February 28, 2018

Transfer of payment credentials between devices

Roman Kalukiewicz

Justin Brickell

Transfer of payment credentials between devices

ABSTRACT

Payment credentials for use in mobile wallets are stored on a user's mobile device through a provisioning process. When a user switches devices, the new mobile device has to be provisioned with the user's payment credentials to enable mobile wallet functionality on the new device. Such provisioning can be cumbersome. This disclosure describes secure transfer of payment credentials between mobile devices by physically tapping the devices together. A new mobile device is configured as a payment terminal. The user is instructed to tap the old mobile device against the new mobile device. Upon tapping, the old mobile device transfers payment credentials to the new mobile device. The credentials are verified by the card issuer. Upon verification, the payment credentials are provisioned on the new mobile device. Thus, the techniques enable seamless, rapid, and secure transfer of payment credentials to the new mobile device.

KEYWORDS

- CDCVM
- Mobile wallet
- Payment credentials
- Payment terminal
- User verification
- NFC
- Device provisioning
- Mobile device setup

BACKGROUND

Payment credentials for use in mobile wallets are stored on a user's mobile device through a provisioning process. The provisioning process stores payment information of a user, e.g., credit/debit card, bank or financial institution account number, etc., on the device in encrypted form for subsequent use, e.g., at a merchant's payment terminal. Payment credentials are generally scoped to only one device.

When a user switches devices, the new mobile device has to be provisioned with the user's payment credentials to enable mobile wallet functionality on the new device. Provisioning payment credentials on the new device usually requires the user to fill forms on the new device with details such as the user's billing address, credit card numbers, card verification codes (CVC), etc. This is a cumbersome task. Techniques for speeding up provisioning and simplifying the payment credential transfer process can improve user experience.

DESCRIPTION

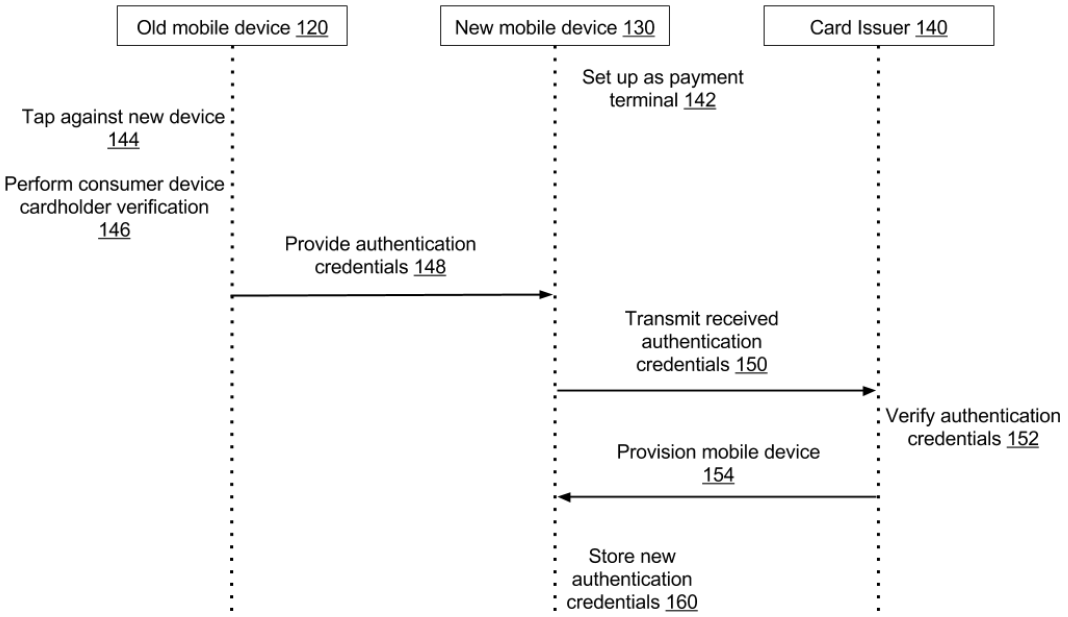

Fig. 1: Payment credential transfer between mobile devices

Fig. 1 illustrates a process to transfer payment credentials from a provisioned (old) mobile device (120) to a new mobile device (130). The techniques are implemented upon user permission. The new mobile device is configured to function as a payment terminal (142). The user is then instructed to tap the old mobile device against the new mobile device to initiate the transfer of payment credentials.

Tapping initiates wireless communication between the devices, e.g., using near field communication (NFC). Upon tapping, the user is required to authenticate (144), authentication process is initiated for the requested transfer of credentials by performing, e.g., a consumer device cardholder verification method (CDCVM) using the old device (146), which provides the authentication credentials to the new mobile device (148). The credentials are transmitted (150) to the card issuer (140) and are verified by the card issuer (152). Upon successful verification, card and payment details including codes, numbers, keys, images, EMV cryptograms, etc., associated with the payment method are provisioned (154) on the new mobile device. The new mobile device stores the received payment credentials (160) and can now provide these upon user request.

The collected details, including, e.g., an EMV cryptogram, are verified by the card issuer as proof of card possession for the mobile wallet. This offers a secure method of proof of card possession, as compared, e.g., to entering card number and CVC, since the EMV cryptogram cannot be obtained other than by tapping and since the EMV cryptogram cannot be reused.

As explained earlier, while the new mobile device functions as a payment terminal, the old mobile device is utilized to perform a consumer device cardholder verification method (CDCVM), a mechanism employed by payment networks to verify ownership of the card and/or

account. This ensures that the transfer of payment credentials by tapping is initiated by the genuine card or account owner.

Further, additional risk signals are attached to the provisioning request, e.g., list of cards already provisioned by the user, etc. This indicates, for example, that a user with the same identity has already stored on the device the card presently being transferred. The additional risk signals serve as an additional proof of identity, reduce the need for further user verification, and enable immediate provisioning of payment credentials to the new phone.

The additional risk signals ensure that even if a user's identity is stolen, e.g., an attacker has access to user data, the attacker still needs physical access to the user's mobile device to perform a transfer of credentials. The techniques of this disclosure ensure that even with complete physical access to the card/device, the transfer of credentials can be effected only when accompanied by authentication by the user, e.g., via CDCVM). This serves as a further guard against illicit credentials transfer.

The techniques for transfer of credentials as described herein are implemented upon specific user permission, and only upon initiation by the user. The payment credentials are accessed and transferred specifically for the purpose for provisioning the new mobile device.

Further to the descriptions above, a user may be provided with controls allowing the user to make an election as to both if and when systems, programs or features described herein may enable collection of user information (e.g., information about a user's social network, social actions or activities, profession, a user's preferences, or a user's current location), and if the user is sent content or communications from a server. In addition, certain data may be treated in one or more ways before it is stored or used, so that personally identifiable information is removed. For example, a user's identity may be treated so that no personally identifiable information can

be determined for the user, or a user's geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user may have control over what information is collected about the user, how that information is used, and what information is provided to the user.

CONCLUSION

This disclosure describes secure transfer of payment credentials between mobile devices by physically tapping the devices together. A new mobile device is configured as a payment terminal. The user is instructed to tap the old mobile device against the new mobile device. Upon tapping, the old mobile device transfers payment credentials to the new mobile device. The credentials are verified by the card issuer. Upon verification, the payment credentials are provisioned on the new mobile device. Thus, the techniques enable seamless, rapid, and secure transfer of payment credentials to the new mobile device.