Digital Secure Remote Payment:
How Apple Pay can change the future of remote payments

Authors
Marcel Fehr, MSc (Royal Holloway, 2017)
Konstantinos Markantonakis, ISG, Royal Holloway

Abstract

Besides Point of Sales (PoS) security improvements for contactless payments with the global introduction of Chip Cards, the secure remote payment path will soon experience important changes as it is expected that the Card Present (CP) fraud figures will further drop and we will see a significant rise in CNP fraud figures. This is partly caused by the global migration towards EMV payments at point of sales, where the payment transaction is now well protected from fraud by EMV chip technology.
This is where Apple Pay's digital secure remote payment (DSRP) implementation can play an important role in the future. The reader will be able to appreciate that the use of tokenization combined with dynamic EMV payment cryptograms renders captured payment details mostly useless for use in cross-channel fraud. Besides that, and more excitingly, Apple Pay allows, in comparison to other wallet solutions, the bridging of device boundary, supporting not only mobile in-app purchases using an EMV payment token and cryptograms but also connected devices.[a]

[a]This article is published online by Computer Weekly as part of the 2018 Royal Holloway information security thesis series `https://www.computerweekly.com/ehandbook/Digital-Secure-Remote-Payment-How-Apple-Pay-can-change-the-future-of-remote-payments`. It is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full thesis is published on the ISG's website at `https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/`.

We are living in a world where smartphones follow us at every turn. We are used to "bringing our own devices". Why not introduce secure mobile payments as part of our daily purchasing experience? Indeed, the trend in consumer preference for mobile wallets over physical wallets is well documented, and is mainly caused by the publicity around the launch of the three "Pay" solutions, namely Apple Pay, Samsung Pay, and Android Pay. But what makes Apple Pay really different to the other wallet solutions? It introduces EMV cryptographic strength to your remote payments, not only for in-app payments on your iPhone but also for your interconnected Apple devices - this feature is named Digital Secure Remote Payment (DSRP). Entering credit card numbers and security codes (CVV) during online purchases will be a thing of the past. DSRP provides a feasible option to successfully reduce Card Not Present (CNP) fraud figures.

> You can use your MacBook for online shopping and authorize the payment on your iPhone.

Setting the scene - credit cards, tokenization and cryptograms

Apply Pay successfully applies tokenization and dynamic one-time cryptograms to secure online payment transactions. First, we introduce you to those enabling technologies and main players.

The anatomy of credit card numbers The card number found on payment cards, such as credit cards and debit cards, is referred to as PAN (Primary Account Number). The PAN as well as tokenized PANs (tokenPAN) are needed in clear text because they serve as routing information to send the payment requests through the payment network to the Issuer Bank of the customer. The Issuer and Bank identification numbers (IIN, BIN) are unique and allocated to the corresponding bank. Figure 1 shows the credit card allocation scheme.

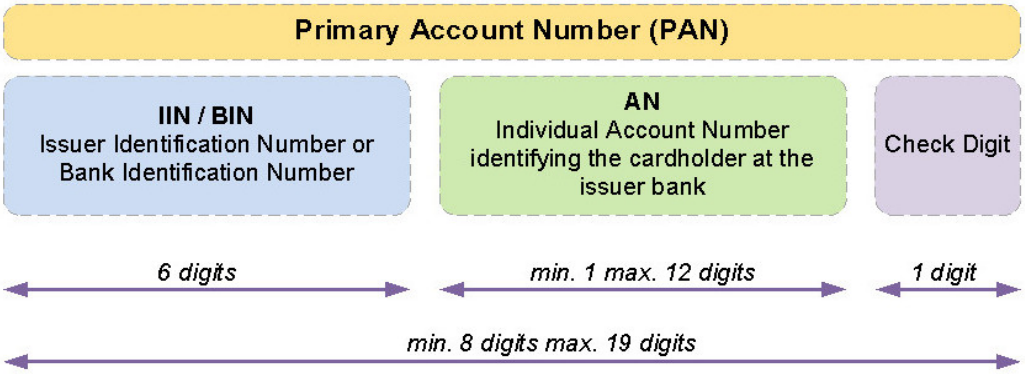

Figure 1: Credit card anatomy

Tokenization Through the replacement of the valuable PAN with a unique surrogate low-value equivalent (tokenPAN) within a payment transaction, called tokenisation, we can remove sensitive account data from the payment environment. To reduce the impact of a PAN disclosure, tokenization has been applied in the payment industry for quite some time as a mechanism for protecting payment credentials at rest, but now we change the game and apply tokenization to the online payment process.

In case of a data breach, a tokenised PAN is of very little value because it cannot be used without the dynamic payment cryptogram. For example, PoS malware (RAM scrappers) retrieving account information will no longer be a source for stolen payment data.

Tokenization service is offered by TSPs (Token Service Providers) to Issuers. When a payment request with a tokenized PAN travels its way up to the Issuer, it must be routed first to the assigned TSP, which translates the tokenized PAN into the PAN and vice versa - see Figure 2. Form and size of the tokenized PAN must comply with the anatomy of a credit card to allow the payment request to be routed through the payment network.

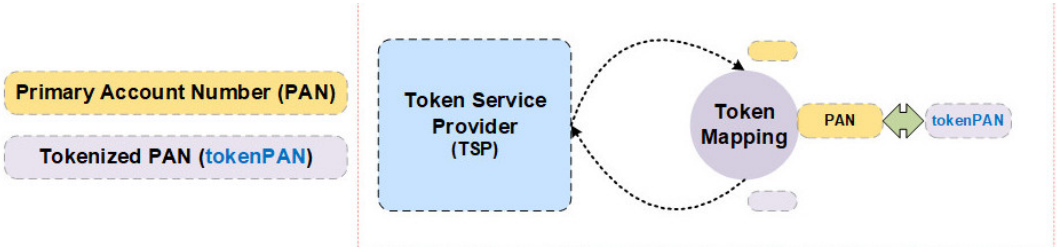

Figure 2: Token Service Provider

Dynamic Cryptograms To add an additional layer of transaction security, years ago EMV Chip Technology has been introduced to the card reader environment. The same technology has been adopted by Apple Pay. EMV chip cards generate dynamic one-time cryptograms that are unique to each payment transaction, so stolen chip card data cannot be used to create a counterfeit card - the PAN is tokenized and the transactions are integrity protected.

The payment cryptograms are named Authorization Request Cryptogram (ARQC). As the name says, they are used to request a payment authorization. EMV chip technology and ARQCs are already in use for contact and contactless payment at PoS and are generated by the smart credit cards. Figure 3 shows the simplified structure of such a payment request.

The ARQC contains payment transaction data (e.g. currency, amount, terminal id) and bank specific data (tokenPAN, EXP Date, etc.), which are needed by the issuer to conduct fraud analytics and

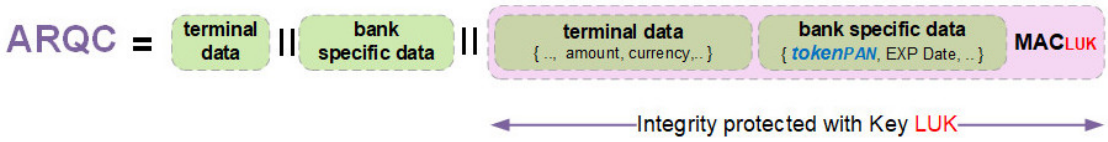

Figure 3: Authorisation Request Cryptogram (ARQC)

finally to authorize the payment. To protect the integrity of the payment request, the included data is appended with a message authentication code (MAC_{LUK}) .

Note that one might think if we capture a tokenPAN in cleartext we could try to use it in a fraudulent online transaction - but this won't work as the tokenPAN must always be accompanied by the corresponding payment cryptogram, whose cryptographic key material (LUK) is protected and generated within the payment device's smartcard chip - the two components are inherently connected to each another. The TSP will verify the magic duo when doing the mapping process.

Apple Pay and its ecosystem - what does it look like?

Now you have been introduced to the important ingredients used to cook Apple Pay. The simplified diagram in Figure 4 shows how Apple Play integrates the iPhone as a payment device into the overall payment process. Besides the TSP (2), who is responsible for the token mapping process and Apple Services (6), the other players conform to the stakeholders of a standard credit card payment transaction. Those include the Merchant (4,5), where the customer (7) does the shopping either contactless (8) or as a CNP or DSRP (9) transaction, the payment network (3), which routes the payment requests to the Token Service Provider (2) for the token conver-sion and finally to the Card Issuer (1) for approval.

Apple Pay on iPhone Key Characteristics (see Figure 4)	a) Cardholder needs an Apple ID. b) High value tokenPAN and cryptographic keys are stored in a secure element (SE). c) Issuer certified payment app is stored in SE. d) SE smartcard is managed by Apple (Java Card Platform). e) Use of scheme (e.g. Visa, MC) controlled (TSP) tokenisation. f) NFC interface is only accessible via SE and not open for other apps. g) Only Apple Pay wallet application can be used for payment. h) Apple Pay does not need internet connectivity during payment process. i) Fingerprint, PIN and Face Recognition are used to verify the Cardholder.

Apple's Digital Secure Remote Payment - what does it do better?

Apple Pay does offer contactless payment at PoS, the most common application, but what makes Apple Pay really different is DSRP. So far Apple Pay is the only wallet supporting DSRP while using on board EMV chip technology to generate payment cryptograms in its web payment process. We will now have a closer look at DSRP where we bridge the device boundary. This means we do online shopping, for example, on a MacBook, and approve the payment on the iPhone hosting the Apple Pay wallet - how exciting is that!

First, what are the known weaknesses of CNP payments? One main concern in the online payment process (CNP), where the merchant cannot physically identify that the legitimate cardholder is using their own credit card, is that we only have a limited set of options for verifying details that only the

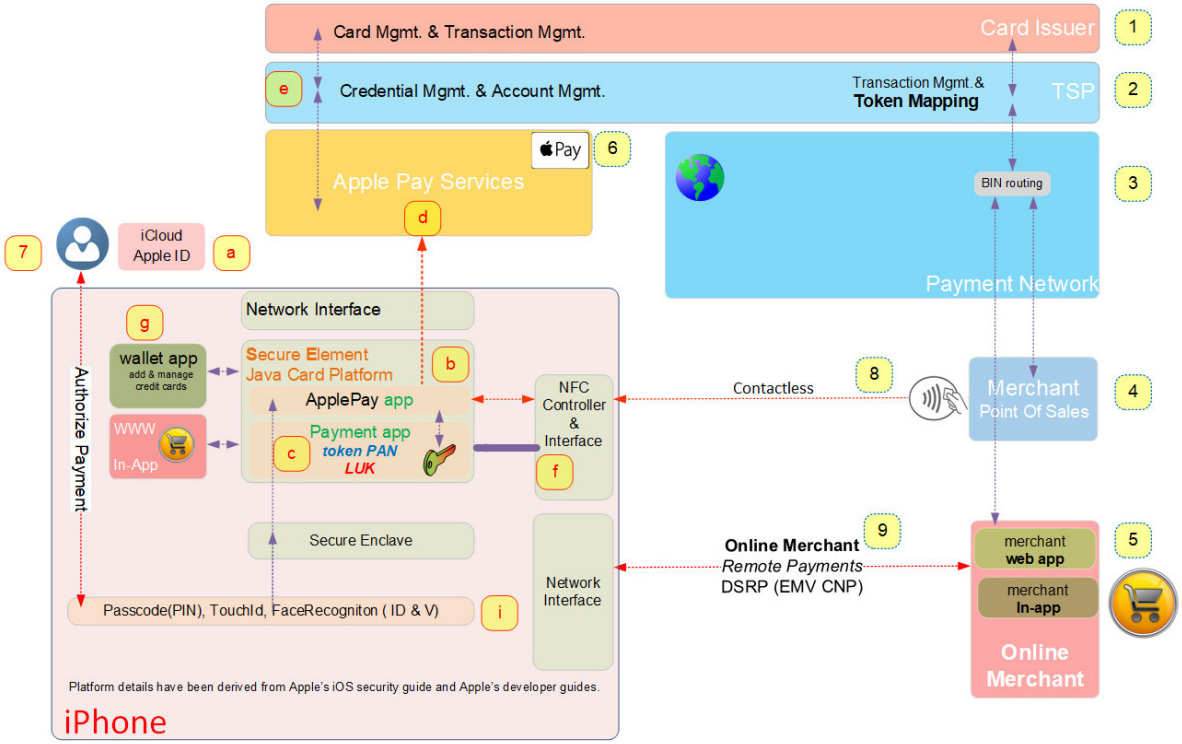

Figure 4: Apple Pay ecosystem

legitimate cardholder knows. This means the Identification and Verification (ID&V) process lacks the necessary strength. The same problem applies to the cardholder; there is no physical merchant identification available - that is a reason why fake web shops are set up to harvest credit card details.

Therefore, when it comes to remote (online) payment transactions using a standard web browser application, the following weaknesses are prevalent:

A. There is no merchant identification to the customer. We have no confidence who we are dealing with.

B. The issuer's fraud management is limited to the cardholder details we can verify, which are the cardholder name, the card number, the card expiry date, and the card verification code (CVV2) printed on the back of the credit card, and the cardholder address. For the latter, only the numerical values will be verified because of the probability of spelling and keyboard errors.

C. The issuer fraud management is further limited, as there is little meta data available regarding the payment device, location, device id, *etc.*.

D. All cardholder details we enter during a payment process are potential targets of phishing and social engineering attacks.

E. The payment process is vulnerable to "man in the browser" and "man in the middle" attacks, where malware attempts to access cleartext payment data and cardholder details.

F. Access to the credit card details is not protected via strong authentication methods. For example, a screenshot of the card is sufficient to use it for CNP cross channel fraud.

How does Apple Pay address the CNP payment weaknesses? Let's have a look at the communication flow (Figure 5). First, to offer Apple Pay as a payment method, a merchant must register with

Apple Pay (1) and upload its public key. This registration process provides some degree of merchant identification and verification. During online shopping the merchant application checks (3) whether Apple Pay is available on the customer's smartphone (3) - this is done with Apple's proprietary handoff function. This is where the magic happens - we have just bridged the device boundary. If Apple Pay wallet is available, the merchant checkout process delivers the "payment sheet" to the customer (1,3), who authorises the transaction via user identification (4). After successful payment authorisation (5) by the user the SE (6) generates the EMV payment cryptogram, which includes some other transaction data, such as merchant identification. This data is finally encrypted (7), and sent to Apple Pay. This payment information is confidentiality protected, and can only be decrypted by Apple Pay.

Apple Pay decrypts the data, encrypts it with the public key of the merchant and signs it. Then, it is sent back to the smartphone (8), which in turn forwards (9) the payment data via handoff (3) back to the merchant's shopping application. We provide confidentiality protection for the payment data and data origin authentication by adding the signature. The merchant decrypts the payment token, and forwards it via payment network via Token Service Provider (11) for issuer authorisation (12). Details of this can be found in the thesis.

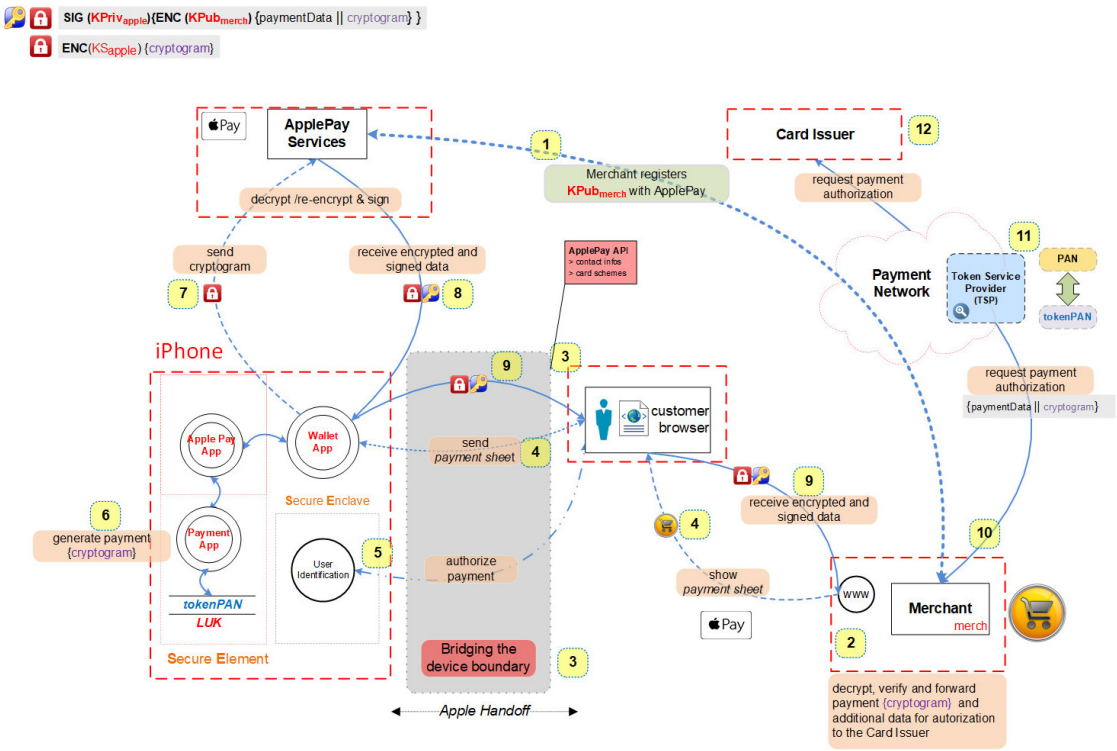

Figure 5: Apple Pay web payment. *(This Information has been derived from Apple IOS Security Guide and the corresponding Payment Token Format Reference.)*

Putting the pieces together Apple Pay's web payment introduces several security mechanisms that were missing in standard CNP transactions, and provides a significant security improvement for the online payment process. The main improvements are:

- **EMV strength:** The iPhone SE generates an EMV-strength cryptogram. A captured payment token is useless, owing to tokenisation, and the dynamic key generation used to construct the $\mathrm{MAC}_{\mathrm{LUK}}$ of the cryptogram. This prevents cross channel fraud.
- **Encryption:** Sensitive payment data is confidentiality protected not only via transport channel but also by explicitly by encrypting specific content (8). Even a successful "Man in the Middle Attack" or a malware infected browser does not allow access to unprotected payment data.

- **Merchant identification:** Apple serves as trusted third party, and provides merchant identification through its merchant enrolment policy and the decryption and re-encryption process of payment information. A fake website won't be able to decrypt the encrypted payment data.
- **Strong cardholder authentication:** The Consumer Device Cardholder Verification Method (CD-CVM) supports two-factor device authentications, where one factor can be fingerprint authentication or the recently added face recognition. This protects the Apple Pay credit card from unauthorized access.
- **Fraud Management & Meta Data:** The payment process includes far more meta data for supporting fraud analytics than a standard CNP transaction. This includes meta data related to Apple purchases, device information (such as location), tokenPAN information, and other information.
- **Payment Device Life Cycle Management:** In case the digitised credit card of you Apple Pay wallet needs to be replaced or disabled, Issuers can instantly cancel the card and prompt the user for a new enrolment, without the cost of a physical replacement - this is definitely a good reason why the card Issuers like this kind of solution. The savings related to card issuing and replacement costs might even compensate the commission fees the Issuers have to pay to Apple.

Closing Remarks

Apple Pay has the potential to make online payments far more secure than before. We can now move forward security-wise, while extending EMV chip technology to CNP payments using smartphones with a mobile browser, or to non-smartphone devices using standard browsers to access the merchant's online tools and conduct secure EMV-strength payments which are supported by the additional security features of strong cardholder and merchant identification.

Apple Pay's intriguing method of expanding DSRP from pure in-app payments into the world of the connected devices, such as iPads or other devices running Mac OSX to facilitate payments, is indeed very promising. However, "DSRP and bridging the device boundary" works seamless as long as we use Apple devices, but what about scaling Apple's solution up and aiming for facilitating mobile payments on a third-party device? The next solution should be universal, and not bound to a single vendor technology. Might this solution be not too far away as we already have many options to bridge the device boundary - for example, displaying a QR-Code from a merchant application and reading it for approval with an integrated Apple Pay QR Code Scanner?

> Entering credit card details *will* be a thing of the past!

Biographies

Marcel Fehr B.Sc., MSc. received his B.Sc. in Electronic Engineering (University of Applied Science, Zurich) in 1988, his MSc. in Information Security in 2017 from Royal Holloway, University of London. He also holds the following industry certifications CISA, CISM and CISSP-ISSAP. He currently works as a principal security architect with focus on cyber resilient infrastructures.

Konstantinos Markantonakis B.Sc. (Lancaster University), M.Sc., MBA, Ph.D. (London) received his BSc (Hons) in Computer Science from Lancaster University in 1995, his MSc in Information Security in 1996, his PhD in 2000 and his MBA in International Management in 2005 from Royal Holloway, University of London. He is the Director of the Information Security Group Smart Card and IoT Security Centre (SCC). His main research interests include smart card security and applications, secure protocol design, key management, embedded system security and trusted execution environments, cyber physical systems, NFC/RFID/HCE security, electronic voting protocols and Internet-of-Things (IoT). He has published extensively in international conferences and journals. He is also a member of the IFIP Working Group 8.8 on Smart Cards. Since June 2014, he is vice chair of IFIP WG 11.2 Pervasive Systems Security. He is an experienced consultant on a variety of topics including smart card security, key management, information security protocols, mobile devices, smart card migration program planning/project management for financial institutions, transport operators and technology integrators.

Series editor: S.- L. Ng