W3C Work Shop Web Payment - Paris -March 2014

Worldline Position Paper - Blois –France - 07 February 2014

Olivier Maas: olivier.maas@worldline.com

Jean Claude Barbezange: jean-claude.barbezange@worldline.com

Worldline: an international Payment Service Provider

Worldline - http://worldline.com - an Atos subsidiary - is an international company present in Europe, Latin America and Asia Pacific in particularly India. It is the European leader and a global player in the payments and transactional services industry. Worldline delivers new generation services, enabling its customers to offer smooth and innovative solutions to the end consumer. As a key actor for B2B2C industries and with over 40 years of experience, Worldline is positioned to support and contribute to the success of all businesses and administrative services in a perpetually evolving market. Worldline offers a flexible business model built around a global and growing portfolio, thus enabling end-to-end support. Its activities are organized around three axes: Merchant Services & Terminals, Mobility & e-Transactional Services, Financial Processing & Software Licensing. In 2012, Worldline's activities within the Atos Group generated pro forma revenues of 1.1 billion euros. The company employs more than 7,100 people worldwide.

Interest in Web Payment

Worldline has been providing e-commerce payment solutions since 1995. These solutions evolve permanently to meet the market requirements, the government, industry and financial rules and the rapid evolution of technologies including Web trends, mobility, security, cryptography… Other Worldline solutions have appeared since around MPI, ACS, wallets, loyalty, POS, fraud detection, Cloud services...

The evolution of Web payment

At the beginning of the e-Commerce twenty years ago, the main solution of Web payment were based on secured forms (https) to fill banking card information (card number & validity date) combined with online control and connection with the card issuer to request an authorization. These kinds of services are still proposed by trusted players such as banks or specific providers. Payment means vary between countries so card information is replaced in places by – for instance - bank account identification with credit transfer or direct debit. For low amounts, payments are mainly done through Telco or ISP rebilling.

Specific solutions dedicated to payment or more globally to check-out such as virtual cash register were launched on the market. They proposed to include complementary user information such as shipping user address. Overall, these solutions have not reached a wide success (e. g. Passport from Microsoft).

Another approach has been to link the payment mean to an account hosted by a service provider. Payment is done using a simple identifier such as an e-mail address (E.G. Paypal), phone number or other specific ID. A first level of security is provided by a password filled on the secured form. These solutions rely on legacy bank payment: debit card; credit card, credit transfer, ..)

Some mechanisms such as pay button, "one click" payment … increase the user convenience.

After some shorted-lived eCash trials at the end of 1990s (E. G. CyberCash), crypto-currency solutions became mainstream five years ago with Bitcoin. Based on new functional scheme not relying on trusted third party, these open source P2P solution use basic cryptography and Internet network technologies to propose alternative solutions to legacy scheme and wallet application. There are similar approaches with alternative currencies in the alternative communities (social network, local initiative, ..). They provide ways for low amount payments without pre-paid or Stored Value Accounts.

Finally, the mobile and connected devices (smartphones, tablets, TV, play station, connected car interface, ..), mixing web and apps complete the landscape. The information exchange between this various channel may use activation with local messaging or push notifications, bar code (QRcode) flashing, NFC technology, WiFi or BLE technology, … or even manual user action or refilling.

For security reasons and to limit fraud, the one-line web form has been extended by more personal informations (e.g. Secure Code from MasterCard) and an authentication phase has been developed (e.g. 3D Secure process) requiring additional web form to fill personal data, OTP, ... For additional fraud detection, the legacy transaction information (buyer identification, buyer financial velocity, … , merchant and product/service risk, ..) are completed by more extensive user profiling based on user agent chain and device/browser information (fingerprinting).

For face to face payment, some new POS (Point Of Sale) terminals are built around a Web architecture approach (E. G. Web POS in Brazil).

In 2014, the number of innovative solution of web payment soars with a trend of convergence between e-commerce and brick & mortar commerce.

Main Market requests

Today, payment is becoming less a standalone asset. It has become part of the check-out in the global user experience. It is or it will be a mandatory commodity characterized by strong availability, seamless integration, trustable by buyers, adaptable to innovation, .. but without high value for the end user. Like electric power, it just has to be available.

The added value is positioned on all the purchase lifecycle : at the check-in (buyer identification, push of special offers, recommendation, ..) or at the check-out (discount, loyalty, shipping, credit, ..).

For merchant, payment needs to be adapted to enable a differentiating user experience. So payment needs to be integrated in the merchant's innovation process to increase its turnover. Merchants are also expecting a similar user experience in face to face and in remote payment.

For buyers, the requirement is to have the right level of information to understand what he does and what will be the usage of his personal data. The technical web tools have to assume transparency and privacy.

The financial institutions and merchants aim at reducing the fraud level on the payment transaction. It is a part of organization and risk management.

In summary, the payment user experience requests both more convenience and more trust.

Lack of standard in the scope of W3C

Today, there are no fully adapted functional and technical responses to cover all the market Web Payment requirements. Current answers seem even more badly adapted to enable future innovations due to web ecosystem evolution (new local connected devices of Internet of Thing, wearable technologies, …)

It remains a big challenge for W3C to fill this gap and to provide efficient technical standard tools.

Potential Worldline contributions to W3C Work shop

Worldline would contribute to several topics to specify or complete some W3C standards:Input type and taxonomy

Some input type require standardization for example by setting as default AUTOCOMPLETE=OFF for some fields like "cardnumber" or "cvv" and require the same behavior as on smartphone(last character displayed then replaced automatically by astar)

In terms of taxonomy, an effort needs to be done – see the work of GoodRelations for example

Activation/interface html tag

Several technical standardization needs are identified concerning legacy web forms to simplify the user look & feel and the developer task. For example (not exhaustive):

Virtual PAD

Payment data are obviously sensitive data. When a user provides these data from his device using classic keyboard input, a keylogging risk exists. In some cases, depending on how sensitive the data are, the use of virtual keyboard could be standardized in order to reduce the risk of keylogging. However, attention shall be paid to the fact that virtual keyboards are currently implemented as on-screen keyboards and thus visible for an external observer.

Bar code as QRCode

QR (Quick Response) code is a machine-readable matrix barcode containing information. In a payment context, a QR code can offer a quick and effortless access to the payment application or platform (along with all the context data related to the transaction). QR code convenience could increase conversion rate.

CAPTCHA

A CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a kind of visual (and audio) challenge-response test which aims to determine whether the “user” is human or a computer. A common implementation uses a distorted image representing letters and/or digits that the user has to type.

In the payment context, use of CAPTCHA could be used for example to prevent bots from trying to provide many successive card numbers in order to discover accepted or not enrolled ones.

Wallet

Payment wallets are applications or online services that allow users to store and use their payment means.

Regardless of wallet implementation, information has to be exchanged with the e-commerce platform which should:

- Provide a transaction context to the wallet in order to initialize the transaction
- Receive a transaction payment response from the wallet
- Be notified on the payment process

To ensure interoperability with any wallet application or service, steps and exchanges should be specified and standardized.

Authentication integration

Seamless authentication integration in web page payment or check-out phase becomes mandatory to maintain an acceptable balance between user convenience and trust. Strong authentication is a main part of Web payment front office transactions.

The authentication is evolving today with mobility and new needs (commerce, convergence between physical and logical access, BYOD, ..) with introduction of biometric tools (probably more behavioral than physiological) the multi-device following and new approach. We will be reviewing the first publications of the FIDO Alliance (www.fidoalliance.org/) and we will investigate future Web standard tools that help get a better integration and interoperability of these authentication modes.

This part has to cover the needs for pilot biometrics interface from Web browser (BioAPI).

Smart card reader html tags

For strong authentication or for connection to payment application hosted in a Secure Element device (EMV), the reference to ISO 7816 protocol exchange cannot be ignored. The requirement is to have a set of html tags to manage interaction with contact or contactless smart card reader on the device:

- To select or activate à reader
- To open/close a session
- To send/receive APDU one by one or by block.

The specification contributions initialized by Gemalto and Intel on a Secure Element API (http://opoto.github.io/secure-element/) could be a base for W3C Web payment common standard initiative.

Web RTC peer-to-peer

Web RTC is today technically promising in P2P model. Regarding the adoption of peer to peer (P2P) currencies, we could expect that the ecosystem will suffer from the same difficulties and pitfalls as the communication or file sharing ecosystem.

In those ecosystems, the need to have a client installed on the user's computer or mobile, using the latest version of the P2P communication protocol has resulted in a less rapid adoption, because users had to install or update clients regularly to keep using the P2P system. In P2P communication especially, the ecosystem is currently moving towards using networking mechanism that are embedded in web browsers. Indeed, Web RTC / RTC Web is embraced by a large number of actors that aim at developing and deploying real-time communication services that use the capabilities of Web RTC to establish direct communications between browsers. Our observation of this movement tends to convince us that Web payment systems should embrace Web RTC too to ease the deployment of P2P payment mechanisms. This will come at the expense of an effort to ensure the privacy and the security of those direct communications, but we are convinced that the advantages of an effortless deployment are worth it.

Fraud detection data profile

Web payment fraud is increasing. The scoring of transaction has to integrate more information about web browser, its software environment, its option parameter, its hardware environment,.. The user agent client string could be reviewed and extended to increase the software user fingerprinting in the respect of user data privacy. Fraud detection is indeed based on information shared between the players. Financial part of transaction are already standardized (ISO 20022 or ISO 8583). Extension to the Web part with a shared data dictionary is now compulsory.