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

Dave Raggett, W3C
Why?

• Greater freedom for users in how they can pay
• Reduced effort on behalf of merchants and developers
• Improved user experience and reduced abandonment rates though instant gratification
• Open competition as basis for easier payments, reduced overheads, and value added services
• Moving away from cash based payments
  – Reducing the burden on merchants to hold cash
  – Easier payments and receipts, e.g. taxis, restaurants
• Easier person to person payments
Payment Front-End Process

- User clicks/taps “pay” button on web app
- Web app script invokes payment request API
- Browser routes this to the user's “wallets”
- Wallet checks which of user's payment solutions are applicable to this transaction
- User selects which payment solution she wants to use
- Wallet invokes selected payment solution
- Payment solution interacts with user as needed to authorise the payment
- Proof of purchase/Receipt passed back
Opportunities for standardization

Web Application → Web Browser → Web Wallet

Request payment, get proof of payment → Invoke registered wallet → Install, Use, Uninstall

Standard Interfaces

Payment Solutions
- MasterCard
- VISA
- PayPal
- Google Wallet
- etc.

Including Carrier billing and other approaches

Wallet and payment solutions can be locally installed or based in the cloud

Web Payments workshop, Paris 2014
Payment Request

• What information is needed from the web app?
  • The amount and currency
  • Description of what the payment is for as sufficient for a receipt
    – Human vs machine interpretable
  • What payment solutions the merchant accepts
    – And the associated details as needed for payments
  • The merchant's identity and the legal jurisdictions applicable to the transaction
    – Reference to contract?
  • User's identity can be provided by the wallet?
    – Delivery address for physical goods
    – As needed for DRM for virtual goods

• What's needed for 3rd party value-added services?

• What about escrow mechanisms?
Proof of payment/Receipt

• Who needs what?
  – Proof of payment for merchant to proceed with delivery of the product/service
  – Receipts for users
    • Held by wallet and available to trusted 3rd party services
  – Legal requirements
    • Taxation
    • Disputes

• Which is better?
  – Proof of payment passed to web app via wallet
  – Or it could be delivered direct to merchant
Improving the User Experience

- Poor User experience increases abandonment rate
- How can we reduce the effort needed from users?
  - Fewer steps and minimal data entry
    - Commensurate with the risk model as understood by a payment solution
- Wallet shouldn't show payment solutions that can't match the merchant's requirements
  - e.g. don't show AMEX if merchants won't accept it
    - List of names for accepted payment solutions
    - Bridging the gap between users and merchants
    - There should be sufficient funds to cover the payment
- Users will want to see
  - How much funds are currently available for each payment solution
  - The transaction surcharge they would incur for each payment solution
Enabling Competition

• The importance of a level playing field
  – Standards should be unbiased, what does this imply?
  – Effective competition as key to improving user experience, richer features and reduced overheads

• Open market for wallets and payment solutions
  – User's should be able to install and un-install these!
  – Standard should allow locally installed or cloud based wallets and payment solutions, right?

• We increasingly have many personal devices
  – Users will want consistency across devices
    • A shared wallet across my devices?

• What about offline payments?
Suite of Standards

• Payment solution providers have their own approaches to managing risk
  - Standards need to provide building blocks rather than forcing a one size fits all approach
  - New APIs for trusted web applications

• Moving away from user name and password
  - User authenticates to device, device to payment solution provider
    • Device or trusted identity provider?
  - Role for secure elements and 2\textsuperscript{nd} factors
    • Issue of who controls the secure element!
  - Revocation of credentials when device is lost, stolen, broken, discarded, or on a change of owner
  - Strong identity as basis for trust (privacy friendly KYC)

• Related technologies
  - Bluetooth beacons, NFC and barcodes
Loyalty Schemes?

- Leather wallet stuffed full with discount coupons clipped from newspapers and junk mail
- Does this model still hold for web payments?
  - Merchants want to know how their customers came to know about them
    - Search engine, link from another website, social or physical media, or plain old word of mouth
  - Encouraging repeat customers
    - Save as you go schemes across a group of participating companies, e.g. UK's Nectar loyalty card
- Is there a role for the wallet to manage discount coupons and prepaid vouchers?