The role of Web standards for enabling a level playing field for payment solutions

Dave Raggett, W3C
W3C Workshop on Web Payments
24-25 March 2014, Paris, France

Introduction

The main purpose of this workshop is to determine whether it is timely to start work on web standards for payments, and whether there is sufficient consensus and support to achieve wide deployment. Before we answer this we first need to answer the following questions:

- Why new standards are needed
- Who they would help
- What are the high level requirements
- What we want to get out of the workshop

The increasing range of payment mechanisms, and the need to support payments across different countries, with different currencies, payment networks and regulatory requirements is imposing an increasing burden on service providers. End users are seeking greater freedom in how they choose to pay, along with improved usability and security. For standards that address these challenges to be widely adopted, it will be critically important to enable a level playing field — open standards should be neutral with respect to payment solution providers large and small, existing or new.

This paper proposes the general solution will involve decoupling web applications from payment solutions, thereby creating greater freedom in how users can choose to pay, and reducing the need for developers to support an increasing range of payment solutions or risk losing customers. How could this work? In the following, the term "wallet" is used for the intermediary between the web applications and the payment solutions. This could be part of the web browser, or it could be provided by third parties.

Payment Process

The steps involved in requesting and fulfilling a payment:

a. The user clicks/taps the pay button on a web app
b. Web app script invokes payment request API
c. Browser routes this to the "wallet"
d. The wallet checks which of the user's payment solutions are applicable to this transaction
e. The user picks from the relevant payment solutions
f. The wallet invokes the chosen solution

g. The payment solution interacts with the user to authorize the payment
h. The payment solution passes proof of payment to the web app via the wallet

In step (e) the user will only want to be shown payment solutions that are applicable to this transaction:

- this solution is capable of satisfying the requester's payment requirements
- there are sufficient funds available to cover the payment
- the user can see the transaction fee she will incur for each payment solution

The user is also likely to want to know how much she has left in each payment solution as a consideration in her choice of which solution to use for this transaction. This all points to the need for open standards for the interface between a wallet and the payment solutions.

It's your wallet

Users should be able to install and uninstall payment solutions. These shouldn't be dictated by one party to the disadvantage of others, e.g. subject to control by the device vendor, browser vendor or the network operator for mobile devices.

Implementation Choices

Payment solutions can be implemented in several ways:

- in the cloud
- as an installed trusted web app
- as an installed native app

The first two could make use of an HTML IFRAME element, as well as the system APIs exposed by the browser or web run-time. These include access to native crypto algorithms, access to secure elements, and access to NFC and Bluetooth.

Security, Privacy, Identity and Authentication

To protect users' privacy and reduce the risk of fraud, payment solutions should minimise the need to transfer and hold sensitive personal data. This is where the discussion about tokenization standards for (virtual) card payments are very timely. Payment solutions are free to use the identification and authentication mechanisms of their own choosing. This could involve the user entering a PIN, pass phrase, secret touch gesture or finger print scan or another biometric.

Identity could be associated with public key pairs stored securely. Payment solutions could be implemented on secure elements, e.g. SIM, micro SD cards, integrated as part of the device's hardware, or even on a separate smart card accessed via NFC.

Who Provides the Wallet?

In all three cases listed above, the wallet would act as an intermediary between the app requesting a payment and the payment solutions.

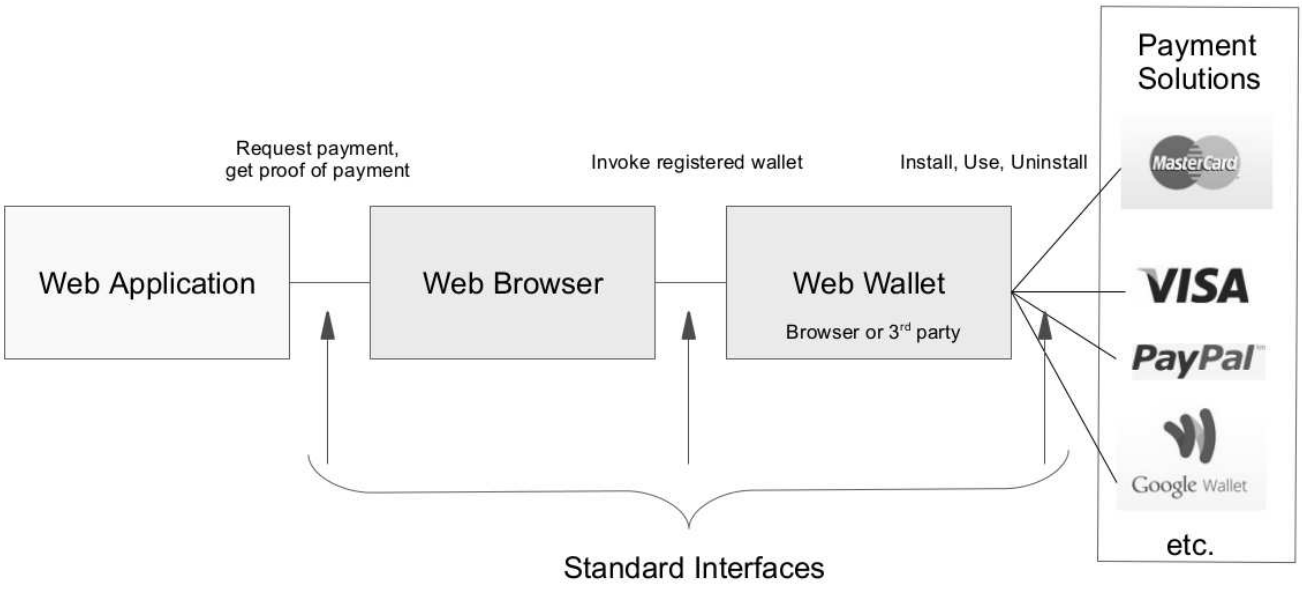
The wallet itself could be provided by the browser vendor, but other possibilities should be allowed. This is important for a competitive market for value added features, including:

- synchronization across the user's devices
- support for loyalty schemes e.g. discount coupons
- prepaid vouchers
- 3rd party apps for reviewing your expenditure and advising on healthier/cheaper alternatives, etc.

The wallet could be implemented in the same three ways as payment solutions. An interesting question is the business model for the wallet provider. There are likely to be different approaches as fits the user's personal preferences, for instance, a subscription fee, or a fee for use of value added services, or the wallet could be provided free in exchange for anonymised access to the user's spending habits, and the user could be encouraged to spend with targetted marketing offers. Business models that favor particular payment solution providers would be a problem!

Matching Process

The matching of requests to payment solution starts with some token matching. Each payment solution provides a list of tokens for the payment schemes it supports. Wild card tokens are possible for solutions that are capable of using trusted third parties to bridge the gap between the user's means of payment and those accepted by the merchant (e.g. differences in currency or payment networks). Such flexibility is likely to involve a higher transaction fee to cover the costs of the various intermediaries involved.



Summary

The burden on developers to support an increasing range of payment solutions, and the desire by users for greater freedom of choice and improved usability point to the need for an intermediary between web applications requesting payments, and payment solutions. This intermediary can be thought of as a virtual wallet. Users should be free to install and install payment solutions just as for a real (physical) wallet.

Standards work could be initiated first for the interface between a web application and the browser, and then for the interface between the browser and the wallet, and the wallet and the payment solutions. These standards should aim to improve the user experience, and must ensure a level playing field for payment solution, as any bias will negatively impact free competition amongst paymentment solution providers. Future work could address person to person payments, and offline payments.