Secure Payment Confirmation

December 2024

Editors:

Marc Findon, Nok Nok Labs

Jonathan Grossar, Mastercard

Frank-Michael Kamm, Giesecke+Devrient

Henna Kapur, Visa

Sue Koomen, American Express

Gregoire Leleux, Worldline

Alain Martin, Thales

Stian Svedenborg, BankID BankAxept

Contents

Figures

1. Introduction

Global e-commerce is booming and is expected to reach more than $6T by the end of 2024[1]. Having the ability to sell products online has provided great opportunities for merchants to sell goods and services beyond their local market; however, it comes with increased fraud. In fact, it is estimated that in 2023, global ecommerce fraud was roughly to reach $48B[1], with the US accounting for 42% of that and the EU with about 26%.

1.1 Current Challenges in Remote Commerce

There are many types of ecommerce fraud, but the most prevalent type is transaction fraud. Transaction fraud occurs when a transaction is made on a merchant site with a stolen card and/or stolen credentials. Stolen credentials are readily available on the dark web to those who know how to access and use them.

To address those concerns, measures have been introduced to increase the overall security of remote commerce transactions, including tokenization of payment credentials and cardholder authentication. In some countries, regulations are mandating the adoption of either or both measures, such as in India or in Europe (second Payment Services Directive PSD2). These regulations are meant to ensure secure remote transactions; however, they add complexity to the checkout flow, as they may require a switch between the merchant and another interface, such as a bank's interface.

Unfortunately, additional authentication may add friction which can result in cart abandonment. The main reasons for cart abandonment include a distrust in the merchant website or a complicated check out flow. Customers prefer a simple payment process that doesn't add friction such as that caused by payment failure, the need to respond to a one-time password (OTP) on a separate device, or the need to login into a banking application.

1.2 How FIDO can help

The use of biometric authentication enabled through the Fast Identity Online (FIDO) Alliance standards is an opportunity to deliver a better user experience during the authentication process and hence reduce the risk of transaction abandonment.

FIDO has established standards that enable phishing-resistant authentication mechanisms and can be accessed from native applications and from the most popular browsers – thereby enabling a secure and consistent experience across the channels used by consumers. FIDO refers to 'passkeys' as the FIDO credentials based on FIDO standards, used by consumers for passwordless authentication.

The World Wide Web Consortium (W3C) has developed Secure Payment Confirmation (SPC). SPC is a web API designed to enhance the consumer experience when authenticating to a payment transaction using FIDO authentication, and to simplify compliance with local regulations (such as PSD2 and dynamic linking in Europe).

1.3 Scope

This whitepaper intends to:

- Define Secure Payment Confirmation (SPC) and the benefits that it brings when FIDO is used to authenticate payment transactions

[1] https://www.forbes.com/advisor/business/ecommerce-statistics/#:~:text=The%20global%20e%2Dcommerce%20market,show%20companies%20are%20taking%20advantage.

- List the current SPC payment use cases that can deliver those benefits and illustrate consumer journeys
- Provide a status on SPC support and the list of enhancements that could be added to the web standard to further improve security and user experience

2. Secure Payment Confirmation (SPC) Benefits

Secure Payment Confirmation (SPC) is an extension to the WebAuthn standard, and aims to deliver the following benefits:

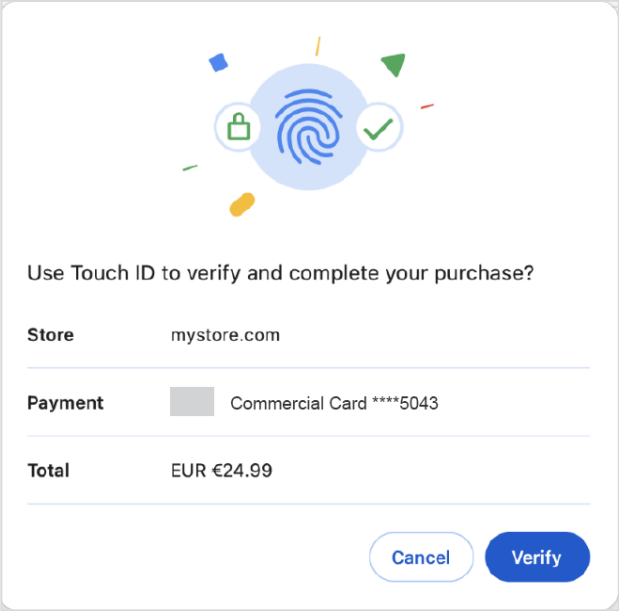
- A browser native user experience that is consistent across all merchants and banks
- Cryptographic evidence of authentication (FIDO assertion) including transaction details signed by a FIDO authenticator
- Cross origin authentication - For example, even if passkeys are created with the bank as the Relying Party, merchants can invoke cardholder authentication with passkeys within their environment, using input parameters received from the bank, so there is no need to redirect the consumer to the bank to authenticate with passkeys.

2.1 Browser Native User Experience

SPC introduces a standardized payment context screen showing details such as a merchant identifier, the card logo, the last 4 digits of the card number, and the transaction amount. The consumer is invited to explicitly agree to the transaction information displayed and then authenticate. Therefore, SPC can be experienced as a mechanism to collect consent from the consumer about the transaction details.

As in standard WebAuthn, the payment context screen is controlled by the user's browser which renders common JavaScript presentation attacks ineffective. The screen provides increased security, as it ensures that malicious web content cannot alter or obscure the presentation of the transaction details to the user - the browser display always renders on-top of the web content from the triggering website. Figure 1 depicts an example of the SPC experience in chrome.

Figure 1 Example of SPC experience in chrome



2.2 Generation of FIDO Assertion

With SPC, the transaction-related information displayed to the consumer, such as the merchant identifier and transaction amount, is sent securely to the FIDO authenticator and is signed by the same authenticator (transaction data signing).

The FIDO assertion generated by the authenticator reinforces compliance with some regulations as it does with the dynamic linking requirement under PSD2 in Europe, because the merchant identifier and transaction amount will be signed by the authenticator itself. When combined with the browser native user experience described in section 2.1, the relying party can be confident that the user was shown and agreed to the transaction details.

2.3 Cross Origin Authentication

When using FIDO without SPC, a consumer that creates a passkey with a relying party will always need to be in the relying party's domain to authenticate with that passkey. In the remote commerce payment use case, this means that the consumer typically needs to leave the merchant domain and be redirected to the bank's domain for authentication.

With SPC, any entity authorized by the relying party can initiate user authentication with the passkey that was created for that relying party. For example, a merchant may be authorized by a bank to authenticate the cardholder with the bank's passkey.

Note that the mechanism for the relying party to authorize an entity to invoke SPC may vary. For example, a bank may share FIDO credentials with the merchant during an EMV 3DS interaction or through another integration with a payment scheme. The merchant will then be able to use SPC to initiate the payment confirmation and authentication process with a passkey, even if that passkey was created with the bank. Ultimately, the bank maintains the responsibility to validate the authentication.

2.4 Interoperability With Other Standards

SPC can be used in combination with other industry standards such as EMV 3-D Secure and Secure Remote Commerce (SRC), both of which are EMVCo global and interoperable standards.

3. SPC Use Cases

SPC can be used to streamline payments in a variety of remote commerce checkout scenarios such as guest checkout or a checkout using a payment instrument stored on file with a merchant.

In each of those payment scenarios, the relying party may be the issuer of the payment instrument (the bank), or a payment network on behalf of the bank.

The flows provided in this Chapter are for illustrative purposes and may be subject to compliance with applicable laws and regulations.

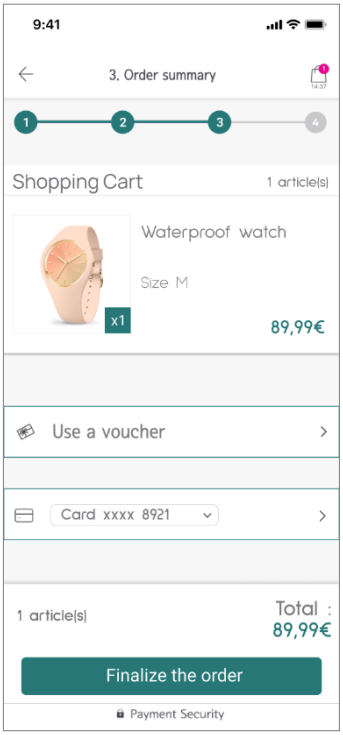
3.1 SPC With Bank as Relying Party

The creation of a passkey can be initiated outside of or during the checkout process:

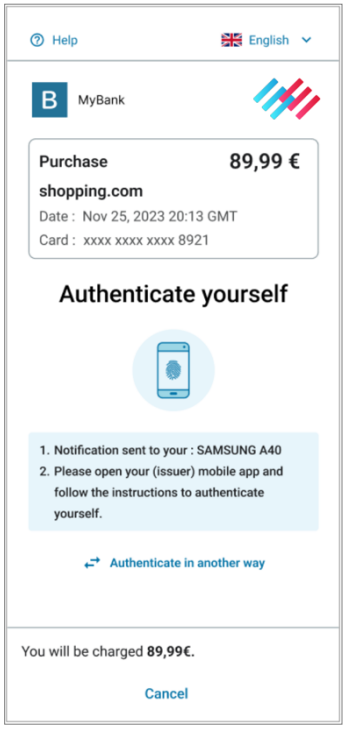
- Within the banking interface:
  - For example, when the consumer is within the banking application and registers a passkey with their bank, in which case the passkey will be associated to one or multiple payment cards and to the consumer device
- Within the merchant interface:
  - For example, when the consumer is authenticated by the bank during an EMV 3DS flow and is prompted to create a passkey with the bank to speed up future checkouts – in which case the passkey will be associated to the payment card used for the transaction (and to additional payment cards depending on the bank's implementation), as well as to the device used by the consumer

Figure 2 depicts the sequence (seven steps) of a passkey creation during a merchant checkout, where the merchant uses EMV 3DS and the consumer is authenticated by their bank:

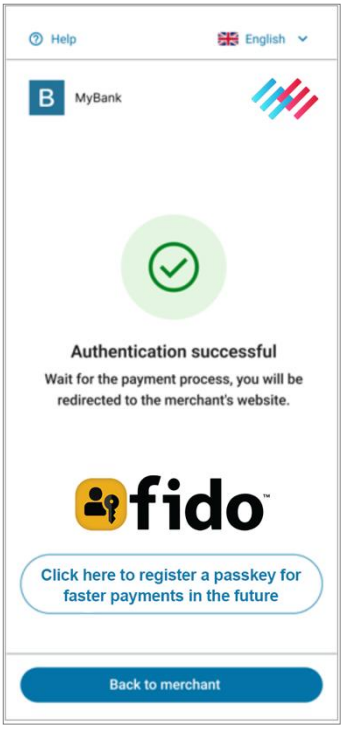
Figure 2: Passkey creation during checkout



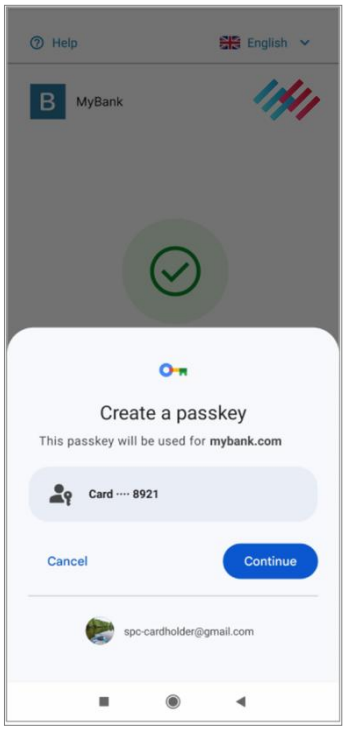
Checkout at the merchant's store



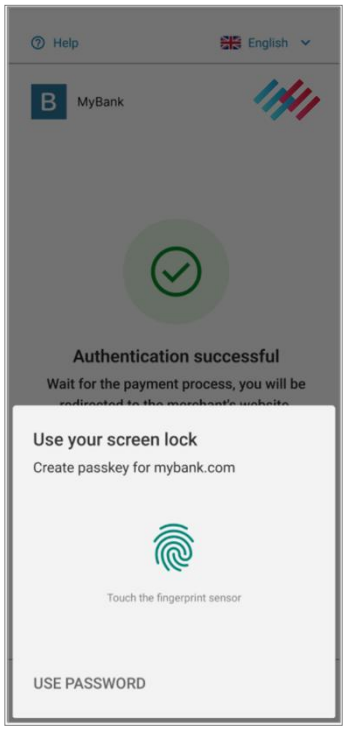
Bank's authentication page requests cardholder to authenticate



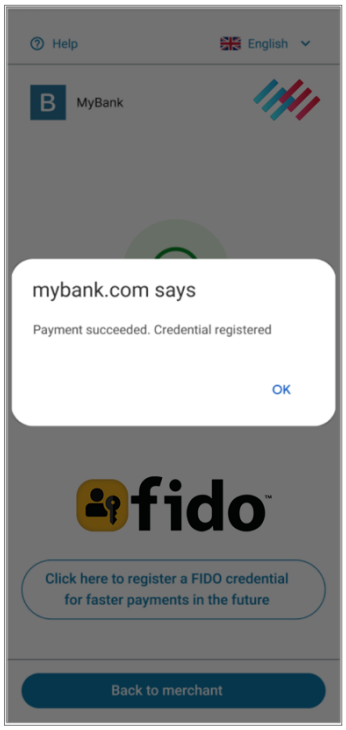
Authentication complete, cardholder is offered to create a passkey with the bank



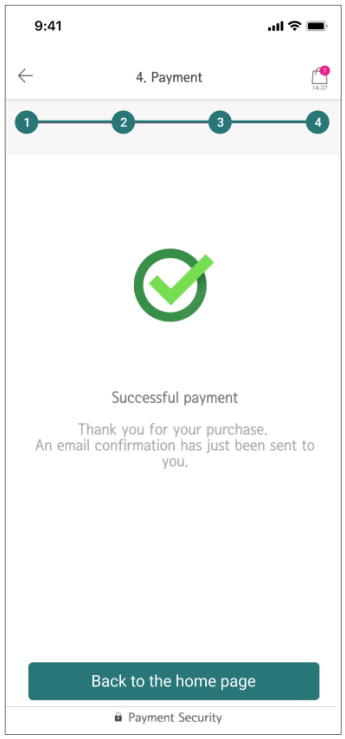
Cardholder can create a passkey associated to the payment credential and the bank



The device authenticator prompts the cardholder for their gesture



The passkey is created



The original transaction is completed by the merchant

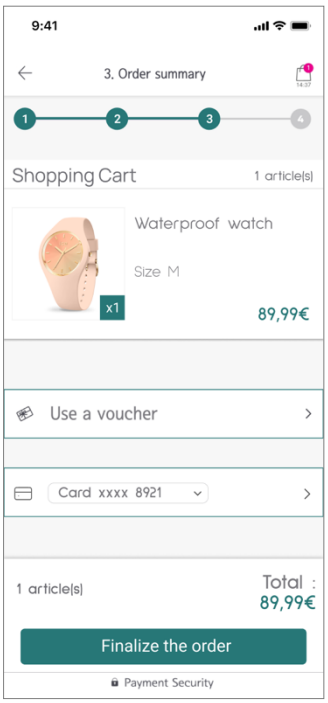
Once the passkey creation is complete, any merchant that has received the passkey information (which includes FIDO identifiers and Public Key) from the bank, through a mechanism agreed with the bank or the payment scheme, will be able to use SPC. Such a mechanism may include EMV 3DS or another integration with the payment scheme. For example, a merchant who implements EMV 3DS (i.e., version 2.3[2]) will be able to benefit from SPC through the following steps:

1. When the merchant initiates EMV 3DS to authenticate the consumer, the bank decides whether an active authentication of the cardholder is necessary. If the decision is to perform the active authentication of the cardholder, the bank can first retrieve one or several passkeys associated with the card used for the transaction, verify that the consumer is on the same registered device, and then returns the passkey(s) information to the merchant.
2. The merchant invokes the SPC web API to a SPC-supporting browser, including a few parameters in the request, such as the passkey information, card / bank / network logos, the merchant identifier and the transaction amount.
3. If the browser can find a match for one of those passkeys on the device used by the consumer, the browser displays the logos, merchant identifier and the transaction amount to the consumer, and prompts for authentication with the passkey.
4. The authentication results are returned to the merchant, who in turn will share those results with the bank for validation through the EMV 3DS protocol.

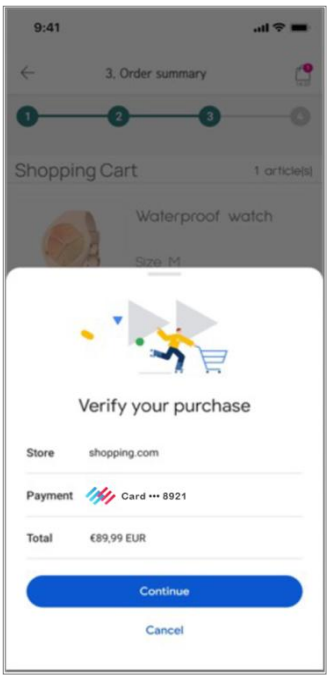
Figure 3 depicts an example of an authentication flow using SPC and EMV 3DS, with a previously registered passkey:

[2] Subject to support by payment schemes

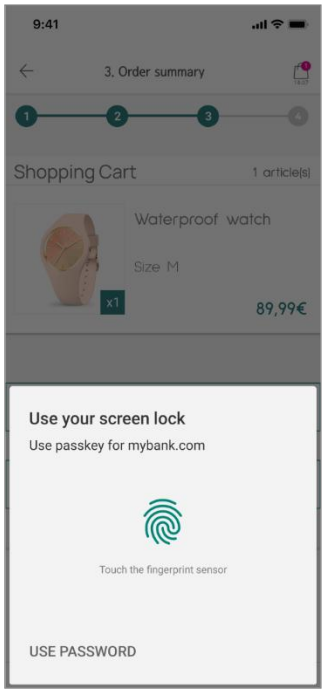
Figure 3: Authentication sequence using SPC and EMV 3DS



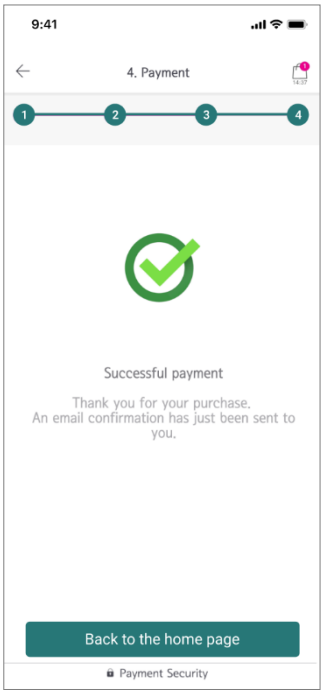
Checkout at the merchant's store



Passkey found; transaction details displayed and consent gathered



The device authenticator prompts the cardholder for their gesture



Transaction completed by the merchant

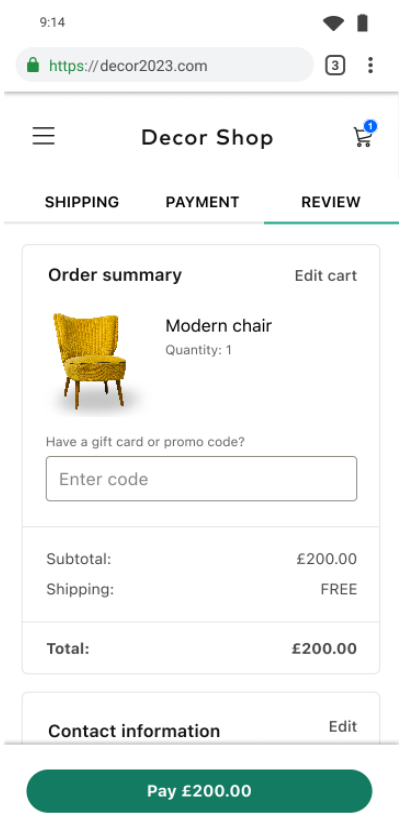
3.2 SPC With Payment Scheme as Relying Party

In some payment scenarios, payment schemes can be a relying party on-behalf of the banks to remove the need for banks to deploy a FIDO infrastructure, thereby scaling the adoption of passkeys faster.

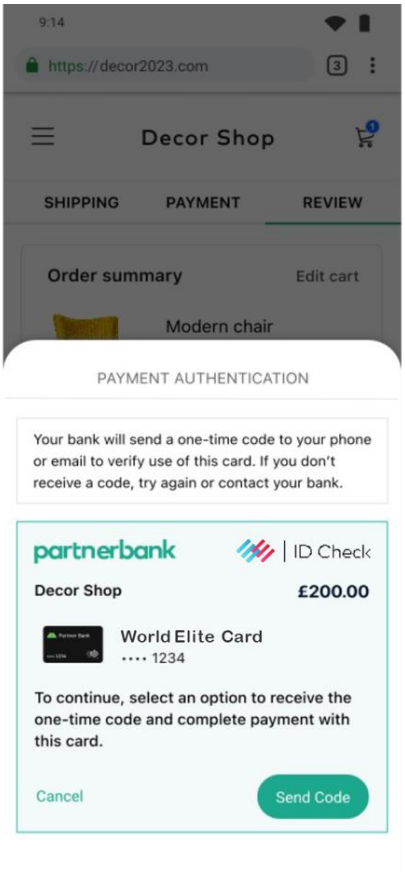
The creation of a passkey can be initiated outside of or during the checkout process:

- Outside of the checkout: for example, when the consumer is within the banking application and the bank invites the consumer to create a passkey for faster and more secure transactions, the passkey can be created with the payment scheme as the relying party, and will be associated by the payment scheme to one or multiple payment cards and to the consumer device; or
- Before, during or after a checkout: for example, the consumer may be prompted to create a passkey for faster and more secure transactions at merchants supporting the payment scheme's payment method. The passkey will be associated by the payment scheme to one or multiple payment cards and to the consumer device, once the identity of the consumer has been verified by the bank. Figure 4 depicts this sequence.

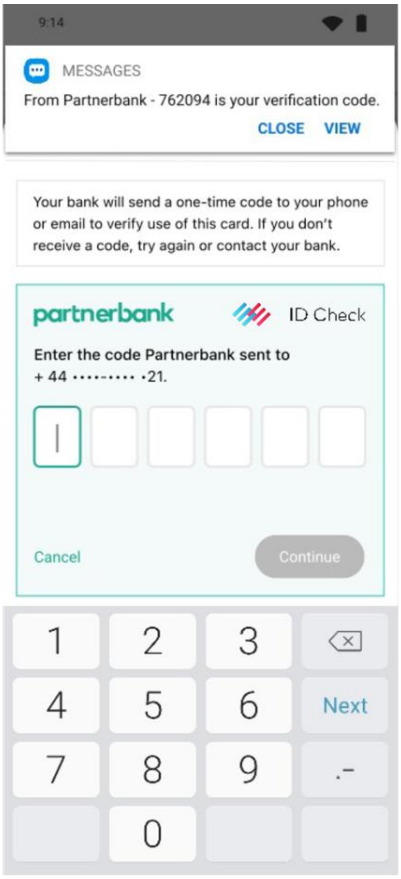
Figure 4 Passkey creation during checkout



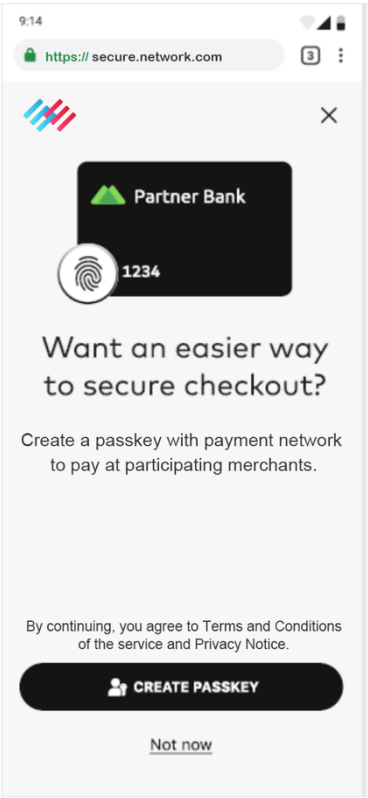
Checkout at merchant's store



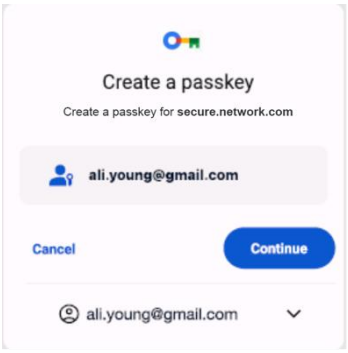
Bank's authentication page requests cardholder to authenticate



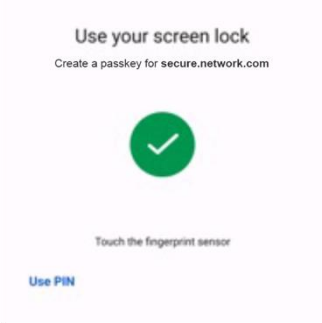
Cardholder authenticates to the bank



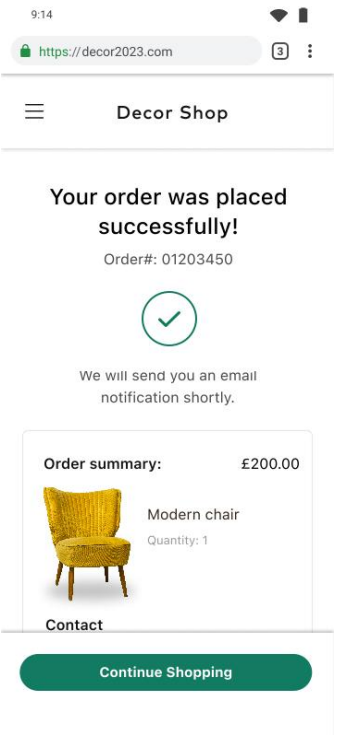
Cardholder is invited by card's payment network to create a passkey for secure checkout



Cardholder accepts the passkey creation request



Device authenticator prompts cardholder for their gesture



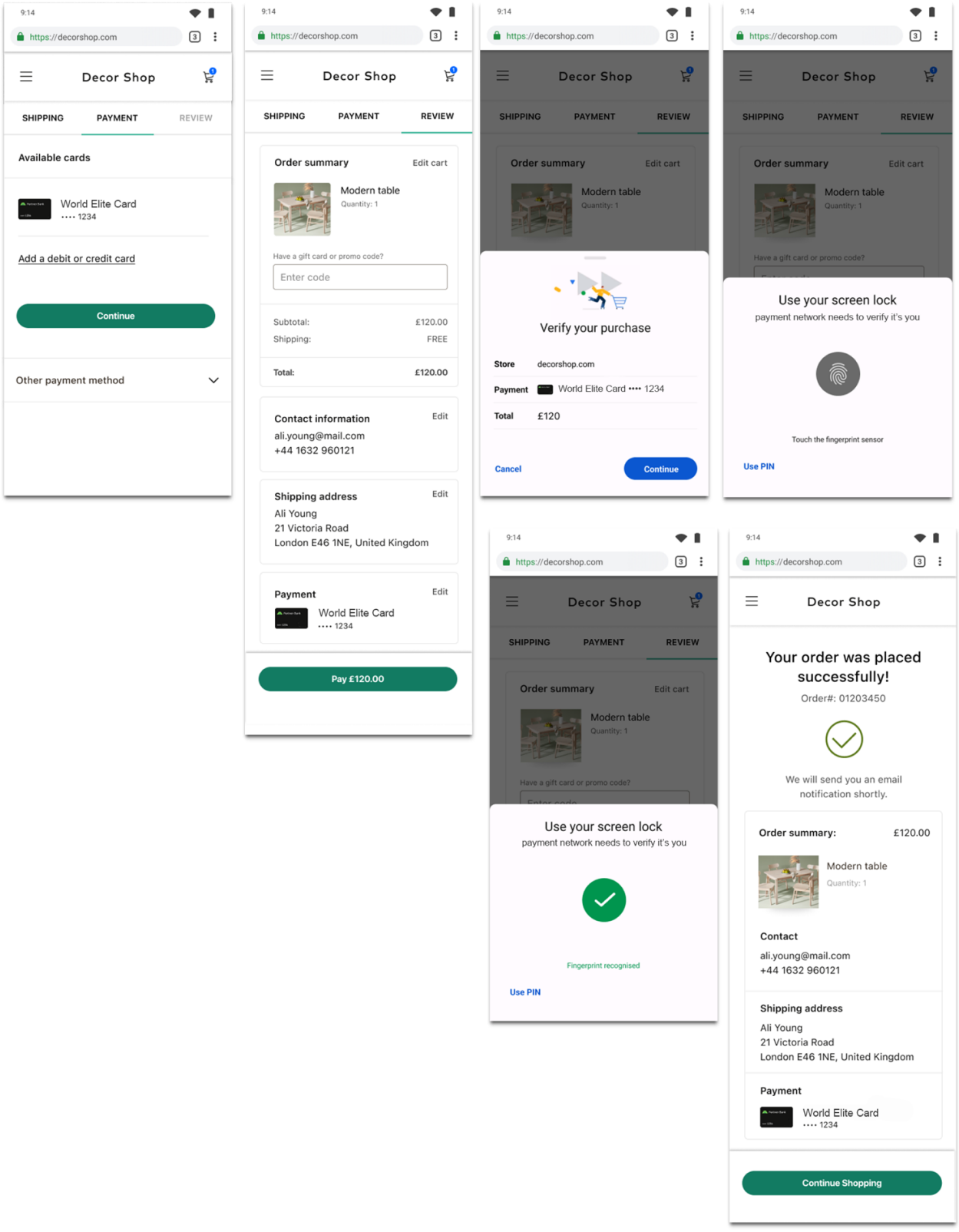
Transaction is completed by the merchant

Once the passkey creation is complete, any merchant that is using the authentication facilitated by the payment scheme will be able to benefit from SPC:

- The merchant checks with the payment scheme that a passkey is available for the card used in the transaction and retrieves the passkey information from the payment scheme.
- The merchant invokes the SPC web API with the merchant identifier and transaction amount.
- If the browser can find a match for one of those passkeys on the device used by the consumer, the browser displays the merchant identifier and the transaction amount to the consumer, card / bank / network logos, then prompts for authentication with the passkey.
- The authentication results are returned to the payment scheme that validates the results. The payment scheme shares those results with the bank, during an authorization message, for the bank to review and approve the transaction. Figure 5 shows this sequence.

Figure 5: Authentication sequence using SPC

(left to right) 1. & 2. Checkout at the merchant's store, 3. Passkey is found, transaction details displayed and consent is gathered 4. Device authenticator prompts cardholder for gesture 5. Confirmation of gesture 6. Transaction completed by the merchant



3.3 Summary of SPC Benefits

The benefits provided by SPC include:

- **Cross-origin authentication** - Any merchant authorized by a Relying Party can request the generation of a FIDO assertion during a transaction even when they are not the relying party. This provides a better user experience as there is no redirect that is required to the relying party to perform consumer authentication.
- **Consistent user experience with increased trust** - With SPC, the consumer has a consistent user experience across all merchants and independently of who plays the role of relying party. In each case, the consumer will see a window displayed by the browser, that includes payment details, the logos of their card / bank / payment scheme, increasing the trust in using FIDO authentication for their payments.
- **Increased security** - With SPC, the FIDO assertion will include payment details in the cryptogram generation such as the merchant identifier and transaction amount, making it difficult to modify any of those details in the transaction without being detected by the bank or payment scheme. This also simplifies the compliance with local regulations such as PSD2 regulation related to dynamic linking.

4. Status of SPC Support and Future Enhancement

4.1 Availability

Secure Payment Confirmation is currently published as a W3C Candidate Recommendation, and there is on-going work to include this as an authentication method in EMVCo specifications.

At the time of writing, the availability of the Secure Payment Confirmation API is limited to:

- Google Chrome and Microsoft Edge browsers
- MacOS, Windows, and Android operating systems.

4.2 Future Enhancements

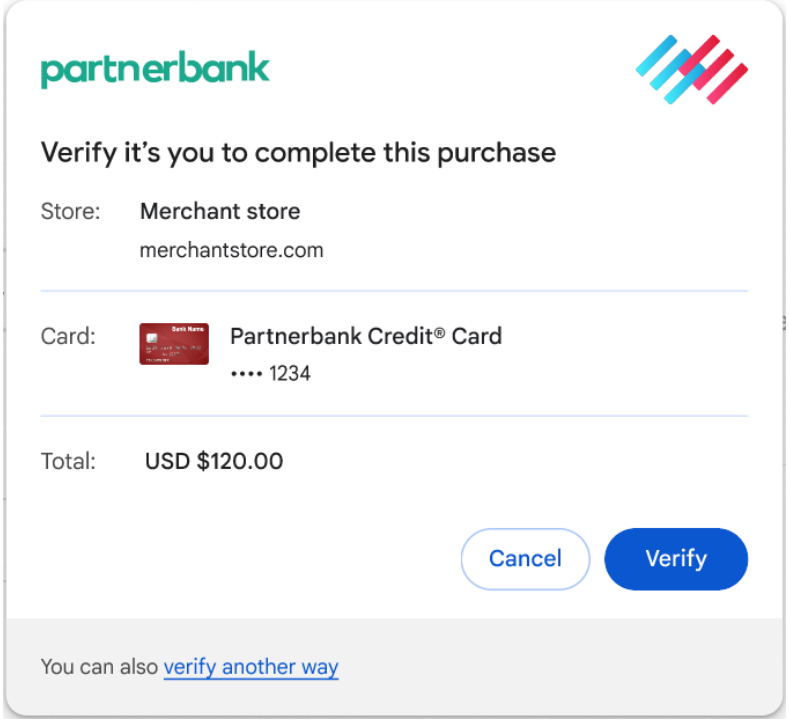
The W3C Web Payments Working Group continues to work and iterate on Secure Payment Confirmation with the goal of improving the security and the user experience when consumers authenticate for payments on the web.

Features currently under consideration include:

- Improve user and merchant experiences when there is not a credential available on the current device (i.e., a fallback user experience)
- Improve consumer trust with additional logos being displayed to the user, such as bank logo and card network logo
- Improve security with support for device binding, with the browser providing access to a browser/device-bound key
- Consider additional use cases such as recurring payments or support for roaming and hybrid FIDO authenticators

An example of enhanced SPC transaction UX that is under review is illustrated in Figure 6.

Figure 6: SPC transaction UX under review



5. Conclusion

Secure Payment Confirmation (SPC) is a web standard that has been designed to facilitate the use of strong authentication during payment transactions with best-in-class user experience, where the relying party can be a bank or a payment scheme.

The main benefits of SPC are to deliver an improved user experience, with the display of transaction details that the consumer approves with FIDO authentication, and to enable cross-origin authentication when a merchant authenticates a consumer without the need to redirect to the relying party (the bank or the payment scheme).

SPC also facilitates the inclusion of the transaction details within the FIDO signature, which can help deliver higher security and/or simplify the compliance with local regulations.

6. Acknowledgements

The authors acknowledge the following people (in alphabetic order) for their valuable feedback and comments:

- Boban Andjelkovic, BankID BankAxept
- John Bradley, Yubico
- Karen Chang, Egis
- Jeff Lee, Infineon
- Olivier Maas, Worldline

7. References

[1] "EMV 3-D Secure," [Online]. Available: https://www.emvco.com/emv-technologies/3-d-secure/.

[2] "Secure Payment Confirmation," [Online]. Available: w3.org/TR/secure-payment-confirmation/.

[3] "Secure Remote Commerce," [Online]. Available: https://www.emvco.com/emv-technologies/secure-remote-commerce/.