Lyra-Network Position Paper for **W3C Workshop on Web Payments**.

Authors:

Grégory Estrade gregory.estrade@lyra-network.com

Laurent Penou laurent.penou@lyra-network.com

Introduction

> "The web is more a social creation than a technical one. I designed it for a social effect — to help people work together — and not as a technical toy. The ultimate goal of the Web is to support and improve our weblike existence in the world. We clump into families, associations, and companies. We develop trust across the miles and distrust around the corner."

Tim Berners-Lee, "Weaving the Web"

> "I can't in good conscience allow the U.S. government to destroy privacy, internet freedom and basic liberties for people around the world with this massive surveillance machine they're secretly building."

Edward Snowden

Allow us to be a bit provocative: all card-based payment schemes are broken. They basically fail at understanding the need of both identity and anonymity, which are the critical topics that should be addressed at the Web level. Recent issues highlighted in the news about privacy, stories about sensitive data theft and global surveillance, should alert us, as citizens of the world, to how we want the future of information processing to be.

We need to get rid of insufficient data protection schemes, avoid whenever possible the use of trust models relying on a single central authority. The problem is global, and is way beyond the scope of this document, but we still can do something about it for the subject addressed in this workshop.

Our main concern is to find ways to enforce good practices, by participating in the definition of a set of standards that would allow seamless introduction of distributed, networked trust models, as we can find nowadays in cryptocurrencies schemes like Bitcoin or Dogecoin.

As we are also pragmatic, and aware that such changes will take years, we will address existing payment scenarios, and hopefully pave the way for safer traditional schemes.

Digital wallets and distributed models generalization

In this chapter, we will conduct a tour of the most common payment scenarios.

Then we will make some proposals to provide a more uniform payment processing scheme, so that the user experience feels more comfortable, and more trustworthy as well, by limiting disclosure of required information to zones where it becomes necessary.

Based on this work, we will envision some work-arounds for exisitng payment methods, and discuss how Web standards could accelerate the migration.

Card processing

State of the art

Let's review the steps of a Visa/MasterCard e-commerce payment:

- The cardholder provides his card details to the acceptor.
- These details, along with transaction information (amount, currency) are relayed to the issuer through the acceptor for 3-D Secure authentication.
- As a whole, the same information is relayed through the acceptor and the acquirer to the issuer for authorization.

The first step assumes that the cardholder is ready to trust the acceptor at some level.

The second step which is ultimately important, as it is designed to provide a strong authentication of the cardholder, can be bypassed.

Choosing not to use 3-D Secure is often a decision of the acceptor, that has to put in balance the risk of a void sale, compared to the risk of a fradulent transaction. Again, this is a matter of trust level.

Finally, the third step feels rendundant with the second step, information-wise.

The first step is basically *flawed at Web scale*.

Althought it has its justifications for retail transactions processing, on which the e-commerce model is based, this step feels unnecessary and rises many security concerns.

Proposed alternative

Another way to envision this payment could be:

- The acceptor provides some identification information, as well as transaction details to the cardholder.
- The cardholder authenticates himself to the issuer and provides transaction details.
- Authorization is performed at issuer level, and its result is handed back to the acceptor through the acquirer.

The advantages of this scheme, besides the fact that it feels more natural, is that the trust environments are already there, as the cardholder only has to trust the issuer, and the same applies to the acceptor and the acquirer.

Dealing with legacy

We believe that these suggested changes, although they seem important, could be handled more easily with the help of new standards and their implementation at the browser level, while keeping all the 3-D Secure infrastructure and authentication scheme. However, this is beyond the scope of this abstract.

Asymmetry concerns

Running an e-commerce business still requires in most cases the subscription of an acceptor contract and a dedicated account for card processing (with the notable exception of PayPal).

Those make the process of receiving money through most debit and credit cards a complicated one, compared to the ease of subscription and use of these cards.

Digital currencies don't suffer from these issues, and it can be stated that perfect symmetry is not only built-in, but also a requirement for them to work.

Lately, initiatives have come to light, as some markets are emerging, and the focus of established financial institutions on small businesses and individuals makes us envision a unprecedented growth in payments.

E-commerce payments will benefit from this growth, for sure, but the higher increase rate should happen for retail, as the mobile point-of-sale (mPOS) solutions allow the same category of merchants to accept cards.

To sum up, what can be foreseen about Web payments is that in years to come, anyone may be concerned by them not only as a customer, but as a seller as well.

Beyond the wallet scheme

Users of digital currencies are familiar with the idea of digital wallets. These wallets can be used for both selling and purchasing goods and services, and are based on public key cryptography.

Our proposal is to extend the same wallet concept to include both existing payment methods and acceptance means, providing a single local entity to manage both centralized and distributed schemes.

Such a wallet could be shared among different devices: desktops, laptops, smartphones, tablets, etc. but also on servers.

Depending on the use cases of the public keys, they may be signed by a Certificate Authority, or using a "Web of trust" scheme instead.

Use case

Initialization

From the customer (cardholder) side:

- Alice owns an account at Bank A, which also provided her with a credit card.
- Alice provided a public key to Bank A, and after some identity verification, Bank A signed this public key.
- Alice also owns some coupons from Company C, and owns a public key signed by the same entity.

From the merchant (acceptor) side:

- Bob runs an e-commerce store. Bank B provided him with an account, as well as an acceptor contract.
- Bob provided a public key to his bank, and after some identity verification, Bank B signed this public key.
- Bob's store accepts coupons from Company C, therefore one of Bob's public key has been signed by the same entity.

Payment process

Alice shops at Bob's store. On checkout, Bob's server provides a set of public keys related to his acceptance capabilities, as well as list of accepted payment methods, an amount, a currency, and a transaction identifier.

Alice's browser displays the available payment methods providers, namely Company C and Bank A.

Alice chooses Company C. The coupon itself is stored in the wallet, so it could be handed back directly to Bob's store.

Alice then chooses Bank A. Bank A identifies Alice, due to her signed public key. An additional authentication step is then performed by Bank A. Upon success, Alice chooses her credit card.

Bank A performs the authorization based on information provided by Bob's store (this information is digitally signed by Bob's private key).

Bank A relays the authorization result to Bank B, which itself relays the result to Bob's server.

Security and Identity Management

In a previous paragraph, we stated that some public keys may be signed by a Certificate Authority managed by a financial institution, be it an acquirer or an issuer.

These public keys might be used for *identification* purposes, from the financial institution side. However, from the cardholder/acceptor side, these are used for *anonymization* purposes.

Even in distributed payment schemes as provided by digital currencies, these public keys should be used solely for *anonymization* purposes.

However, at some point, there is a need for strong identification, in order to address the following subjects:

- Distributed identity management.
- Secure transportation of the aforementioned private keys across devices.
- Revocation of these keys.

We feel that this specific part of the whole architecture is probably the most important and difficult one.

However, some standards are already there, to help build up its foundations, namely the WebID protocol and FOAF specification.

We also believe that the specifications issued by the JOSE working group, especially those related to key protection, should be taken into account.

We would like to address the issue with local storage of private keys, as it is a "single point of failure", and envision a distributed approach on that subject.

References

Distributed private key management: http://individual.utoronto.ca/aldar/paper/2012/dpkg.pdf

WebCryptoAPI: http://www.w3.org/TR/WebCryptoAPI/

Web of trust: http://en.wikipedia.org/wiki/Web_of_trust

Protecting JSON Web Key (JWK) Objects: http://tools.ietf.org/html/draft-miller-jose-jwe-protected-jwk-02

WebID provider using Node.js: http://magnetik.github.io/node-webid-report/

FOAF Vocabulary Specification 0.99: http://xmlns.com/foaf/spec/

WebID 1.0: http://www.w3.org/2005/Incubator/webid/spec/