Web Payments Capabilities

Editors:
Patrick Adler, Federal Reserve Bank of Chicago
Jörg Heuer, Deutsche Telekom
Adrian Hope-Bailie, Ripple Labs
Ian Jacobs, W3C
Manu Sporny, Digital Bazaar

Contributors:
Patrick Adler, Federal Reserve Bank of Chicago
David Ezell, National Association of Convenience Stores (NACS)
Katie Haritos-Shea, W3C Invited Expert
Jörg Heuer, Deutsche Telekom
Adrian Hope-Bailie, Ripple Labs
Ian Jacobs, W3C
Dave Raggett, W3C
Manu Sporny, Digital Bazaar

Abstract

This document is part of a series of deliverables from the W3C Web Payments Interest Group:

- A @@Vision for Web Payments@@ describes the desirable properties of a Web payments architecture.
- Web Payments Use Cases 1.0 is a prioritized list of Web payments scenarios that the Interest Group expects to address via the payments architecture. These use cases establish a scope of work and an analysis of the use cases will result in a set of requirements (technical, regulatory, etc.) that will inform future standardization.
- This document describes a set of high level capabilities and key architecture principles needed for web payments. When used together they will enable those involved in a payments process to successfully complete the outlined use cases.
- A Roadmap proposes which groups (in or outside of W3C) should take the lead on creating standards that support these capabilities.

This document is structured by functional capabilities and core overarching principles to facilitate uptake by future standards groups and with the intention of helping ensure consistency across resulting standards work.

We organize features for which we expect to propose standards into blocks of “capabilities.” There are other features one would ordinarily expect related to a capability (e.g,. the ability to generate a statement for an account). However, we only list those features for which we expect to propose standards work.

We have organized the capabilities into two groups: those capabilities that we propose should be standardized starting in 2015, and those (not yet ordered) capabilities to be standardized subsequently. The Web Payments Interest Group plans to reach consensus on stable set of capabilities for 2015 and use the second section as a repository for ideas that arrive on an ongoing basis.

Status of This Document

This section describes the status of this document at the time of its publication. Other documents may supersede this document. A list of current W3C publications and the latest revision of this technical report can be found in the W3C technical reports index at http://www.w3.org/TR/.

This document is in early draft state and is expected to rapidly evolve based on broad feedback and input from the Web Payments Interest Group
This document was published by the Web Payments Interest Group as an Editor's Draft. If you wish to make comments regarding this document, please send them to public-webpayments-comments@w3.org (subscribe, archives). All comments are welcome.

Publication as an Editor's Draft does not imply endorsement by the W3C Membership. This is a draft document and may be updated, replaced or obsoleted by other documents at any time. It is inappropriate to cite this document as other than work in progress.

This document was produced by a group operating under the 5 February 2004 W3C Patent Policy. W3C maintains a public list of any patent disclosures made in connection with the deliverables of the group; that page also includes instructions for disclosing a patent. An individual who has actual knowledge of a patent which the individual believes contains Essential Claim(s) must disclose the information in accordance with section 6 of the W3C Patent Policy.

This document is governed by the 1 August 2014 W3C Process Document.

Contents

- Capabilities for the next iterations of standards
- @@Possible appendices to add
- Guiding principles and high-level requirements

Roles involved in capabilities

The capabilities described in this document primarily involve interactions among the following parties to a transaction:

Payer
The payer provides a source of funds as required by a transaction.

Payee
The payee receives funds as required by a transaction.

Payment Account Provider
At its core, a payment is a transfer of value from one account to another. An account is a store of value with a balance and change history. The payment account provider is responsible for managing and controlling access to one or more accounts on behalf of the account holder (payer or payee). Payers and payees access their accounts through payment instruments. The rules that govern usage of a payment instrument constitute a payment scheme. The set of accounts offered by a payment account provider is called a ledger.

Payment Services Provider
The payment services provider provides services to the payer and/or payee to facilitate a payment.

Regulator
The regulator is responsible for monitoring some payments activities and enforcing legal requirements.

About roles

A role may be carried out by many different *types of organizations*. For example, "account provider" may be carried out by financial institutions, mobile operators, tech companies, or cryptocurrency systems.

A given role may be carried out by *several collaborating parties*. For instance, a payee may use a payment service provider which in turn uses a card network. The actions of these intermediaries may vary, from simply forwarding messages to fulfilling regulatory obligations.

Capability Groups

This document groups functional features into capability groups which are intended to provide a consistent structure for representing coarse grained capabilities and detailed features across working groups and standards bodies, and which also allows for consistent focused conversation topics for the IG to be able to communicate with these groups as standards for these capabilities are developed.

The coarse grained capabilities are:

- **Identification and Authorization** - includes features related to the identification of actors and systems participating in the System, as well as features related to the credentialing or authorization of actors to perform actions within the System
- **Offers -** includes features related to generating, sending and receiving offer information in a standard way for communication with entities external to the system and between entities in the system.
- **Invoices -** includes the ability to communicate invoice information in a standard way between both defined roles in the System and from external systems.
- **Payments** - includes the most core aspects of the payment process and are focused on only those features which are common to all payment processes
- **Accounts** - includes functionality required to manage accounts used as part of the payments process
- **Receipts** - includes functionality related to the communication of receipts in a standard way between both defined roles in the System and from external systems.
- **Loyalty** - includes functionality required for creation and exchange of standardized loyalty information between defined roles in the System
- **Core** - Includes functionality that applies broadly to the entire System or enabling functionality that is required to support one or more of the defined capabilities

Capabilities for standardization starting in 2015 (Iteration 1)

The section defines capabilities and features that have been identified by the Interest Group for the initial iteration of web payments standardization work.

Identification and Authorization

1. Registration
    a. Payer and Payee able to register with Payment Services Provider to obtain credentials used for payments process

2. Identification and Discovery
    a. Payer is able to securely locate public identifier of Payee to be used as part of payment process
    b. Payee is able to obtain public identifier of Payer participating in payment process
    c. Payer identifier is persistent across devices
3. Credentials
    a. Payer is able to exchange standard format credentials with Payee to validate attributes necessary to complete the payment
4. Strong Identity Binding
    a. For payments and accounts meeting certain requirements, strong binding of Payer or Payee Identity will be required to adhere to regulatory requirements

Offers

1. Generate Offer
    a. Payee is able to generate a standard format offer which provides information on specific products or services being offered, and additional information on payment instruments accepted, or terms of the offer.
    b. Payer is able to generate a standard format offer which can be accepted or declined by the payee.
    c. Payee is able to create scheduled/recurring offers
2. Receive Offer
    a. Payer is able to receive offer in machine readable format and use it to initiate payment request
    b. Payee is able to receive offer in machine readable format and use it to create invoice and

Invoices

1. Invoice creation
    a. Payee is able to generate a standard formatted invoice and communicate to Payer as part of the negotiation of payment terms
2. Invoice receipt
    a. Payer is able to receive standard formatted invoice
3. Invoice data
    a. Invoice provides payer with Payment instructions for making payment to Payee
    b. Invoice identifier is returned to Payee via payment process to verify payment is complete

Payments

1. Payment Instrument Discovery and Selection

A. Payer and payee are able to discover payment instruments/schemes which they have in common and are able to be used in the payment process
B. Payer is able to select payment instrument for use in the payment process
C. Payee is able to communicate requirements (or preference) if a specific instrument is accepted

2. Payment Initiation
    A. Payer is able to initiate a payment using selected payment instrument
    B. Payer is able to select Payee via:
        1. Information received via Invoice
        2. Individual contact information
        3. Information from past payees
    C. Payee is able to initiate a request for payment to payee's designated account provider
    D. Account provider is able to initiate a payment on behalf of the Payee based on Payee's requested schedule and frequency (recurring payment)
3. Payment Acknowledgement
    A. Payee is able to receive confirmation that payment has been successfully complete
    B. Payer is able to receive verification that payment has been successfully received.
    C. Account provider is able to receive confirmation that payment is complete
4. Regulatory/Legal Compliance
    A. Regulator is able to access/view required payment, payer, and payee details for payments that take place within their jurisdiction
    B. Regulator is able to intervene in payments meeting or exceeding certain thresholds or criteria in order to comply with jurisdictional laws and requirements

Accounts

1. Account Registration/Enrollment
    a. Payers and Payees are able to register accounts that will be used as part of the payment process with Payment Service Provider of their choice
2. Receive Funds
    a. Payees are able to receive payments funds to registered accounts

Receipts

1. Create Receipt
    a. Payee is able to create receipt and communicate receipt to Payer following completion of payment

2. Receive Receipt
    a. Payer is able to receive receipt and persist for future use (ex. returns, reimbursement, etc)

Loyalty
TBD

Core
TBD

@@We would like to include diagrams; may not have them for June FTF meeting

Capabilities for the next iterations of standardization

The purpose of this section is to serve as a pipeline of capabilities and features that have been identified by the Interest Group for prioritization of subsequent iterations of standardization work.

Identification and Authorization

TBD

Offers
1. Discounts
    a. Payee is able to able to apply discount to offer and invoice
    b. Payee is able to apply standard loyalty identifiers to offers
2. Coupons
    a. Payer is able to apply coupons to offers
    b. Payee is able to issue general use coupons
    c. Payee is able to issue coupons specific to payer identifier

Invoices
TBD

Payments
1. Settlement and Clearing

2. Scheduled Payments

Accounts
TBD

Receipts
TBD

Loyalty

Core
TBD

Summary of Capabilities for Version 1

Credentials and Identity

- Provision and verification of credentials (e.g., for account creation, at purchase time, for delivery of product, to meet regulatory requirements, etc.).
-

Security

We expect the underlying system (e.g., browser, operating system) to provide support for the following security features that support the other capabilities:

- Strong Authentication
- Digital signatures and validation
- Transport layer and content security

Summary of Capabilities after version 1

Offers

- Machine readable offer
- Operation from within a native application
- Subscription
- Operation from point of sale kiosk via NFC

Payment

- Automated and assisted selection of payment instrument

Marketing Elements

- Application of coupons and loyalty cards to purchase

Guiding principles and high-level requirements

A number of principles and high-level requirements should be taken into account as part of future standardization. The Web Payments Interest Group also anticipates creating a more detailed set of requirements as input to future standards groups.

Extensibility

- Because the Web payments architecture will accommodate a great variety of payment schemes (existing and new), we expect to future standards to support interoperability on a minimal set of features and also support scheme-specific extensions. Therefore, data formats must be easily extensible.

Identifiers

- Payment schemes define identifier syntax and semantics (e.g., primary account numbers (PANs) for credit cards, or bitcoin account identifiers). We expect to support scheme-specific identifiers. But where global identifiers are required and are not scheme specific, we expect to use URIs.

Security

- Messages must not be altered in transit, but may be included as part of encapsulating messages created by intermediaries.
- It must be possible to provide read-only access to transaction information to third parties (with user consent).
- Signatures must be non-forgeable.

Identity, Privacy, and Consumer Protection

- To satisfy regulatory requirements and financial industry expectations, some use cases will require strong assurances of connections between a Web identity and a real-world identity.
- At the same time, any source of information that can lead to the unintended disclosure or leakage of a user's identity (or purchasing habits) is likely protected in a jurisdiction somewhere in the world by a legal/regulatory entity having responsibility for its citizens.
- For discussion: the role of per-transaction pseudo-anonymous identity mechanisms for some use cases. These mechanisms would make it much more difficult for an unauthorized party to track a user's purchasing habits from 1 transaction to another

transaction. This will also eliminate the loss of that identity from affecting other services that user is enrolled in.

- Regulations in several jurisdictions require the consumer to be notified every time their personal information/credentials are accessed. To discuss: cryptography requiring a user's input/knowledge to open that information.
- Some purchases in combination (e.g., products accommodating prenatal care needs) will leak sensitive information. To discuss: dynamic key construction can be applied to each line item in a receipt to help prevent unauthorized data mining of individuals, legal & regulatory snooping. Even if the protected information is stolen or accidentally forwarded to unauthorized parties they will not have the correct tokenized inputs to recreate the dynamic keys to unlock access to the protected information.
- Role based access controls when applied to dynamic key construction for each individual credential or large sets of data will help facilitate interoperable access without needless duplication and encryption of information for each authorized party. For discussion: Use dynamic keys to protect a static key where various dynamic keys can be used to unlock the static key that protects the sensitive content.
- The system should support privacy by requiring only the minimal amount of information necessary to carry out a transaction. Additional considerations (e.g., marketing initiatives with user consent, or legal requirements) may lead to additional information exchange beyond the minimum required.
- Payment account providers must take measures to ensure that account identifiers are not, on their own, sufficient to identify the account holder.
- Another suggestion: "Don't require personal authentication, but make sure it can be done properly"

Legal and Regulatory

- In some jurisdictions legal or regulatory entities may need to be granted "time-limited access" to a transaction to view specific credentials and purchased items of the user. The system should limit what is viewed to the minimum necessary. Examples: Government subsidies such as food stamps, controlled substances. In these cases those particular line items in the receipt may be required to be viewable via individuals or computers charged with the responsibility to prevent abuse of those programs (e.g., unauthorized reselling). There may also be a requirement to view identities or credentials.
- For certain classes of payments, such as high value or international, it must be possible to provide role-based access controls to pierce a pseudo-anonymous identity mechanism so the transaction can be counter signed by a legal, regulatory, or KYC/AML system yet safeguard against disclosing unnecessary information. It must be infeasible for the piercing of this mechanisms to leak enough information for those authorities to forge user information.

Appendix A: Capabilities organized by payment phase

@@Ian includes here the short labels (e.g., Payment Instrument Discovery and Selection) ordered by payment phases; should be generated based on tagging.

Appendix B: Capabilities organized by role

@@We will see; should be generated based on tagging.

*********Incorporate the material below into the "details" section above or the "guidelines/principles" section as appropriate********

Functional Capabilities

Offer Management

Capability Overview

Components need to be able to generate, send and receive offer information in a standard way for communication with entities external to the system and other components in the system.

Interactions

Offer management services are likely to be required by both the Payer and Payee roles as this portion of a payment flow may be initiated by either role.

Key Considerations

Invoice Management

Capability Overview

The architecture willPayment agents need to desribe a meansbe able to receive invoice information in a standard way from both External Entities and from other Payment Agents. Invoices should be represented in a structured way which can be understood and interpreted by both human and system actors.

Interactions

Offer management services are likely to be required by both the Payer and Payee roles as this portion of a payment flow may be initiated by either role.

Key Considerations

Invoice data must include:

- Acceptable Payment Methods
- Invoice Currency
- Payee Name
- Identity/Location of Payment Address (URI of the Payment Agent or System that will receive payment)
- Non-Forgeable Cryptographic Hash/Digital Signature to prevent tampering
- Structured list of items and purchase amounts included as part of the invoice
- Total amount of invoice
- Date/Time invoice was generated
- Identification of the Payer and Payee entities that are a party to the transaction
- Container or data fields to allow for inclusion or reference to information that may be part of or required to fulfill the invoice (ex. terms and conditions)

Core Capabilities

Persistence

Capability Overview

Components need the ability to persist information and represent state related to the their operation. The following information will need to be included:

1. Authorization information defining which entities have permission to perform which actions.
2. Authentication data (credentials) required to execute actions against other components or systems (such as account providers).
3. Cache data to facilitate ease-of-use and efficiency (Example: Recurring payees).
4. History of payments processed
5. Identity and configuration metadata of the component instance

Cryptographic Signatures / Signing of core data elements

Capability Overview

Due to the distributed nature of this architecture, it will be critical for components to be able to access or provide Cryptographic Signature capabilities for the exchange of information in a

secure/tamper-resistant manner. Key information that will need to be signed/encrypted include:

- Offer and Invoice Data
- Payment/Transaction Details
- Proof of Purchase (Receipt)
- Sensitive account and personal details used as part of the payment process

User Interface

This section outlines key capabilities that are specifically needed to support the interaction of users with the components of the Web Payments Architecture.

Interface

User agents (ex. browsers, native apps, server software) need to be able to call a standard interface/api that will provide the following functions:

1. Account Management
    a. Get Account
    b. Get Balance
    c. Preferred Payment Instrument Order
    d. Account Nicknaming
2. Consume an Offer
3.
4. Transaction Management (Coordination of payments process)
    a. Create Transaction
    b. Complete Transaction (Record fulfillment of invoice)
5. Invoice Management
    a. Receive Invoice (payment request)
    b. Process Invoice (initiate payment)
    c. Generate Invoice (request payment)
6. Payment Management
    a. Pay
    b. Accept (Receive Payment)
7. Receipt Management
    a. Create Receipt
    b. Accept Receipt

Account Provider Interface

Components need a way to interact with accounts that they will use as part of the payments process. To facilitate this, they need to provide an interface/set of apis to facilitate interaction with accounts, account providers/custodians (ledgers) and any other stores of value.

Interface

1. Get Accounts
    a. Local
    b. Remote
2.

Communication

Persistence

Discovery of Available Payment Agents

Discovery of Payment Agents

Privacy of Payer Information

Security

Secure communications between componentss

Transport Layer

Content (payload) Layer

Authentication and Authorization of Entities and User Agents