Electronic Commerce Research and Applications xxx (2015) xxx–xxx

Contents lists available at ScienceDirect

Electronic Commerce Research and Applications

journal homepage: www.elsevier.com/locate/ecra

Towards a web payment framework: State-of-the-art and challenges

Antonio Ruiz-Martínez

Department of Information and Communication Engineering, Faculty of Computer Science, University of Murcia, Spain

ARTICLE INFO

Article history:
Received 2 August 2015
Received in revised form 4 August 2015
Accepted 4 August 2015
Available online xxxx

Keywords:
Electronic commerce
Electronic payment systems
Web payment framework

ABSTRACT

In the Internet era, through the web, and access to content, products and services has evolved in a spectacular way. At the same time, different business models have been developed for access and consumption. Many of these business models are based on making a payment via the web. The use of electronic payments in the web is a complex issue since it involves the support of multiple payment instruments, the secure exchange of payment information, receipts, and so on. A proposed solution approach to web payments is the development of a *web payment framework* based on a layered approach. This article analyzes the functionality this framework should provide, what solutions may be used, and what issues still need to be addressed so that a web payment framework can make e-payments more widespread.

1. Introduction

In the last ten years, electronic commerce activities have been associated with important changes and innovations, from a technological perspective and for the business models that have been introduced. Recent advances in electronic payments also reflect this. The use of e-payments based on credit and debit cards has been growing on the Internet over the years, and systems such as PayPal have seen as its volume of payments have increased year by year. More recently, the birth of Bitcoin (Nakamoto 2008, Barber et al. 2012) has been a watershed event in the adoption of electronic cash to make payments on the Internet (Peck 2012, Hileman 2014). Until recently, the adoption of e-cash had mostly been a series of failed initiatives. At the same time, new payment systems such as Apple Pay have appeared. With several payment instruments available today, many of them mobile payment systems, the challenge has been to make it easier for the different to perform the different steps that take place for a purchase transaction so that security and interoperability are guaranteed. This includes a variety of stakeholders, such as consumers, merchants, banks, mobile operators and payment services providers.

B2C transactions on the web typically take several steps in which payment information and payment systems are used, in order to complete them (Ruiz-Martínez et al. 2012). First, the consumer locates the product or service (shortened to just "product" hereafter) to be purchased or consumed through her web browser installed on her PC or her smartphone. Then she will obtain the description of the product with the payment conditions required by the merchant. Depending on the kind of transaction, the price and payment options available may be negotiated and chosen. Thereafter, the consumer will proceed with the checkout and the payment will be made. If the payment succeeds, the transaction will finish and the consumer will be able to acquire the product, for example, via a ticket that is issued to confirm purchase. Associated with the purchase, the merchant will provide a receipt of the transaction to the consumer. The consumer may receive some loyalty information (ticket, points, coupons) that can be used in subsequent transactions to obtain better prices or other advantageous conditions (Turban et al. 2014).

Related to product access, if a problem occurs or the product does not satisfy the conditions agreed to, the consumer will be able to request a refund. If the request is accepted, the merchant will refund the payment by issuing a ticket or some kind of a coupon that will be considered as an alternative currency (de Lange et al. 2012), or by making a payment to the consumer. In this scenario when a web payment is made, there are different exchanges of information. In these exchanges, different kinds of payment information and different payment instruments can be used. Currently, the web and the different standards that define it do not offer a comprehensive and standard solution that supports all of the steps mentioned though. The solution proposed to overcome this challenge has been the definition of a *web payment framework* (Ruiz-Martínez et al. 2012, Jaffe and Boyera 2015, W3C 2015b). It aims to facilitate, along the purchase process, the exchange of payment information and the use of different payment instruments in an easy way at the same time it guarantees interoperability, trust and security.

The development and adoption of this kind of framework is a challenge though. It requires the definition of a set of components

E-mail address: arm@um.es
URLs: http://ants.inf.um.es/~arm

http://dx.doi.org/10.1016/j.elerap.2015.08.003
1567-4223/

that perform different kinds of tasks. With this in mind, I will analyze two issues. First, I will examine the tasks a web payment framework should accomplish in each step of the purchase process, and what solutions have been defined for these tasks so far. Second, based on the current state-of-the-art, I will asses the different issues that are still to be overcome in order to have a comprehensive and standard solution that performs the tasks previously mentioned.

2. Web payment frameworks: layers, goals, and current solutions

The development of a web payment framework has been addressed in several previous academic and industry research works. They include: the Joint Electronic Payment Initiative (JEPI) (Chung and Dardailler 1997); the Secure Electronic Marketplace for Europe (SEMPER) (Lacoste et al. 2000b); and the W3C Common mark-up for micropayment per-fee-links (Michel 1999). The latter contains some ideas proposed in this specification that were followed in another article, by the present author (Ruiz-Martínez et al. 2009). Other initiatives include the Internet Open Trading Protocol (IOTP) (Burdett 2000, Hiroya and Kawatsura 2004, Dulai et al. 2013), and the Payment Frameworks (PayFrameworks) related to the purchase of electronic products (Ruiz-Martínez et al. 2012).

These solutions were not adopted due to two main reasons. First, the use of e-payment systems was not widely diffused, and some of the core technologies were not mature enough to support payments effectively (e.g., the web, security, and semantics). Second, not all of the stakeholders were taken into account in their development. The participation of all stakeholders is especially relevant for the success of any mobile payment initiative (Gannamaneni et al. 2015).

Currently, the situation in the e-payments area is different. The use of e-payments is thriving and there are different mobile payment solutions too. They include: Paypal, EMV, BulaPay, Google Wallet, Square Cash, Bitcoin, Apple Pay, MPesa, and APSWPP, among others (Javan and Bafghi 2014). The variety of e-payments solutions, mainly mobile payment systems, is causing problems with interoperability, usability, and security. To solve these problems and to enable competition and innovation in web payments, the W3C has launched the Web Payments Interest Group (WPIG) (Jaffe and Boyera 2015, W3C 2015b). There are also other initiatives of standardization considering issues regarding e-payments such as the Financial Business Ontology (2015).

Fig. 1 shows a *conceptual layered architecture* that reflect all of the elements a payment framework should define to support the core tasks, and that is based on the initiatives I have mentioned.

In this work, I will follow a top–down approach for the description of the different layers and solutions available so far. The Web Application layer shows information about the product that a consumer may be interested in purchasing through a web page, and also includes payment information. How this information is provided is fundamental to produce a good consumer experience and prevent the risk of shopping cart abandonment. This information should also be exchanged in a secure way. To this end, it is embedded in the web page using some language that allows its automatic processing, which also is intended to improve the consumer experience. For embedding this information in a web page (HTML5), such microformats as Turtle, RDFa and JSON for Linking Data (JSON-LD), which has been adopted by WPIG, can be used. These formats attempt to express meaning on the web in a simpler way than the XML vocabularies do.

With this data, a consumer should also have information about the identity of participating entities in the system that allows her to determine their trustworthiness. For identification and authentication, there are several mechanisms available. They include X.509 certificates, OpenID Foundation (2015, Recordon and Reed 2006), Mozilla Persona (Mozilla 2015), WebID (Story 2015, W3C 2015c), and Identity Credentials from WPIG (Sporny 2014b, W3C 2015a). The latter initiatives have arisen because certificates do not provide enough information about the kind of entity that is involved. For example, the WebID and Identity Credentials aim at identifying an entity through the web at the same time they allow working with her credentials. Currently, these initiatives are still in draft form and need to be developed further.

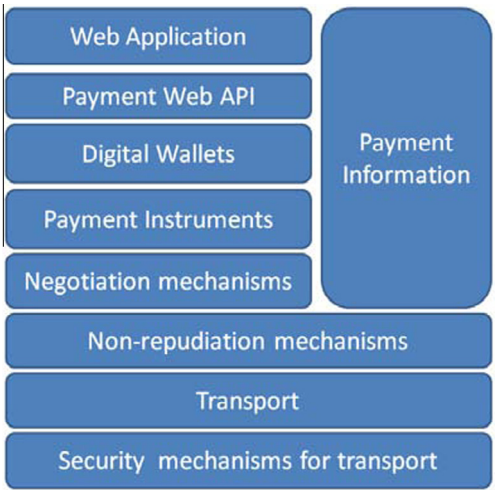

Fig. 1. Web payment framework layers.

As for trust, there are two approaches to determine the extent of trust that exists for a web site. On the one hand, it is possible to use directories of certifying identities, such as TRUSTe. On the other hand, some mechanisms based on the concept of the "Web of Trust" are being developed, such as the Monkeysphere Project and WebID. The Identity Credentials specification (Sporny 2014b) aims at unifying the work done in identity projects such as WebID and Mozilla Persona. It provides expressive information on identity that allows associating third-party information with an entity and establishing whether it is trustworthy. It also aims to define integration mechanisms with other solutions, such as OpenID and OAuth.

When the consumer confirms the transaction, the payment process is executed by invoking the services provided by the Payment Web API. This process should be easy, quick and comfortable for the consumer.

The *Payment Information layer* represents the vocabularies and semantics used to describe information related to a purchase: products and their categories within various catalogs, payment instruments, loyalty information, and so on, as I noted earlier. The representation of this information in a semantic way facilitates the process, so that subsequently, the purchase processes can be delegated to intelligent agents (Rosaci and Sarn 2014) or recommender systems can be built (Wang et al. 2014). This information can also be shared in applications of social commerce, as an extension of e-commerce (Huang et al. 2014). The use of loyalty and coupon schemes is being introduced in mobile wallets as an additional feature (Gannamaneni et al. 2015).

Currently, the main efforts being made to define ontologies available for this purpose are progressing. They include: the GoodRelations ontology for details of products, which is widely supported by search engines (Ashraf et al. 2011); the schemas and ontology defined in the per-fee-link framework, mainly focused on payment information (Ruiz-Martínez et al. 2012); and

Please cite this article in press as: Ruiz-Martínez, A. Towards a web payment framework: State-of-the-art and challenges. Electron. Comm. Res. Appl. (2015), http://dx.doi.org/10.1016/j.elerap.2015.08.003

the Payments Ontology defined by United Kingdom's government for organizational spending information (Reynolds 2010). Another ontology is the Financial Industry Business Ontology (FIBO) for financial data. There also are other vocabularies that are being defined by WPIG for the different types of commercial transactions, web payments networks, credit cards, product offers and receipts (Sporny 2014a). As yet though, there is no comprehensive vocabulary that manages all the concepts needed during a purchase.

The *Payment Web API layer* is responsible for defining an API that allows the development of different processes (negotiation of a payment instrument, making a payment, receiving a receipt) associated with the use of different payment instruments to make a purchase. This API has to be independent of the payment instrument and the use of a payment instrument will be made through a standard API defined in the Digital Wallet layer. Thus, any web application (merchants websites, social networks), through the web browser or any web agent can use different payment instruments in a uniform and well-established way. Furthermore, this API helps the consumer to manage her different payment instruments, which improves the consumer experience. In the PayFrameworks, the approach is to define special URLs representing payment-based products. In the WPIG, at this stage of its development, the Web Commerce API (Sporny 2014d) only offers a single operation to initiate the payment.

The *Digital Wallet layer* has to offer a generic API, independent of the payment instrument, which provides the functions needed to perform the operations related to a payment using a particular payment instrument. This payment instrument may be a credit card, a crypto-currency, a mobile payment system, a cloud-based payment instrument, or others. This generic API should be defined to be able to support the new e-payment systems that are appearing and the use of new business models that appear. They are often based on the participation of financial entities, but now there are different partnerships among various entities, such as mobile phone carriers, financial institutions, payment processors, and social networks.

With this kind of API, the developer must know how a particular payment instrument works and whether it is based on the use of hardware devices (e.g., smart cards). Another possibility is that the implementation is based on other technologies, such as Web Crypto (Sleevi and Watson 2014). Thus, the use of any payment instrument will occur in the same way, which improves usability. This API has to be defined for and invoked from a web browser or from a native mobile applications. Furthermore, for a payment instrument, there may be different implementations and the consumer will wish to use the most reliable one. This improves security and innovation, and reduces fraud, of course. For this purpose, there are some related APIs, such as those defined in SEMPER (Lacoste et al. 2000a), IOTP (Dulai et al. 2013) and PayFrameworks (Ruiz-Martínez et al. 2012), which is the most generic one. In WPIG, the digital wallet is viewed as the consumer payment agent, but at this moment, it has not been fully defined.

The *Payment Instrument layer* comprises the set of payment instruments available to make a payment. In this layer, the consumer should have different kind of instruments supporting different models, such as credit cards or token-based payments. Currently, there are multiple payment systems that I noted earlier. And new systems will appear and offer Internet-based payment solutions that reduce the risk of fraud, and improve security and anonymity features. Each payment system offers different features, such as availability, security, anonymity, and usability.

The *Negotiation Mechanism layer* is defined so that the consumer as payer and the merchant as payee can agree on the payment instrument to be used in the transaction and, optionally, the price or payment conditions. Through this layer, the consumer can choose the system that works better for the purchase she is going to perform. This process can also be delegated to intelligent agents. The information exchange can be coded in XML or in JSON, which is more lightweight. This coding facilitates the automation of the process based on the consumer preferences, which can also improve the consumer experience (Jaffe and Boyera 2015). In SEMPER and PayFrameworks, there are mechanisms to perform this negotiation. However, in the WPIG, this layer, or the functionality related to this issue, has not been defined so far.

The *Non-Repudiation Mechanisms layer* is defined for transactions for which non-repudiation has to be guaranteed independently, whether the payment instrument provides some repudiation mechanism or not. Currently, there are different non-repudiation protocols. However, there is not a defined framework that can be applied to HTTP messages. For its definition, different standards related to electronic signatures (e-signatures) can be used, such as PKCS#7/CMS, and CAdES/XAdES. Thus, the WPIG is working on the definition of mechanisms that could be the building blocks for the construction of this layer, such as the secure messaging specification (Sporny 2014c) or the Signing HTTP Messages specification (Cavage and Sporny 2015). From these elements, the building of the non-repudiation evidence for the origin, recipient, or delivery will become possible.

The *Transport layer* is the building block over all the exchanges of payment information are made. At this moment, the main transport protocol is HTTP. This protocol defines an error code, 402 Payment Required (Fielding and Reschke 2014), to indicate that the access to a resource requires a payment. However, this code is not being used and its semantic details are not yet defined. In mobile payment systems, the most convenient transport mechanism is NFC, although BLE and RFID are also being used (Ali et al. 2014).

The *Secure Transport layer* is used to guarantee that the exchange of information is made in a secure way. For this purpose, the main mechanism available is the TLS Protocol Version 1.2 (Turner 2014). Another alternative is TCPCrypt (Bittau et al. 2010; Mazieres et al. 2014, 2015), which provides encryption in the Transport layer as an extension of TCP. Currently, its standardization is, being developed in the TCP Increased Security (TPCINC) Working Group.

3. Issues to be addressed

Now that we have presented the state-of-the-art, next we will present the different issues that have not been completely addressed. In the Web *Application layer*, the set of options to embed information in HTML5 are suitable and the main issues to address are related to security and trust. Standard mechanisms are needed to verify the identity of payer or payee at the same time as the minimum information is released, in order to preserve privacy. These mechanisms will help to reduce fraud. Regarding this issue, the WPIG is still working on the Identity Credentials specification (Sporny 2014b). Once a solution is adopted, the issue will be how to associate a level of trust with an entity or an application. In the social environment, the use of adaptive incentive mechanisms has been proposed (Noorian et al. 2014). The W3C Trust and Permissions Working Group is currently working on trust issues. Furthermore, to foster consumer trust, a legal framework is currently being developed (Vandezande 2013).

In the *Payment Information layer*, when the vocabularies that are being defined by the WPIG are finished, there will be a comprehensive set of vocabularies available. The challenge will be the establishment of some mappings and relations between the concepts of the different vocabularies. In this layer, we cannot suppose that there will be only one vocabulary since there are some successful

Please cite this article in press as: Ruiz-Martínez, A. Towards a web payment framework: State-of-the-art and challenges. Electron. Comm. Res. Appl. (2015), http://dx.doi.org/10.1016/j.elerap.2015.08.003

initiatives. An example is GoodRelations (Ashraf et al. 2011). The investments that have already been made will not be easily replaced with a new standard. This layer could be based on Linked Data Platform (LDP) (Speicher et al. 2015), and use the different mechanisms defined to query resources to include payment information.

The *Payment Web API*, along with the *Digital Wallet layer*, is a key layer in order to support multiple kinds of payment transactions (negotiations, payments, refunds). However, at this moment, there are no standardized solutions. The main issue to consider is how to develop this API and which model to follow. This API can be developed with either the web browser, or browser extensions and plugins. It also can be defined as a "reduced API" that is used to invoke native applications in the system. All these solutions are technically viable but the approach that will follow will mainly depend on the position the different stakeholders adopt – mainly the web browser providers.

Although there are some proposals for the Digital Wallet layer, they are focused on the payments and do not consider the rest of processes associated to the purchase, such as receipts. It also is fundamental that, relative to the definition of this API, all of the stakeholders ought to participate. As a result, this issue should be explored by the WPIG to provide a comprehensive solution that can be used seamlessly for the different types of payment instruments and for both web consumer agents and mobile applications.

It is important to point out that the participation of all stakeholders will help to avoid more than one API for this purpose. This would cause the fragmentation of the web payment market and introduce more development costs. This has occurred with the support of hardware-based cryptography with the PKCS#11 and CSP APIs. Furthermore, for the wallet API, it is challenging to define the information that will support the auto-completion of payment information, which will improve the consumer experience. Other issues to address include the definition of mechanisms and policies to protect access to these elements from malicious applications or by web applications that are not trusted.

In the *Payment Instruments layer*, there already are instruments that are being used. Now, the main issues to deal with are the definition of payment systems that support P2P payments and offline payments, the definition of payment tokens, and to take into account the different financial regulations (Vandezande 2013). It is also important that the definition of group-based payment systems support social commerce.

In the *Negotiation Mechanism layer*, once the mechanism for how to represent payment information is defined (using information from the Payment Information layer), the main issues to be addressed will be how the negotiation of payment mechanisms is accomplished. This process needs to take into account consumer's preferences, and the possible negotiation of the purchase conditions, such as the price. Moreover, the exchange of information will need to be made in the most efficient way. Some previous proposals were defined in XML, however, the use of JSON for these information exchanges may improve the efficiency of the process.

In the *Non-Repudiation Mechanism layer*, the main issue to address is how, from the different elements defined for securing HTTP messages, we can generate non-repudiation evidence that will be usable for HTTP messages (Ruiz-Martínez et al. 2012). Apart from generating evidence, it is also important to address how to manage non-repudiation evidence when it must be stored long term (Vigil et al. 2015).

For the *Transport layer*, HTTP Version 2.0 is being developed. It is intended to reduce latency by means of header field compression, allowing multiplexing as well as the prioritization of requests. This will make purchase transactions more efficient. Another challenge is the storage of digital evidence in a secure way that cannot be tampered with once it has been generated. As for NFC, RFID and BLE, the main challenge is to guarantee security when information exchanges occur in their presence. In addition, these technologies have to be loaded in any mobile device.

Within the HTTP protocol, it is be important to define the use of the 402 Payment Required message (Fielding and Reschke 2014). Within this message, payment information can be included and used to launch the digital wallet to start the payment process. This mechanism has been extended in several proposals to support making payments in the Session Initiation Protocol (Hao et al. 2008; Fischl and Tschofenig 2007; Ruiz-Martínez and Marin-Lopez 2012).

The *security mechanisms in the Transport layer* basically are composed of the TLS Protocol. The issues to be addressed have already been considered by the TLS Working Group for the new TLS Version 1.3 (Rescorla 2015, Turner 2014). This version has as its main challenges the improvement of its security by encrypting handshake information as much as possible, privacy via application traffic padding, and efficiency. This new version is intended to allow all of the operations made during a purchase to be performed in a more efficient and secure way.

After our analysis of the issues that need to be addressed, we conclude that there is a long road to develop a web payment framework that will facilitate the use of multiple payment mechanisms in a way that facilitate interoperability and preserve security.

Table 1
Summary of the solutions and challenges for the different layers.

Component	Solutions	Challenges
Web applications	• Microformats, Turtle, RDFa, JSON-LD, LDP • X.509 certificates, OpenID, WebID, Identity Credentials specification • Directory of certifying entities, Web of Trust solutions	• Linking different vocabularies • Development of web Identities • Provide solutions to determine trust of participating entities
Payment information	• PayFrameworks schemas and ontologies • UK Government Payment Ontology • FIBO • WPGI vocabularies	• Comprehensive vocabularies • Mapping between concepts of different ontologies
Payment Web API	WPGI API, OpenBank API	API supporting different processes related to payment
Digital Wallets	PayFrameworks	Comprehensive API supporting different payment transactions
Payment instruments	Credit Cards, Bitcoin, PayPal, EMV, Google Wallet, and others	Support payments of different amounts, security, usability, privacy
Negotiation mechanism	Payment Frameworks	• Definition of negotiation process • Negotiation based on digital wallets and consumer preferences
Non-Repudiation Mechanism	PKCS#7/CMS, CAdES, XAdES, Secure messaging, Signing HTTP messages	• Guarantees of non-repudiation of payment exchange • Secure storage of digital evidence
Transport Layer	HTTP 1.1, NFC, RFID, BLE	• Definition of HTTP 2.0 • Reduction of latency
Security mechanisms for transport	TLS 1.2	• Improvement in security, privacy • Increases in efficiency

Please cite this article in press as: Ruiz-Martínez, A. Towards a web payment framework: State-of-the-art and challenges. Electron. Comm. Res. Appl. (2015), http://dx.doi.org/10.1016/j.elerap.2015.08.003

There are still important issues to cover though, however, there also are initiatives that are trying to solve these issues. Thus, although support for the tasks and issues defined for the different layers is fundamental for the development of a comprehensive web payment framework – irrespective of whether the payment is mobile, the key layers that the stakeholders have to standardize are the web applications, the Payment Web API, payment information, digital wallets, and the security mechanisms for the Transport layer.

The *Digital Wallet layer* is the cornerstone for the support of multiple payments, increased security, usability and innovation. The layers with Non-Repudiation Mechanisms are required to provide a comprehensive architecture but are not a priority now, and could be developed in a second phase. Table 1 sums up the solutions and challenges to be addressed for the different layers.

4. Conclusions

The support of web payments is a continuing challenge that began when the web was developed and attracted the interest of companies. Since then, many technological solutions have been proposed. But often have failed because they or the components they needed were not mature enough. However, currently, there is a base of payment systems that can be use to make transactions on the web. Also available are new technological components (e-signatures, semantic web, security mechanisms, web standards) that are required for developing systems that support web payments. We are nearer to developing the components needed to facilitate the further development and use of web payments. With these components, we also can build a web payment framework. Its development is a cornerstone to facilitate the use of different e-payment instruments, and to support greater interoperability.

In this article, we analyzed the different components that are required in a web payment framework, its functionality, and the different solutions that are available for its development. From this analysis, we can see that the first steps to provide a web payment framework have been taken and several solutions and projects are covering part of the functionality required in this kind of framework. This analysis also shows that there are still some issues to be overcome.

The most important ones are the definition of a digital wallet API and improved security. This article has also noted that there currently are some starting specifications and projects such as the WPIG or the FIBO specification that can help to cover them. The results of these specifications and projects will be a key for the future development of web payments. Furthermore, taking into account that, for each layer, there are different solutions available, it is important to agree upon rationalized framework that facilities the interoperability of the different solutions and that allows the implementation of services and applications that make use of web payments.

Acknowledgements

This work has been partially funded by the "Seneca Foundation" – Spain for Excellent Group in the Region 04552/GERM/06, the Secure Identity across Borders Linked 2.0 (CIP-ICT-PSP-5) – EU, Análisis y gestión dinámica de riesgos con amenazas hetereogéneas (TIN2014-59023-C2-1-R) – Spain, and Interoperable Trust Assurance Infrastructure (FP7-ICT-2011-8) – EU projects.

References

Ali, A.H., Abouhogail, R.A., Tarrad, I.F., Youssef, M.I., 2014. Assessment and comparison of commonly used wireless technologies from mobile payment systems perspective. International Journal of Software Engineering and Its Applications 8 (2), 255–266.

Ashraf, J., Cyganiak, R., Offiain, S., and Hadzic, M. Open e-business ontology usage: investigating community implementation of GoodRelations. In C. Bizer, T. Heath, T. Berners-Lee and M. Hausenblas (eds.), Proceedings of the WWW 2011 Workshop on Linked Data on the web, Hyderabad, India, March 29. Available via CEUR Workshop Proceedings, 813, at ceur-ws.org/Vol-813, 2011.

Barber, S., Boyen, X., Shi, E., Uzun, E., 2012. Bitter to better how to make Bitcoin a better currency. In: Kerymytis, A.D. (Ed.), Proceedings of Financial Cryptography 2012, Lecture Notes in Computer Science. Springer, Heidelberg, Germany, pp. 399–414.

Bittau, A., Hamburg, M., Handley, M., Mazires, D., and Boneh, D. The case for ubiquitous transport-level encryption. In 2010 USENIX Security Symposium, Washington, DC, August 11–13, 2010.

Burdett, D. (ed.). Internet Open Trading Protocol: IOTP. V. 1.0. RFC 2801, April. Available at: <tools.ietf.org/html/rfc2801, 2000>.

Cavage, M., Sporny, M. (eds.). Signing HTTP messages. January 19. Available at: <tools.ietf.org/html/draft-cavage-http-signatures-04>, 2015.

Chung, E.S., Dardailler, D. White paper. Joint Electronic Payment Initiative, April 9. Available at: <www.w3.org/ECommerce/white-paper>, 1997.

de Lange, J., Longoni, A., Screpnic, A. Innopay online payments report 2012: moving beyond the web. Available via: <www.thepaypers.com/reports/innopay-online-payments-report-2012-moving-beyond-the-web/r749111, 2012.

Dulai, T., Jask, S., Tarnay, K. IOTP and payment protocols. In Tarnay, K., Imre, S., Xu, L. (eds.). Research and Development in E-Business through Service-Oriented Solutions. IGI Global, Harrisburg, PA, 20-56, 2013.

Fielding, R., Reschke, J. Hypertext transfer protocol (http/1.1): semantics and content. Available at: <tools.ietf.org/html/rfc7231>, 2014.

Financial Business Ontology. FIBO semantics repository home page. Available at: <www.edmcouncil.org/semanticsrepository/index.html>, 2015.

Fischl, J., Tschofenig, H., 2007. Making SIP make cents. ACM Queue 5 (2), 42–49.

Gannamaneni, A., Ondrus, J., Lyytinen, K., 2015. A post-failure analysis of mobile payment platforms. In: Bui, T., Sprague, R. (Eds.), Proceedings of the 48th Hawaii International Conference on System Sciences, Kauai, HI. IEEE Computer Society Press, Washington, DC, pp. 1159–1168.

Hao, J., Zou, J., Dai, Y., 2008. A real-time payment scheme for SIP service based on hash chain. In: The Proceedings of the IEEE Conference on Business Engineering. IEEE Computer Society Press, Washington, DC, pp. 279–286.

Turban, E., 2014. Electronic commerce: a managerial and social networks perspective. Springer, Germany.

Hiroya, M., Kawatsura, Y. Payment application programmers interface (API) for v1.0 Internet Open Trading Protocol (IOTP). Available at: <tools.ietf.org/html/rfc3867>, 2004.

Huang, X., Dai, X., Liang, W., 2014. Bulapay: a novel web service based third-party payment system for e-commerce. Electronic Commerce Research 14 (4), 611–633.

Jaffe, J., Boyera, S., 2015. Now is the time for web payment standards. The Banker.

Javan, S.L., Bafghi, A.G., 2014. An anonymous mobile payment protocol based on SWPP. Electronic Commerce Research 14 (4), 635–660.

Lacoste, G., Pfitzmann, B., Steiner, M., Waidner, M., 2000a. The payment framework. In: Lacoste, G., Pftzmann, B., Steiner, M., Waidner, M. (Eds.), SEMPER: Secure Electronic Marketplace for Europe. Lecture Notes In Computer Science. Springer, Heidelberg, Germany, pp. 185–211, 1854.

Lacoste, G., Pftzmann, B., Steiner, M., Waidner, M., 2000b. SEMPER: Secure Electronic Marketplace for Europe. Lecture Notes in Computer Science. Springer, Heidelberg, Germany.

Mazieres, D., Boneh, D., Slack, Q., Hamburg, M., Bittau, A., Handley, M., 2014. Cryptographic protection of TCP streams. Internet Engineering Task Force. Available at:< tools.ietf.org/html/draft-bittau-tcp-crypt-04>.

Mazieres, D., Boneh, D., Slack, Q., Hamburg, M., Bittau, A., Handley, M. TCPCrypt. Available at: tcpcrypt.org, 2015.

Michel, T. (ed.). Common markup for micropayment per-fee-links. Working draft, W3C. Available at: www.w3.org/TR/Micropaymenqt-Markup, 1999.

Mozilla. Persona. Available at www.mozilla.org/en-US/persona, 2015.

Nakamoto, S., 2008. Bitcoin: peer-to-peer electronic cash system. Mimeo.

Noorian, Z., Mohkami, M., Liu, Y., Fang, H., Vassileva, J., Zhang, J., 2014. Social Trust: adaptive trust oriented incentive mechanism for social commerce. In: Proceedings of the 2014 IEEE/WIC/ACM International Joint Conferences on Web Intelligence and Intelligent Agent Technologies. IEEE Computer Society, Washington, DC, pp. 250–257, 2.

OpenID Foundation. OpenID. Available at: openid.net, 2015.

Peck, M., 2012. The cryptoanarchists answer to cash. IEEE Spectrum 49 (6), 50–56.

Recordon, D., Reed, D., 2006. A platform for user-centric identity management. In: Proceedings of the Second ACM Workshop on Digital Identity Management. Association for Computing Machinery, New York, NY, pp. 11–16.

Rescorla, E. (ed.). The Transport Layer Security (TLS) Protocol, version 1.3. July 8. Available at: tools.ietf.org/html/draft-ietf-tls-tls13-07, 2015.

Reynolds, D., 2010. Guide to the payments ontology. Technical report. Epimorphics, Bristol, UK.

Rosaci, D., Sarn, G., 2014. Multi-agent technology and ontologies to support personalization in B2C e-commerce. Electronic Commerce Research and Applications 13 (1), 13–23.

Ruiz-Martínez, A., Marin-Lopez, C.I., 2012. A lightweight payment scheme for real-time services based on SIP. EURASIP Journal on Wireless Communications and Networking 1, 161.

Ruiz-Martínez, A., Canovas, O., Gomez-Skarmeta, A.F., 2009. Design and implementation of a generic per-fee-link framework. Internet Research 19 (3), 293–312.

Please cite this article in press as: Ruiz-Martínez, A. Towards a web payment framework: State-of-the-art and challenges. Electron. Comm. Res. Appl. (2015), http://dx.doi.org/10.1016/j.elerap.2015.08.003

Ruiz-Martínez, A., Reverte, S.C., Gmez-Skarmeta, A.F., 2012. Payment frameworks for the purchase of electronic products and services. Computer Standards and Interfaces 34 (1), 80–92.

Sleevi, M., Watson, W. (eds.). Web cryptography API. W3C candidate recommendation 11 December 2014. <www.w3.org/TR/WebCryptoAPI>, 2014.

Speicher, S., Arwe, J., Malhotra, A. (eds.). Linked Data Platform 1.0. Available at: <www.w3.org/TR/ldp/>, 2015.

Sporny, M. (ed.). Commerce vocabulary. Number Draft Community Group Specification 12 October 2014. Available at:< web-payments.org/vocabs/commerce>, 2014a.

Sporny, M. (ed.). Identity credentials 1.0. Draft Community Group Specification 12 September 2014. Available at: Sporny, M. Identity Credentials 1.0. Number Draft Community Group Specification. <web-payments.org/specs/source/identity-credentials>, 2014b.

Sporny, M. (ed.). Secure messaging 1.0. Available at: <web-payments.org/specs/source/secure-messaging>, 2014c.

Sporny, M. (ed.). Web Commerce API 1.0. Available at <web-payments.org/specs/source/web-commerce-api>, 2014d.

Story, H. (ed.). WebID specifications. Available at: <www.w3.org/2005/Incubator/webid/spec/>, 2015.

Turban, E., King, D., Lee, J.K., Liang, T.P., Turban, D.C., 2014. Electronic commerce: a managerial and social networks perspective, 8th edition. Springer, Heidelberg, Germany.

Turner, S., 2014. Transport layer security. IEEE Internet Computing 18 (6), 60–63.

Vandezande, N. Mobile wallets and virtual alternative currencies under the EU legal framework on electronic payments. Research Paper 16, Interdisciplinary Centre for Law and ICT, Catholic University, Leuven, Belgium, 2013.

Vigil, M., Buchmann, J., Cabarcas, D., Weinert, C., Wiesmaier, A., 2015. Integrity, authenticity, non-repudiation, and proof of existence for long-term archiving: a survey. Computers and Security 50, 16–32.

W3C. Reports. Available at: <www.w3.org/community/reports/>, 2015a.

W3C. Web Payments Interest Group. Available at <www.w3.org/Payments/IG>, 2015b.

W3C. WebID, W3C wiki. Available at: <www.w3.org/wiki/WebID>, 2015c.

Wang, Y., Ou, H.Y., Zhang, J.M., 2014. Design and implementation of e-commerce recommendation system based on ontology technology. Advanced Materials Research 978, 244–247.

Please cite this article in press as: Ruiz-Martínez, A. Towards a web payment framework: State-of-the-art and challenges. Electron. Comm. Res. Appl. (2015), http://dx.doi.org/10.1016/j.elerap.2015.08.003