CORE®

PAY BY BROWSER – PAYMENT REQUEST API AS A UNIVERSAL PAYMENT STANDARD?

Johannes Rauch

November 2017
COREtechmonitor | Blogpost

Key Facts

- Payment Request API defined as a W3C standard for securely storing user and payment data directly in the browser
- Increased convenience due to a reduction in the data that buyers need to enter at the checkout, and an improved conversion rate for online retailers
- Currently only supports credit card payments without a dynamic security factor – little benefit due to updated SEPA regulations as of January 2018
- In the future, payment initiation directly within the account will be possible with Payment Request API thanks to PSD2 in conjunction with FIDO standards – challenging payment services such as Klarna, Amazon Pay, and PayPal
- Local storage of payment data in the browser DOM ("super cookies") is open to criticism from a data protection/data security standpoint

Report

Development Trends in Online Retail

Internet retail is growing rapidly. E-commerce revenues in the German B2C segment have increased almost fivefold in the past 10 years, which is why online payments are becoming even more important. The success of payment services such as PayPal is largely due to their user-friendliness. Customers are no longer required to enter complicated IBANs, PANs, TANs, BICs, or online banking log-in details, but merely have to remember their email address/username and a password of their choice. A stored biometric identifier can be used instead of a password on mobile devices with a corresponding security element, although providers such as PayPal and Amazon Pay charge a very high price for this level of simplicity. Whereas an incoming payment by bank transfer usually only costs retailers a few cents and payments made on the customer's credit card generally no more than 90 basis points since the enactment of the MIF Regulation, a PayPal transaction costs retailers (especially smaller ones) up to 1.9% of revenue and fixed costs of at least 35 cents. However, retailers often put up with these costs in order to boost their conversion rate and thus stop as many eager-to-buy customers as possible from abandoning the process at the checkout.

Even though payment with email address and password constitutes a significant simplification for customers, any checkout is a challenge for customers on their first visit to an online shop.

- Retailers' checkout pages exhibit little standardization
- The individual elements are arranged differently on each retailer's page
- The available payment methods (and their associated conditions) have to be checked each time and compared with the user's own options
- Shipment and billing addresses have to be entered separately in different formats at the end of the process

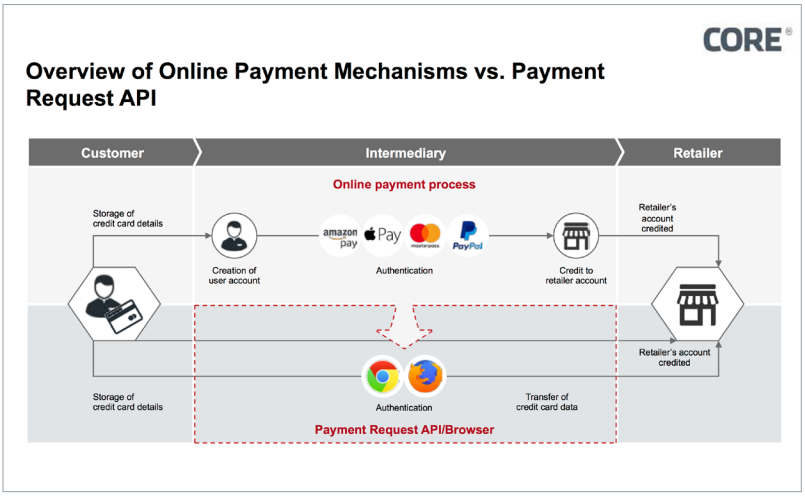

Figure 1: Comparison of online payment services and the browser-based Payment Request API

Generally speaking, the checkout conversion rate on mobile devices is about three times lower than that of desktop devices. In particular, the need to enter additional data – as is necessary on shops visited for the first time – results in many purchases being aborted. Shops address these difficulties with their own mobile-optimized applications, although these find very limited acceptance among customers. Overall, customers are installing even-fewer apps on their mobile devices. Despite payment processes that are actually easier, customers therefore tend to restrict their purchasing to particular online shops and platforms, thus tolerating a reduction in choice and potentially less value for money. By virtue of the standardized checkout, this is not a phenomenon witnessed in bricks-and-mortar retail. There is therefore a need for technological solutions that are system-independent and that work within preinstalled applications such as browsers or messaging services.

Payment Request API

Payment Request API, a recently published W3C standard, makes it possible to store user and payment data (such as addresses and credit card details) directly in the Document Object Model (DOM) of the browser and offers a consistent checkout function. This allows users to transfer the data stored within the browser to the online merchant concerned in a secure and standardized fashion (see figure 1).

As a result, Payment Request API addresses the problems of online retailers and their customers outlined above in two key ways:

Reduced Transaction Costs

Rather than the necessary account or credit card details being stored with an external payment service, this data is transmitted straight from the customer's browser and can be used directly by the retailer without the need for a payment intermediary or, alternatively, can be forwarded to the retailer's payment service provider (PSP). The retailer only incurs the usual transaction fees – and no additional costs for the online payment process.

Universal Integration

Whatever online shop the customer visits, the checkout is designed by the browser and

always appears identical. The address details and payment methods only have to be stored once and can then be used in different shops without the need to register again. Non-stored payment methods are simply not displayed in the checkout. Instead of the user having to download additional apps, the application functions within the preinstalled browser for all online shops that have integrated API.

Limitations

Payment Request API has yet to gain any real foothold. While the technology is already available in the latest version of the browsers Chrome (version 61 and above) and Edge (version 15 and above), it is hidden away in an auto-complete submenu. So far, only a handful of retailers have incorporated the extension into their checkouts (although big names such as Airbnb are among those who have). Furthermore, the initiative is driven chiefly by American companies, which is reflected in the system only being available for “basic credit cards”.

Payments made using the credit card number (PAN), the card expiration date, and the security code (CVV/CVC) will, due to the lack of dynamic security components, no longer be permissible within SEPA once the revised Payment Services Directive (PSD2) comes into force on January 18, 2018.

While the Payment Request API does also support the storage of other data like payment apps access data, or even bank account details to facilitate direct debits, a standard that represents the payment habits of German users has not yet been defined within Payment Request API. Therefore, it is expected that it will only gain limited ground in German-speaking countries.

Potential

Although a breakthrough is not currently expected for Payment Request API, the solution nonetheless harbors enormous potential.

If the final version of the Regulatory Technical Standards (RTS) of PSD2 (published on November 27, 2017) is ratified by the European Parliament in the near future and thus becomes mandatory in spring 2019, it could also be possible to use Payment Request API to initiate payments straight from the customer’s account – a scenario that should strike fear into the hearts of online payment service providers such as PayPal or paydirekt. Especially when it will be possible to push real-time bank transfers (SCTinst, Instant Payments) – which his already possible for HypoVereinsbank customers since November 27, 2017 – using the Payment Request API becomes even more attractive and may replace external payment service, PSPs or acquirers in some cases. This, however, requires much more than just storing and reusing account access information within the browser.

It remains to be seen how account access will work in detail following the acceptance of the Access to Account (xs2a) guidelines within PSD2. However, the required dynamic security factor could be resolved, for example, by integrating the FIDO standard, which is becoming increasingly widespread within the finance industry. FIDO is a protocol that enables authentication on the basis of a security element and using an asymmetrical pair of keys. Therefore, the second factor is not restricted to a specific process such as M-TAN, a defined app, or even a TAN list, but can be used with FIDO-Alliance certi-

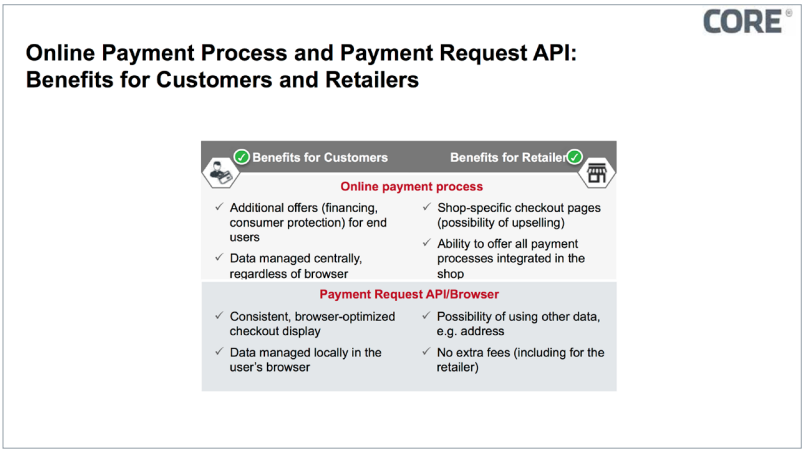

Figure 2: Comparison of both methods for customers and retailers

fied components on all devices. Bank of America and Barclays, for example, employ this standard for their online banking log-in mechanism. German banks should also be alert in this area and seek active communication with W3C and the FIDO Alliance. Even if open standards like these would not result in online banking portals being used more frequently, they do make it possible to weaken the role of intermediaries such as Klarna (Sofortüberweisung) and support the direct access of users to their own bank account interfaces.

Criticism

The published standard offers considerable cause for concern in terms of data protection and security, as well as in relation to the especially acute need to safeguard financial data. The potential clustering of information in the browser opens up several options that, on current interpretation, cannot be utilized without the consent of the user. Direct integration within the browser leaves essential, security-related elements to the mercy of market developments, e.g. the necessary differentiation by use cases and LoAs and the embedding of safeguarding mechanisms. Attacks on the data stored in the browser and the software vulnerabilities exploited for this purpose are part of the standard repertoire of cyber criminals. The ability of browser providers to respond quickly with software patches does not offer protection against vulnerabilities for users who have not installed browser updates or who have not taken sufficient steps to protect their devices against unauthorized access. Therefore, it is questionable whether user data is any safer when stored locally on the user's device, as opposed to an online service. Furthermore, it is open to debate as to whether the process of storing and using log-in data breaches the current applicable Terms and Conditions of European financial institutions. Relevant judgments relating to real-time transfers are already well documented.

Last but not least, a key factor in the success or failure of initiatives such as Payment Request API and the FIDO Alliance is the involvement of financial institutions, which should identify and harness the opportunities offered by open standards.

For more information and analysis on the technology-driven transformation of digital business models, payment processes, identification and data management, please consult our white paper entitled „The Empire Strikes Back“.

Sources

HDE (forecast); GfK; Handel Digital - Online-Monitor 2017, page 3

https://www.w3.org/TR/payment-request/

http://www.ibi.de/aktuelle-meldungen/1520-haendlerkosten-von-kreditkartenzahlungen-im-online-handel-gehen-um-bis-zu-60-prozent-zurueck.html

https://de.statista.com/infografik/2792/konversionsrate-und-den-durchschnittlichen-bestellwert-bei-online-shoppern/

https://www.recode.net/2016/6/8/11883518/app-boom-over-snapchat-uber

http://www.handelsblatt.com/finanzen/steuern-recht/recht/urteil-gegen-sofortueberweisung-ein-unzumutbares-bezahlsystem/12053726.html

Author

Johannes Rauch is a Transformation Manager at CORE. As an expert in strategic sourcing, he develops apposite strategies over the entire duration of complex IT transformation projects of banks and insurance companies. At CORE, Johannes also supports clients in the entire conception and implementation of extensive transformation projects.

Mail: johannes.rauch@core.se

COREinstitute
Am Sandwerder 21-23
14109 Berlin | Germany
https://institute.core.se
Phone: +49 30 26344 020
office@coreinstitute.org

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://www.core.se
Phone: +49 30 26344 020
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://www.core.se
Phone: +49 30 26344 020
office@coretransform.de

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://www.core.se
Phone: +41 442 610 143
office@coretransform.ch

COREtransform Ltd.
One Canada Square
London E14 5DY | Great Britain
https://www.core.se
Phone: +44 203 319 0356
office@coretransform.co.uk

COREtransform MEA LLC
DIFC – 105, Currency House, Tower 1
Dubai P.O. Box 506656 I UAE
https://www.core.se
Phone: +971 4 3230633
office@coretransform.ae