorized to process a financial transaction and a different device designed with intention of using 13.56MHz for a completely different use case (e.g. Physical Access Control). The iPhone® 6 and iPhone® 6 Plus devices do not make this distinction before launching the Apple Pay™ application.

Addressing Concerns

Some iPhone® 6 owners may express concern about this experience. It's important that security leaders and system administrators reinforce that the launch of the Apple Pay™ user interface is not an indication of communication between the reader and the phone. The phone sends no information to the reader when the Apple Pay application launches. Even if a valid biometric is presented, only an authorized payment terminal can retrieve information other than a meaningless random number. HID readers cannot interpret or send any credit card number, bank details, or other personal identifying information.

For those customers who are using HID Mobile Access®, the Apple Pay™ issue has no impact on the performance of the iPhone® 6 when used as a credential for physical access control with iCLASS SE® readers.

Containment

For iPhone® 6 users who express concern about this issue, it's important to communicate that no HID reader can be used to read or harvest private or personal information from Apple Pay™.

For System Administrators who are concerned about the risk that random UID reads could present to physical access security or audit log accuracy, best practice is to disable (through configuration) all UID, CSN and other unsecure reads. Please have the part number of the readers in question and contact HID Technical Support for information on how to modify your configuration.

Corrective Action

There is no reasonable action that can be taken by the HID Global development team, our partners, or our end-user customers to prevent the Apple Pay™ application from launching when an enabled iPhone® 6 or iPhone® 6 Plus is presented to a contactless smartcard reader. A modification to the iOS software is the only reasonable change that can wholly address this behavior.

Support

For additional support please contact HID Technical Support or your local HID Sales Representative.