View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Technical Disclosure Common

Technical Disclosure Commons

Defensive Publications Series

May 23, 2017

Test Token Management

Rebecca Hughes

Jose Damico

Follow this and additional works at: http://www.tdcommons.org/dpubs_series

Recommended Citation

Hughes, Rebecca and Damico, Jose, "Test Token Management", Technical Disclosure Commons, (May 23, 2017)
http://www.tdcommons.org/dpubs_series/535

This work is licensed under a Creative Commons Attribution 4.0 License.

This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.

TEST TOKEN MANAGEMENT

Abstract

Electronic payment systems employing tokens allow a user to create a virtual card that can be stored securely on a smartphone or in the cloud. The user can use these stored cards to complete payment transactions for items either in applications or via the Internet, for example, via a web browser. To ensure such payments are secure, these systems encrypt the card details in what is known as a "token." This token contains the card information, as well additional information to authorize/verify the transaction. Successful implementation of tokenized electronic payment in a production environment requires testing of new functionality in the production environment – which must include what looks like a proper token to the production environment. Letting every developer write his own production environment test token generation app introduces interoperability and security risk to the production environment. The technology described herein creates and manages tokens for use in production environment testing.

Keywords

Tokenized payment; proxy payment; production environment testing; test payment token.

Description

Payment cards, such as credit cards or a debit cards, enable a user to make a payment by electronic funds transfer. Typically, payment cards are electronically linked to a payment account, such as a credit card account or a debit account. These accounts may be deposit accounts, loan accounts, or credit accounts. The payment card is a way for the card user to

access the underlying payment account for payment in transactions, such as in a transaction with a merchant at a point-of-sale (POS) device.

In some instances, the user's phone can serve as a proxy for an underlying physical card and payment account. For example, in mobile wallet technology, also commonly referred to as "electronic wallet" and "digital wallet" technology, a user can present a mobile device at a point-of-sale device, for example by "tapping" the mobile device to conduct a transaction at a brick-and-mortar merchant location. Some electronic wallets allow the user to make online payments via the electronic wallet. Most electronic wallets can accommodate multiple underlying payment accounts.

Referring to Figure 1, in typical electronic wallet architecture, the electronic wallet application provider maintains an account for the user in an electronic wallet server. The electronic wallet server interacts with both merchant systems (such as a point-of-sale system, by "tapping") and conventional payment card authorization and processing systems via the Internet to complete transactions.

Typical electronic wallet applications do not store the user's payment card information on the user's mobile device. Rather, the electronic wallet application tokenizes the payment card. Tokenization is also known as replacing the payment card/account number with a "proxy" card number or account number. With payment card tokenization, an alias/placeholder/proxy account number remains stored on the user's mobile device. The actual payment account information is stored with the electronic wallet server.

A user can initiate a payment transaction with the electronic wallet by presenting the mobile device at a brick-and-mortar merchant's point-of-sale system. Upon presentation, the

point-of-sale system and the user's mobile device establish a communications channel. For example, tapping the mobile device at a point-of-sale system may establish a communications channel between the mobile device and the point-of-sale system using Near Field Communication (NFC) technology. Other communications channels, such as a Bluetooth™ wireless communication technology channel, or a Wi-Fi™ wireless communications channel, can be used apart from, or in conjunction with, the NFC channel.

The user's mobile device and the merchant's POS system exchange information, including the identity of the user's mobile device communicating the token to the merchant's POS system, via the communications channel established between them. The merchant's POS system interacts with the electronic wallet to receive the actual account information. From this point, the transaction can be processed as if the user had presented a physical payment card to the merchant, except that the payment processing system must be involved to translate the token to an issuer's account number to obtain authorization of the transaction.

Outside the brick-and-mortar context, electronic wallets can be used to complete transactions online between a user and a merchant. In such cases, the communications channel between the merchant's web server and the user's computing device is a network such as the Internet.

Referring to Fig. 2, the technology described herein includes a test token generation system that can supply test tokens to a production test systems for use in interoperating with production payment processing systems. A single test token generation system can supply production environment test tokens to multiple production test systems that can interoperate with any one or more of a plurality of production environment payment processing systems, merchant

POS systems, and electronic wallet servers. The interaction can take place over communications networks such as the Internet.

In some embodiments, the test token generation system is an application executing on one or more computer platforms. The application provides a graphical user interface that allows a user to register an account with the test token generation system. Upon registration, the user can indicate, through a graphical user interface of the test token generation system, whether tokens with live data (a "real" token) or tokens with placeholder data (a "fake" token) are requested, and the quantity (one token through a predetermined maximum number of tokens) that is requested.

The application then generates the requested tokens. The graphical user interface of the application then allows the user to communicate the tokens to applications executing in various production test environments.

Access to accounts in the test token generation system can be controlled through a "whitelist." The technology described herein allows PAGM (processor, acquirer, gateway or merchant) partners to test decryption and support for tokenized payments without have to build and release (including verifying the interoperability of) a test token generation application on their own. Using a single test token generation application across PAGM developers reduces the security risk posed by individual PAGM test token generation systems.

As depicted in the Fig. 1, an architecture for the present technology includes network devices; each of which may be configured to communicate with one another via a communications network, such as the Internet. A user associated with a device may have to

install an application and/or make a feature selection to obtain the benefits of the technology described herein.

In situations in which the technology discussed herein collects personal information about users, or may make use of personal information, the users may be provided with an opportunity or option to control whether programs or features collect 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), or to control whether and/or how to receive content from a content server that may be more relevant to the user. 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 personally identifiable information cannot 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 how the technology collects and uses information about the user.

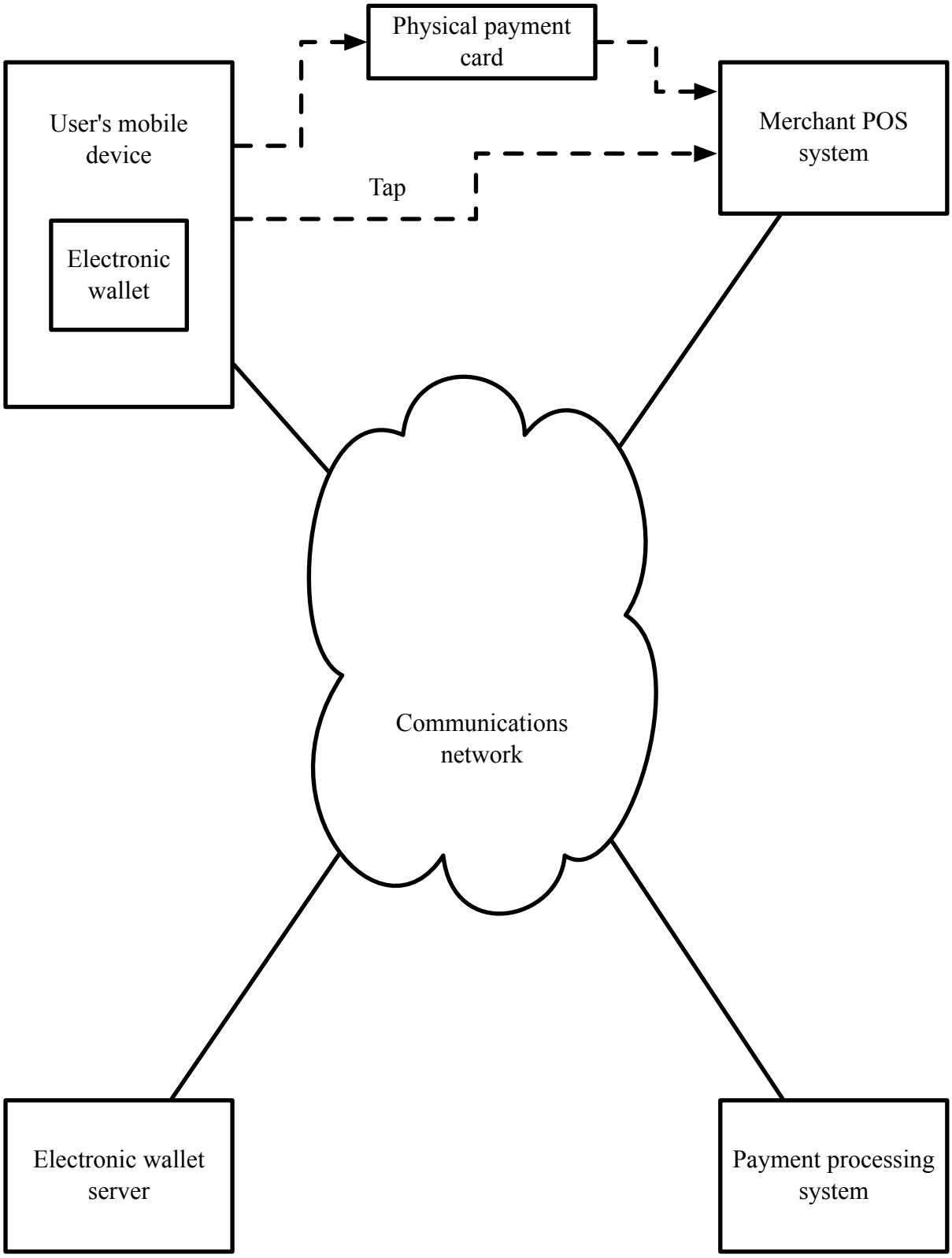
Physical payment card
User's mobile device
Merchant POS system
Tap
Electronic wallet
Communications network
Electronic wallet server
Payment processing system

FIG. 1

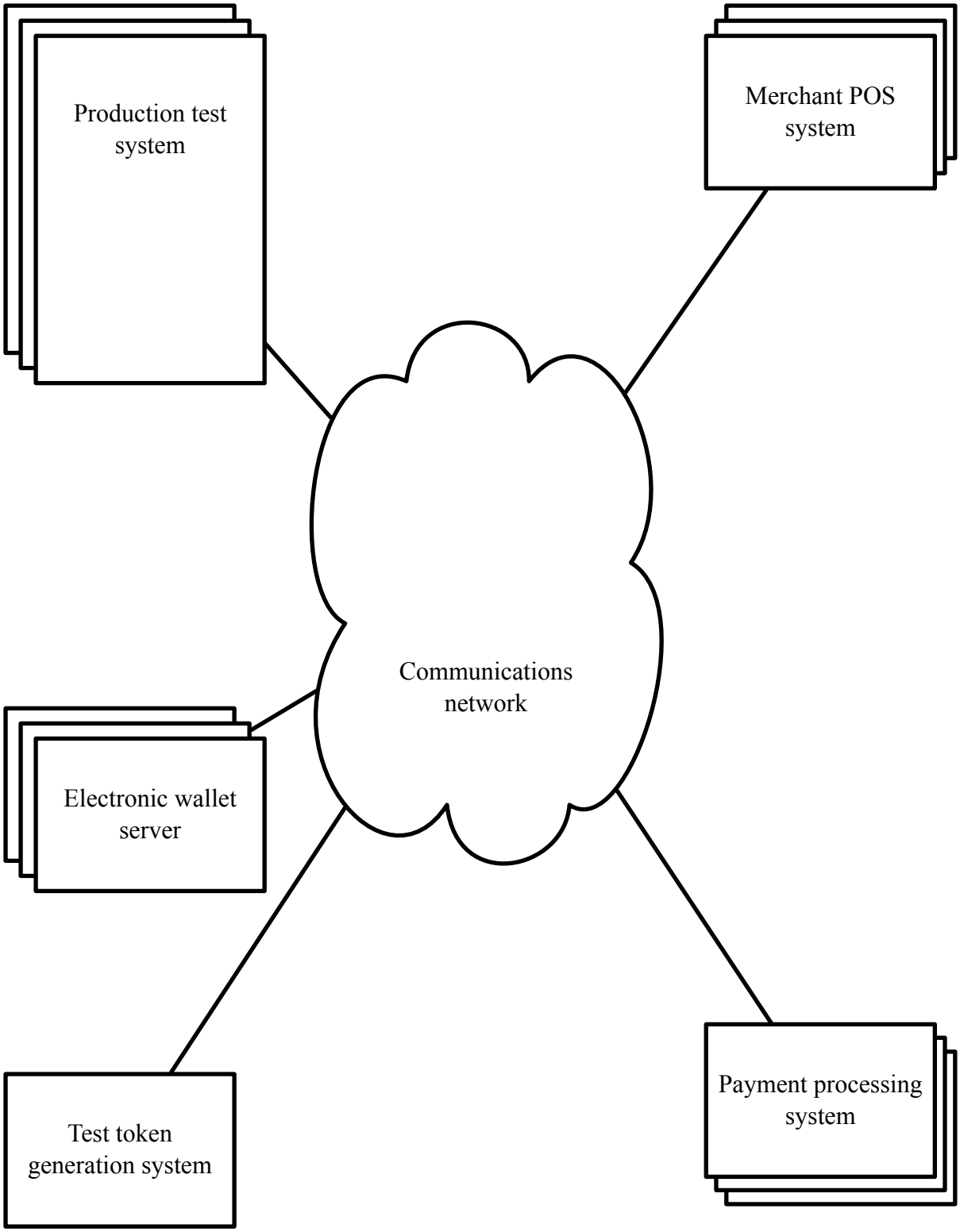
Production test system
Merchant POS system
Communications network
Electronic wallet server
Test token generation system
Payment processing system

FIG. 2