January 2024

# Secure Payment Authentication That Provides Strong Customer Authentication

Annamalai Muthalagappan

Bill Corsello

Christopher Lin

Cong Li

Derek Shu

*See next page for additional authors*

Inventor(s)
Annamalai Muthalagappan, Bill Corsello, Christopher Lin, Cong Li, Derek Shu, Florin Modrea, Habib Sorathia, Hemen Chhatbar, Heng Liu, Jan Czapracki, Jingmin Xie, Karen Langsam Kapila, Karl Cai, Kenneth Tu, Layla Hadinger, Lei Duan, Lucas Petraglia, Lucian Driscu, Matt Mulkeen, Mark Lawley, Meng Deng, Monica Gautier, Raj Govindaraju, Rie Yamaoka, Rocky Meza, Sharon (Xiaoqin) Huang, Shuojing Wang, Stephen John Ratcliffe, Xiaoming Hu, Yinua Wu, Yitian Li, and Yong Ni

# Secure Payment Authentication That Provides Strong Customer Authentication

ABSTRACT

Multi-factor verification steps currently used for authenticating online purchases, e.g., one-time codes sent to a phone, can prove to be a hurdle for some customers. This disclosure describes a strong customer authentication technique, referred to as secure payment authentication (SPA), that enables users to authenticate online transactions using device-bound tokens. Authentication is driven by payment service providers, and a simple device unlock can confirm a transaction. Strong customer authentication is made possible with just a single (or even zero) click. Cross-device authentication can be enabled, such that a customer can authenticate themselves on a payment app on a mobile device while performing transactions on a second device such as a laptop, etc.

KEYWORDS

- Secure payment authentication (SPA)
- Strong customer authentication (SCA)
- Multi-factor authentication (MFA)
- Two-factor authentication (2FA)
- 3D secure authentication (3DS)
- Payment services directive (PSD)
- Device-bound token
- Payment service provider (PSP)
- Dynamic primary account number (DPAN)
- Funding primary account number (FPAN)
- Cryptogram
- Identity and verification (ID&V)
- Payment network
- Card network
- Card-issuing bank

## BACKGROUND

To protect against fraud and to comply with financial regulations such as the payment services directive (PSD), payment authentication flows on the internet (e.g., 3D Secure or

3DSecure 2) make customers go through an additional verification step while making online payments. For example, the customer can be directed to an authentication page on their bank app or required to enter a code sent to their phone via short messaging service (SMS).

However, such additional verification steps can prove to be a hurdle for some customers. For example, in the case of an SMS code sent to the customer's phone, the phone may be temporarily unavailable, the customer may not know where the phone is, the customer may have multiple phones, or SMS can be unreliable. Further, it is possible that SMS can be phished. In the case of customer authentication via a bank app, the bank app is usually triggered from an embedded HTML iframe, which can pose difficulties for banks to serve and can be unreliable.

3D Secure2 (3DS2), a standard currently used to achieve strong customer authentication (SCA) imposes certain limitations on users, merchants, and banks, such as:

- User experiences can be lengthy. The 3DS2 transaction flow is repeated for each payment, which can lead to user frustration.
- Merchants can experience conversion drop-offs due to the additional steps.
- Banks can experience difficulty in collecting strong customer authentication (SCA) factors due to the lack of information that they can access about the payment request, their own technical limitations, and high market fragmentation.

A separate authentication specification - WebAuthn - also has several limitations, such as:

- WebAuthn lacks payment styling, e.g., it is a login-focused API.
- WebAuthn has no payment information in the output cryptogram, leading to difficulties in regulation.

- The challenging bank has to be HTML-iframed back to the merchant page, such that the difficulties with HTML iframe also exist with WebAuthn.
- Inline registration during a challenge flow is not allowed.

Secure Payment Confirmation (SPC), which is a web application programming interface (API) that builds on WebAuthn, is designed to support streamlined authentication during a payment transaction. SPC can scale authentication across merchants, can be used within a wide range of authentication protocols, and can produce cryptographic evidence that the user has confirmed transaction details. However, SPC suffers from privacy limitations for both developers and users, and, for various reasons, its adoption has proven to be slow.

Due to the multiple, and sometimes unreliable, steps currently used for strong customer authentication, payment networks are less competitive for online payments vis-a-vis digital wallets, which are able to achieve customer authentication more seamlessly.

## DESCRIPTION

This disclosure describes a strong customer authentication technique, referred to as secure payment authentication (SPA), that enables users to authenticate online transactions using device-bound tokens (DPANs) or device-bound e-commerce tokens. Authentication is driven by payment service providers (PSPs). A simple phone unlock can confirm the transaction. Cross-device authentication can be enabled, such that a customer can authenticate themselves on a payment app on a mobile device while performing transactions on a second device such as a laptop, desktop, tablet, etc. Two authentication pathways are defined - authentication for users who have an existing device token and authentication for users who do not have an existing device token. The authentication pathways are described in greater detail below.

*Authentication for users who have an existing device token*

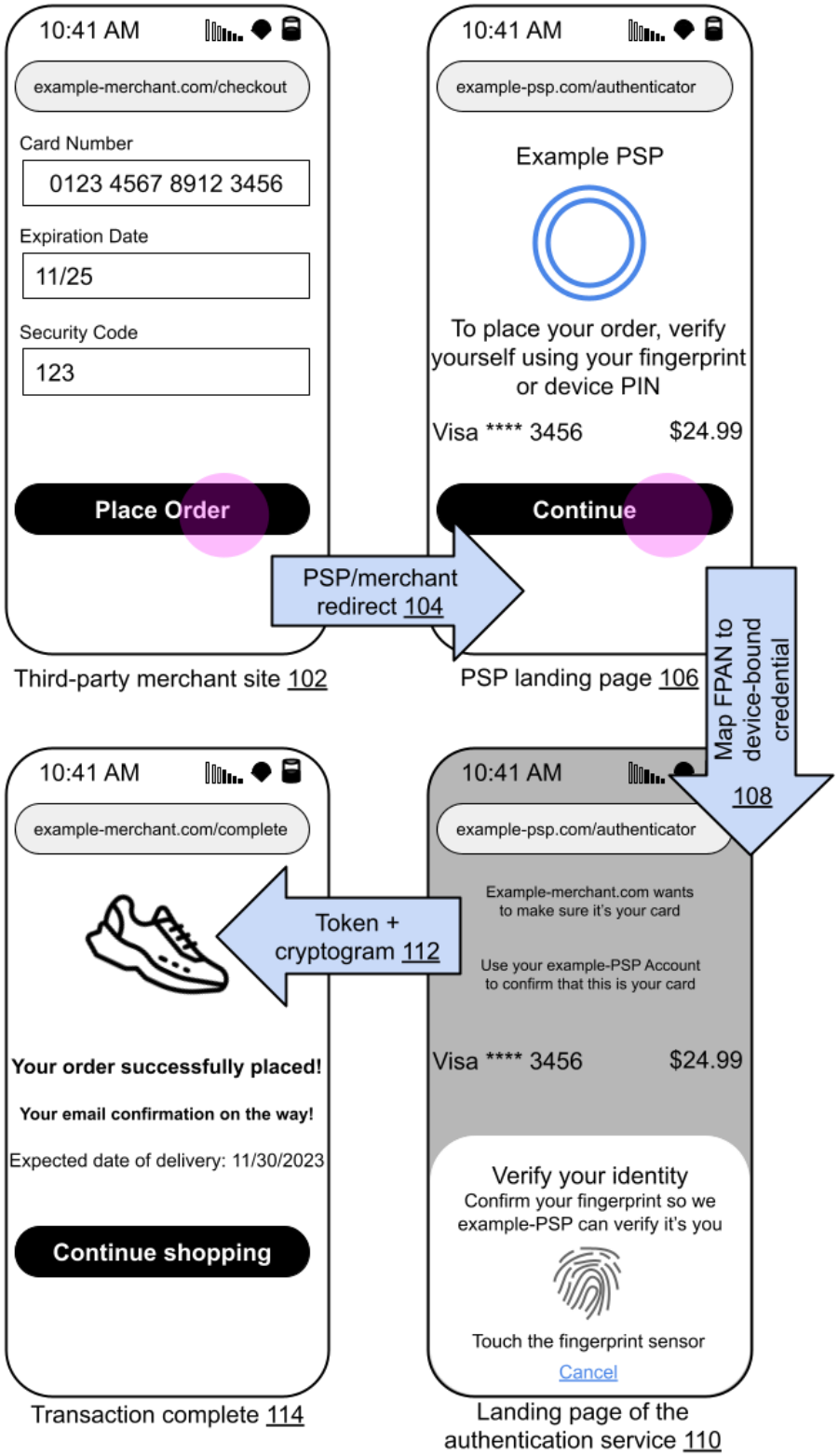


**Fig. 1: Authentication for users who have an existing device token**

Fig. 1 illustrates authentication for users who have an existing device token. The user enters their payment credentials (e.g., funding primary account number, or FPAN) on a third-party merchant website (102) and clicks on a checkout/place-order button. The merchant requests payment processing via their payment service provider (PSP).

The PSP determines that strong customer authentication (SCA) is required and triggers a redirect link (URL) for the merchant to render (104). The user is redirected to the landing page of the PSP (106). The PSP sends relevant payment details to an authentication service via a backend application programming interface (API). The user's FPAN is mapped to device-bound credentials (108).

The user is redirected to the landing page of the authentication service (110). The user is provided with transaction details such as FPAN and the amount being billed and with a biometric or PIN prompt to enable the user to authenticate herself. The user authenticates herself using the biometric or PIN prompt. The biometric or PIN prompt enables the use of device-bound payment credentials for the purpose of authentication. The authentication service maps the payment credentials to a device-bound token, also referred to as a dynamic primary account number (DPAN). The device is unlocked based on the entered biometric signature or PIN.

Upon successful unlocking, a cryptogram is generated for the transaction with the amount and the merchant name. The encrypted token and the cryptogram are passed back to the PSP for further processing (112). The payment is completed, and the user is redirected to the order confirmation page on the merchant site (114).

*Authentication for users who do not have an existing device token*

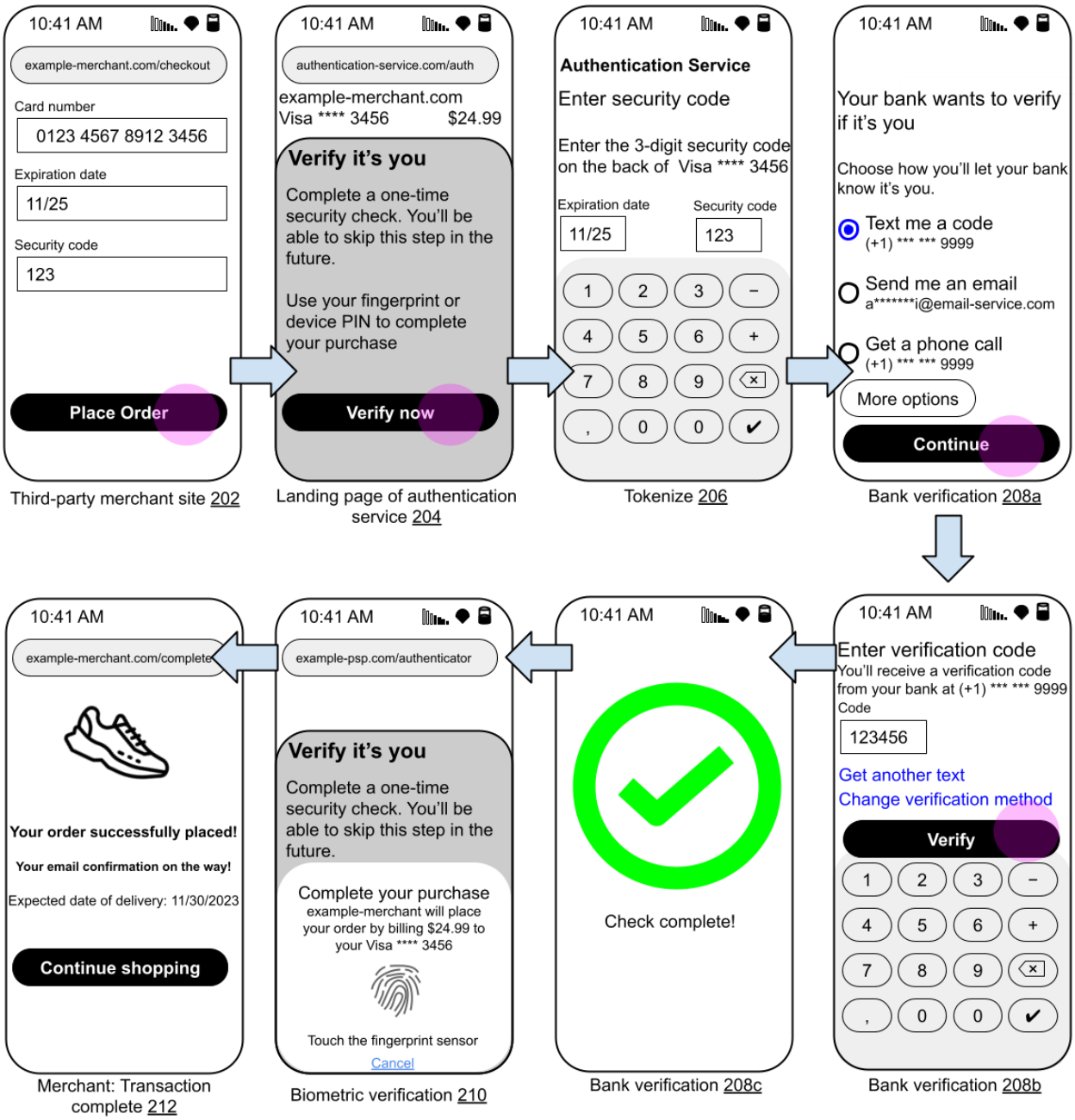


**Fig. 2: Authentication for users who do not have an existing device token**

For users who don't have an existing device token, the initial few steps are similar to the steps for users who do have an existing device token: the user enters their payment credentials

(e.g., funding primary account number, or FPAN) on a third-party merchant website and clicks on a checkout/place-order button. The merchant requests payment processing via their payment service provider (PSP). The PSP determines that strong customer authentication (SCA) is required and triggers a redirect link (URL) for the merchant to render.

The user is redirected to the landing page of the PSP. The PSP sends relevant payment details to an authentication service via a backend application programming interface (API). The user is redirected to the landing page of the authentication service. The user is provided with transaction details such as FPAN and the amount being billed and the terms of service. The user is provided with a verify button which she clicks on. At this point, since the device-bound token does not exist on the user's device, device tokenization is performed, as illustrated in Fig. 2.

Fig. 2 illustrates authentication for users who do not have an existing device token. After entering their payment credentials on a third-party merchant website (202) and placing their order, the user is prompted to sign in to an authentication service (204) if they are not already signed in. Device tokenization is initiated (206) by presenting the user with identity and verification (ID&V) options provided by an issuing bank (208a). Examples of ID&V options include the texting of a code to the user's phone or the user's email address, providing the user with a code over a phone call, etc.

The user chooses and completes the ID&V challenge (208b-c). The user is prompted to unlock their device using a biometric verification, a device PIN, or by a fast identity online (FIDO)-unlock technique (210). Enrollment, e.g., device tokenization, is completed.

Upon successful device unlocking, a cryptogram is generated for the transaction with the amount and the merchant's name. The encrypted token and the cryptogram are passed back to the

PSP for further processing. The payment is completed, and the user is redirected to the order confirmation page on the merchant site (212).

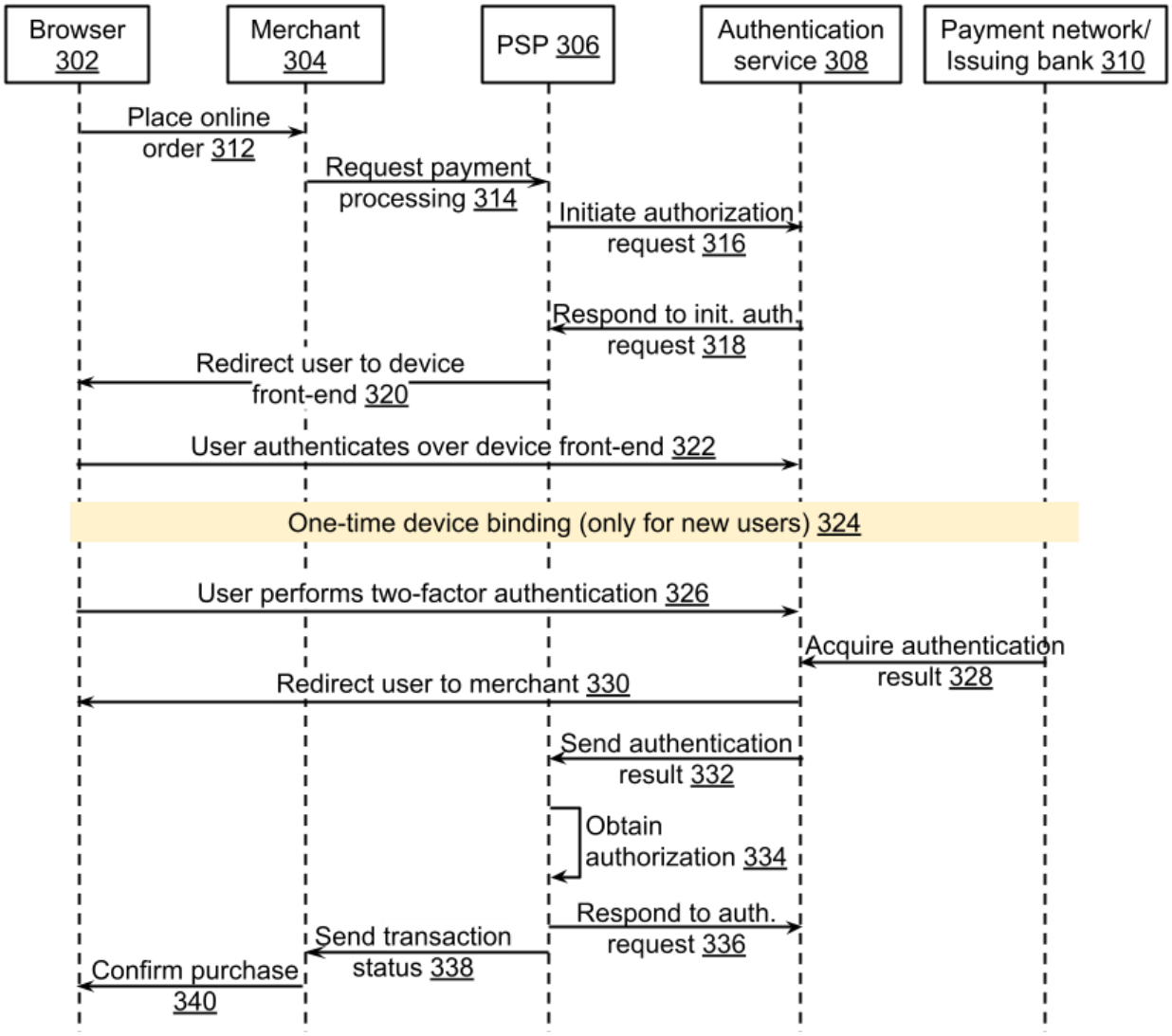


**Fig. 3: Communication flow between the user (browser), the merchant, the PSP, the authentication service, and the payment network**

Fig. 3 illustrates the flow of communications between the user (performing an online shopping transaction using, e.g., a browser (302), the third-party merchant (304), the PSP (306), the authentication service (308), and the payment network (or card-issuing bank, 310).

The user places an online order (312) with the merchant. The merchant invokes the PSP for payment processing (314). The PSP initiates an authorization request (316) with the

authentication service for obtaining SCA via the payment network or the card-issuing bank, and receives a response (318) from the authentication service. The user is redirected to the device front-end (320) for the purposes of biometric or PIN-based authentication. The user authenticates over the device front-end (322).

If the user does not have an existing device-bound token, the user performs two-factor authentication (326) to obtain a device-bound token (324). The authentication service acquires the authentication result from the payment network or card-issuing bank (328), and returns the result to the PSP (332). The user is redirected to the site of the merchant (330). The PSP obtains authorization for the payment (334) by providing the authentication result to the payment network and responds to the authentication service (336). The PSP sends the transaction status to the merchant (338), who confirms the purchase to the user (340).

The described techniques provide an enhanced user experience for online authentication, enabling frictionless online shopping and high conversion rates. The techniques make use of device-bound tokens (DPANs) and device-bound e-commerce tokens, which have high market coverage. Users with existing device-bound tokens can get authenticated by just unlocking their device, e.g., with just a single (or even zero) click. Users who do not have device-bound tokens need enroll only once for their future transactions to be authenticated with zero or one click.

Further to the descriptions above, a user may be provided with controls allowing the user to make an election as to both if and when systems, programs, or features described herein may enable the collection of user information (e.g., information about a user’s payment instruments, biometric or other authentication information, shopping, a user’s preferences, or a user’s current location), and if the user is sent content or communications from a server. In addition, certain data may be treated in one or more ways before it is stored or used so that personally identifiable

information is removed. For example, a user's identity may be treated so that no personally identifiable information can be determined for the user, or a user's geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level) so that a particular location of a user cannot be determined. Thus, the user may have control over what information is collected about the user, how that information is used, and what information is provided to the user.

## CONCLUSION

This disclosure describes a strong customer authentication technique, referred to as secure payment authentication (SPA), that enables users to authenticate online transactions using device-bound tokens. Authentication is driven by payment service providers, and a simple device unlock can confirm a transaction. Strong customer authentication is made possible with just a single (or even zero) click. Cross-device authentication can be enabled, such that a customer can authenticate themselves on a payment app on a mobile device while performing transactions on a second device such as a laptop, etc.

## REFERENCES

1. "CMSPI, smarter payments intelligence" available online at https://cmspi.com/eur/en/ accessed Nov. 25, 2023.
2. "WebAuthn, a better alternative for securing our sensitive information online" available online at https://webauthn.guide/#about-webauthn accessed Nov. 25, 2023.
3. "W3C/secure-payment-confirmation" available online at https://github.com/w3c/secure-payment-confirmation accessed Nov. 25, 2023.