January 2020

Offline Mobile Payments Using Public Key Cryptography

Sandro Feuz

Thomas Deselaers

Offline Mobile Payments Using Public Key Cryptography

ABSTRACT

This disclosure describes techniques for the user of a mobile device to electronically pay another user using a payments app even in the absence of internet connectivity. At the payer's end, a payment message that includes the payee's identity, the amount, and other details is generated. The message is encrypted using the payer's private key and provided to the payee's device via a suitable mechanism such as peer-to-peer transfer, e.g., via Bluetooth. In another mechanism, the payer's device generates an encoded image, e.g., a QR code, from the encrypted message. The message and/or the code is transferred to the payee's mobile device, e.g., via a peer-to-peer connection or capturing an image of the code using a camera of the payee's device. When either device connects to the Internet, the payment is decoded and verified using the payer's public key. A message is sent to respective account providers to complete the payment.

KEYWORDS

- Mobile payment
- Mobile wallet
- Offline money transfer
- Mobile banking
- Electronic wallet
- Digital signature
- Public key cryptography

BACKGROUND

Digital banking and mobile wallet applications have gained in popularity as they provide an easy way to transfer funds instantly from one person to another. Typically, digital banking applications require an internet connection, as the transfer of funds from payer to payee happens through the banking system. In some situations, an internet connection is either unavailable or is too expensive, e.g., when the user is using a mobile device in a foreign country with associated high data charges.

DESCRIPTION

This disclosure describes techniques for a mobile-device user to electronically pay another user using a payments app even when the internet is not immediately available.

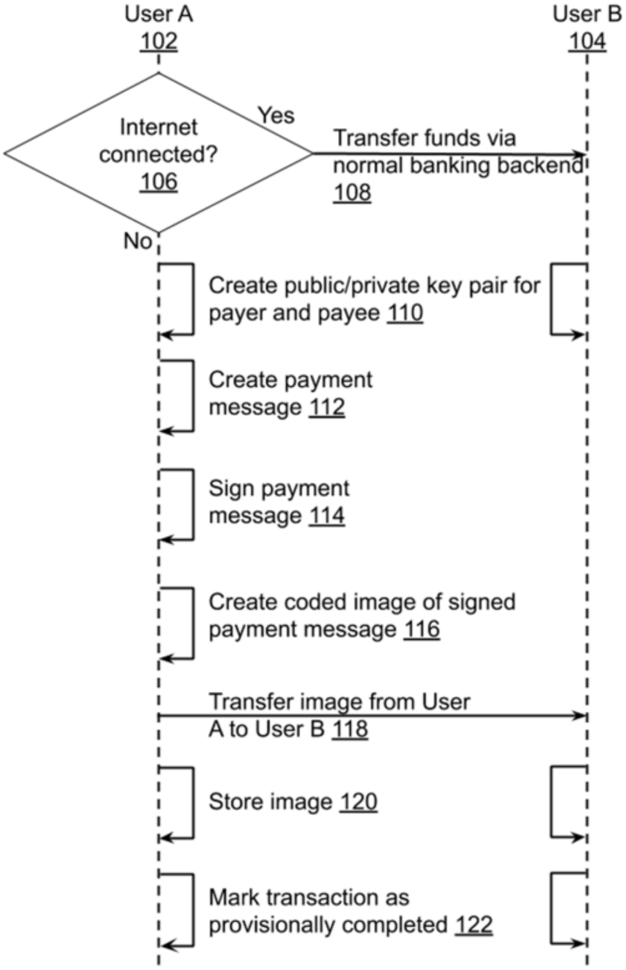
User A
102
User B
104
Internet connected?
106
Yes
Transfer funds via normal banking backend 108
No
Create public/private key pair for payer and payee 110
Create payment message 112
Sign payment message 114
Create coded image of signed payment message 116
Transfer image from User A to User B 118
Store image 120
Mark transaction as provisionally completed 122

Fig. 1: Offline mobile payments using public-key cryptography

Fig. 1 illustrates making mobile payments without internet access using public-key cryptography, per techniques of this disclosure. A user A (102, payer) wishes to pay a user B (104, payee) using a payments app. The two users are in physical proximity to each other. Upon initiating a payment from user A to user B, the app determines if the device that is initiating the payment is connected to the internet (106). If it is, the payment happens normally, e.g., the transfer of funds is executed using the banking backend (108). The payments app establishes a public-private key pair for each user (110). The public key is published and the private key is either tied to the user account in the cloud or kept completely local on the user device.

If the device is offline, or if the banking backend is unreachable, the payments app enables local payment. The payments app generates a payment message (112) that includes the identity of the payer, the identity of the payee, the amount, a random seed that acts as payment ID, other user-permitted metadata, etc. The payments app signs the payments message (114) using the payer’s private key. The signed payment message, together with its signature, is encoded as an image (116) and provided as a barcode, QR code, or other custom code.

The image is displayed on the screen of the payer’s device. The image is transferred from payer to payee (118), e.g., by having the payee capture a photo of the image through the payee’s payment app. Alternatively, the payment message can be transmitted via any suitable p2p data transfer mechanisms. The image is stored in the mobile devices of both the payer and the payee (120). Both users are notified that the transaction has provisionally taken place (122). However, at this time, no funds transfer actually takes place.

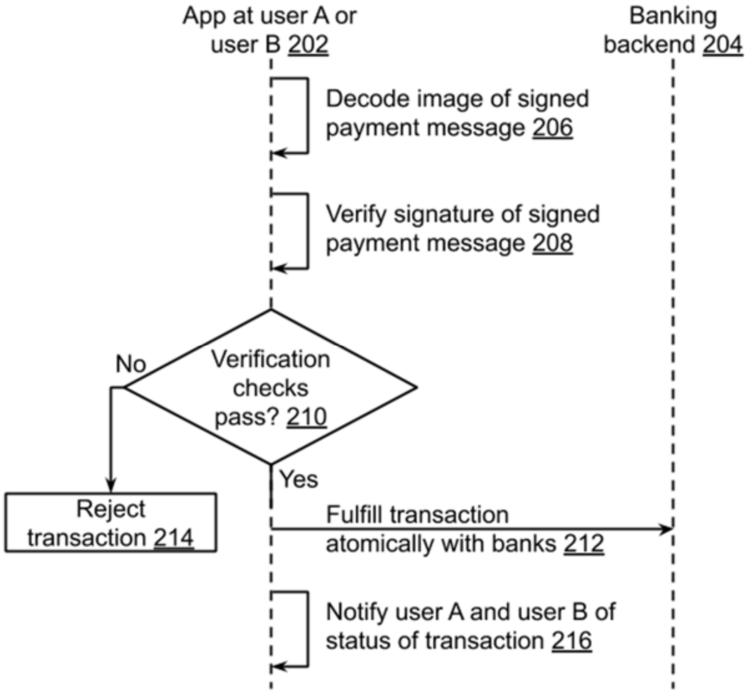
App at user A or user B 202
Banking backend 204
Decode image of signed payment message 206
Verify signature of signed payment message 208
Verification checks pass? 210
No
Yes
Reject transaction 214
Fulfill transaction atomically with banks 212
Notify user A and user B of status of transaction 216

Fig. 2: Completing the transaction when the devices is online

When the device of either user A or user B is online at a later time, the transaction is automatically completed as illustrated in Fig. 2. The payments app at user A or user B (202) decodes the image of the signed payment message (206). It verifies the signed payment message (208) using the public key of user A, thus verifying that user B is the intended recipient, and verifying that the payment with ID as embedded in the payment message is not already resolved.

If verification checks pass (210), the transaction is fulfilled atomically with the account provider (e.g., bank or other provider of the payer and the payee by communicating with the banking backend (204). If verification checks fail then the transaction is rejected (214). Fulfilling a transaction atomically includes actions such as adding the amount to the user B’s (payee) account; subtracting the amount from the user A’s (payer) account; marking the local payment as completed by adding the payment ID to a database; etc., such that either all actions are completed or none are. Optionally, both users are notified (216) that the transaction is now completed.

The users are provided options to limit the maximum amount that can be transferred while their device is offline, can restrict offline payment to specific recipients, or to turn off offline payment entirely.

CONCLUSION

This disclosure describes techniques for the user of a mobile device to electronically pay another user using a payments app even in the absence of internet connectivity. At the payer's end, a payment message that includes the payee's identity, the amount, and other details is generated. The message is encrypted using the payer's private key, and an encoded image, e.g., a QR code, is formed from the encrypted message. The message and/or the code is transferred to the payee's mobile device, e.g., via a peer-to-peer connection or capturing an image of the code using a camera of the payee's device. When either device connects to the Internet, the payment is decoded and verified using the payer's public key. A message is sent to the payee's account provider to complete the payment.