Update on Passkeys and SPC

W3C TPAC – September 2023

Jonathan Grossar

Disclaimer

Information in this presentation or in any report or deliverable provided by Mastercard in connection herewith relating to the projected impact on your financial performance, as well as the results that you may expect generally are estimates only. No assurances are given that any of these projections, estimates or expectations will be achieved, or that the analysis provided is error-free. You acknowledge and agree that inaccuracies and inconsistencies may be inherent in both Mastercard's and your data and systems, and that consequently, the analysis may itself be somewhat inaccurate or inconsistent. All product and company names are trademarks™ or registered® trademarks of their respective holders.

The information, including all forecasts, projections, or indications of financial opportunities are provided to you on an "AS IS" basis for use at your own risk. Mastercard will not be responsible for any action you take as a result of this presentation, or any inaccuracies, inconsistencies, formatting errors, or omissions in this presentation. Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, Mastercard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third party patents, copyrights, trade secrets or other rights.

This presentation may contain projections and other forward-looking statements that have been developed through assumptions based on currently available information. All such statements and assumptions are subject to certain risks and uncertainties that could cause actual market parameters and performance to differ materially from those described in the forward-looking statement in the presentation. Such factors include, without limitation, unanticipated technological, environmental, political, social and economic factors beyond the control of Mastercard. You should not place undue reliance on such statements.

Objectives with passkey authentication in remote commerce transactions

Reduce fraud & false declines

Secure authentication, combined with tokenization, supports increased approval rates and reduced fraud.

Reduce friction at checkout

Authentication performed in merchant environment, with mechanisms that consumers know and use every day to unlock their devices

Improve conversion rates

Build consumer trust when leveraging user-friendly and secure authentication mechanisms in a consistent way, thereby reducing abandonments during authentication process

Examples of passkey use cases for card payments

Issuers implement and use passkeys to authenticate cardholders during an EMV 3DS request where the Issuer believes that the transaction is risky or needs to be authenticated to comply with regulation

Issuer is the Relying Party

Merchants or Digital wallets implement and use passkeys to authenticate cardholders transacting with a card stored on file with the merchant or wallet. Authentication results are shared with Issuers using a mechanism defined by payment networks (e.g., Mastercard Token Authentication Framework)

Merchant, PSP or Digital wallet is the Relying Party

Payment networks e.g., Mastercard facilitate the use of FIDO to authenticate cardholders in a consistent way. Cardholders authenticate when paying with their Mastercard at participating merchants. Authentication results are processed by Mastercard and shared with Issuers.

Mastercard or Issuer is the Relying Party

SPC provides more security and better UX

Avoid authentication failures

Only prompt for passkey authentication when there is a FIDO credential available on the consumer device. This avoids the need for the consumer to cancel the authentication request when asked to select a credential that they don't have (e.g., security key).

Cross-origin authentication

Relying Party (e.g., Issuer or Mastercard) may allow Merchants or their payment service provider to initiate passkey authentication, without the need to iframe or redirect to the Relying Party's page.

Dynamic linking

Transaction amount and merchant identifier are used as input to the generation of the FIDO assertion. This enhances the compliance with PSD2 requirement.

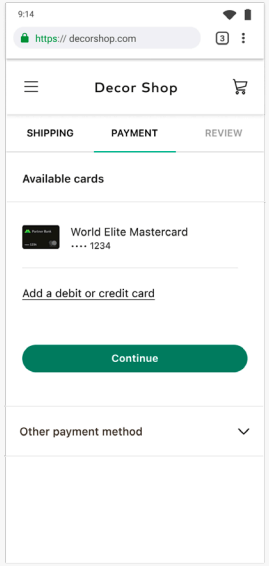
Consistency and Secure display

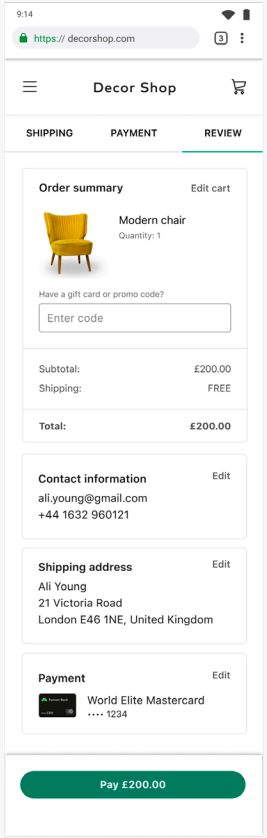
The information displayed to the consumer when authenticating is displayed in a consistent way and is secured to ensure that "what you see is what you sign".

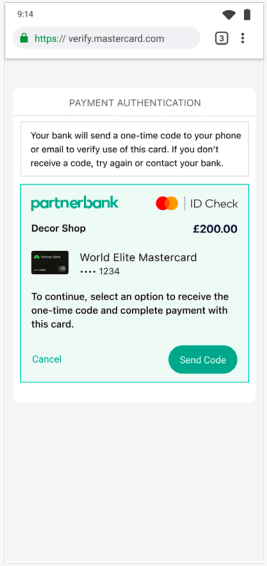
Example of Mastercard facilitating FIDO – registration during checkout*

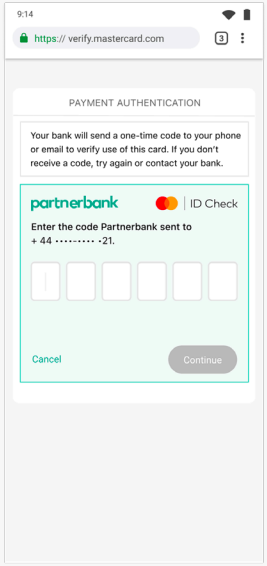
Ali selects a card for payment. After issuer authentication (ID&V), Ali is prompted to create a passkey for Mastercard

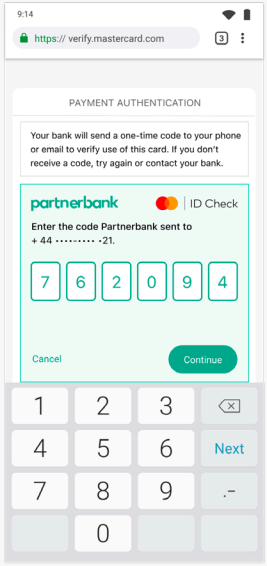
SUBJECT TO CHANGE – FOR ILLUSTRATION PURPOSES ONLY

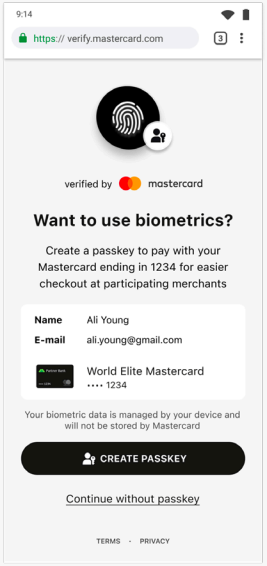












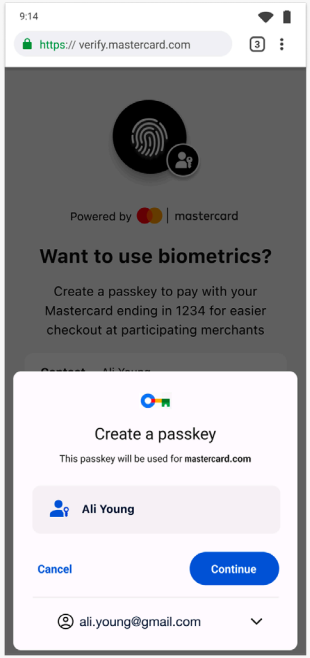
EMV 3DS with Issuer authentication

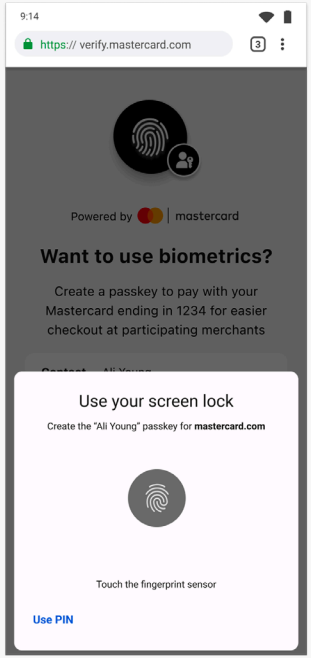
Ali agrees to create a passkey

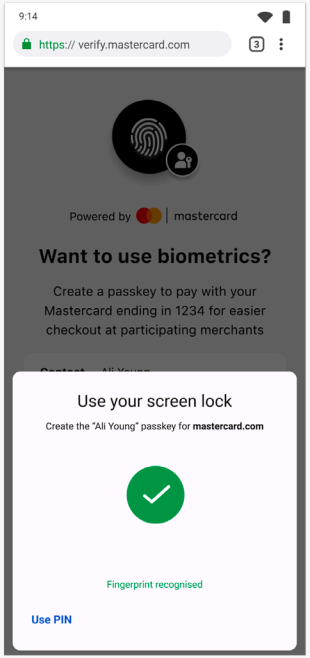
*registration can be facilitated also during card add or within an issuer application

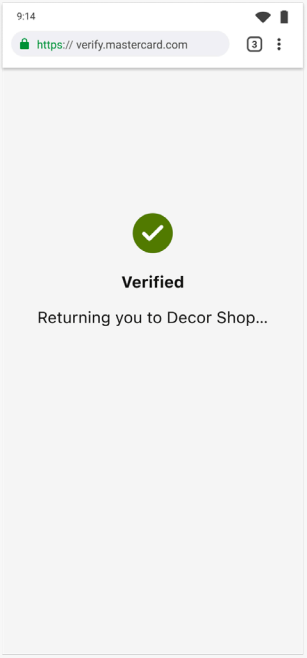
Example of Mastercard facilitating FIDO – registration during checkout

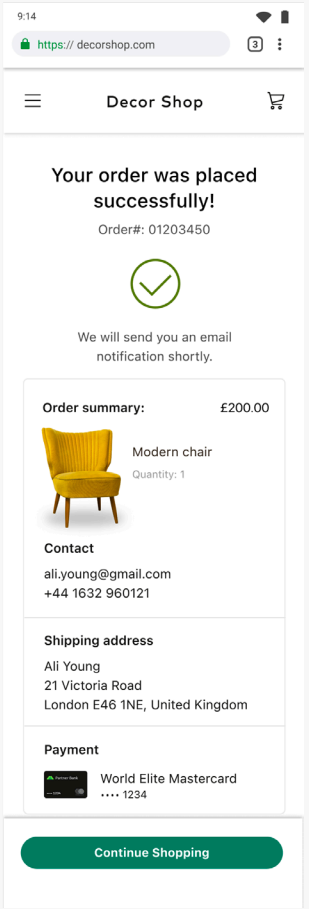
SUBJECT TO CHANGE – FOR ILLUSTRATION PURPOSES ONLY







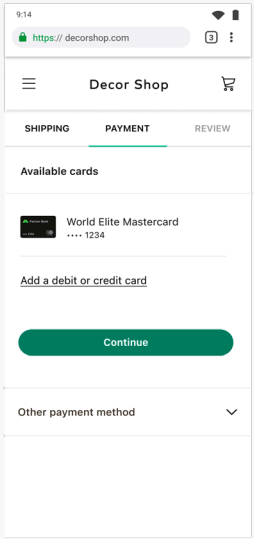


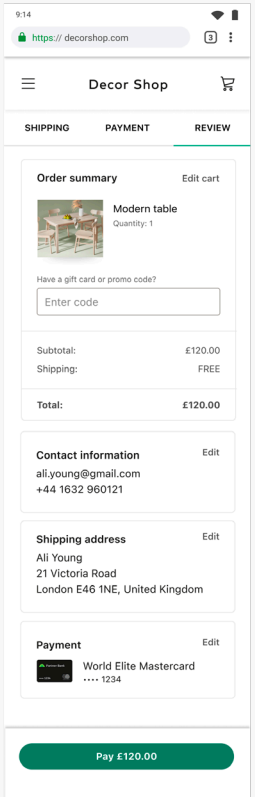


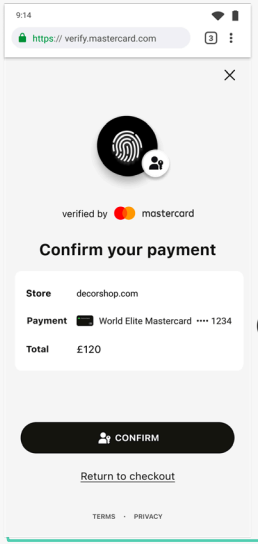
UX driven by device operating system

Example of Mastercard facilitating FIDO – authentication during checkout

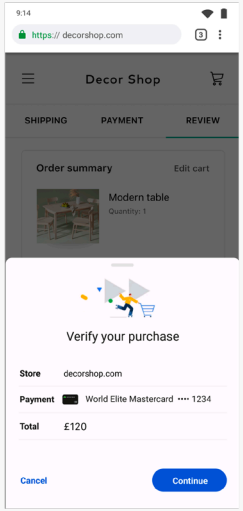
SUBJECT TO CHANGE – FOR ILLUSTRATION PURPOSES ONLY

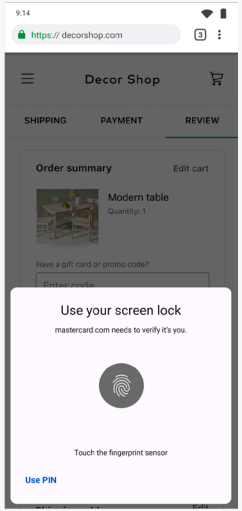


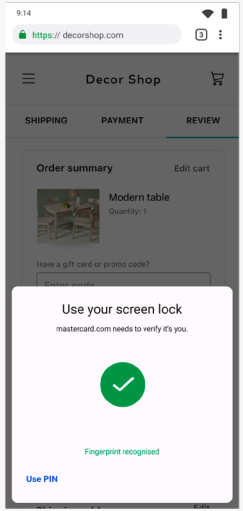




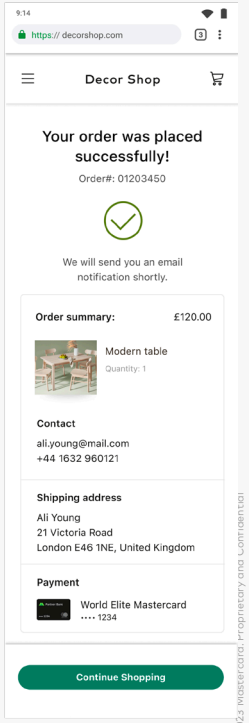
OR



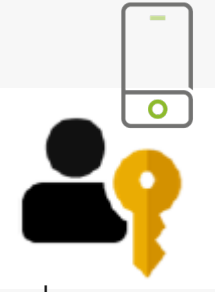




WebauthN OR SPC



The introduction of passkeys comes with new challenges



Challenges

Currently, passkeys do not come with attestation. Relying Parties are not able to identify the source, to validate that the passkey comes from a certified passkey provider

Currently, some passkeys are synchronized across devices without the possibility for Relying Parties to recognize on which device it is used or identify the Operating System's KYC used to recognize the consumer across devices. Hence RPs are unable to validate the identity of the cardholder using those passkeys.

Risks

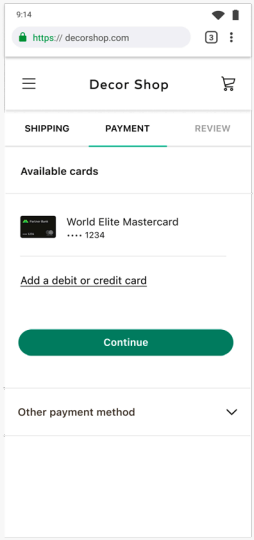
Non-compliance with regulations e.g., PSD2

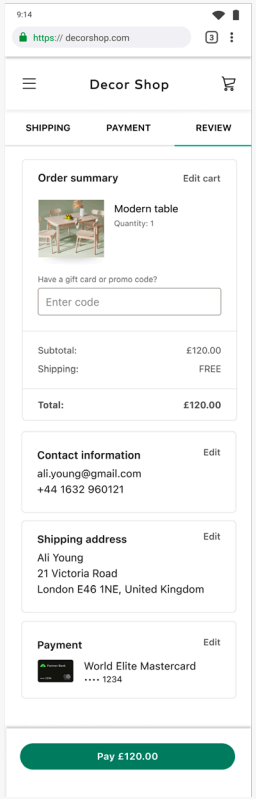
Lack of consumer confidence to use passkeys for payments

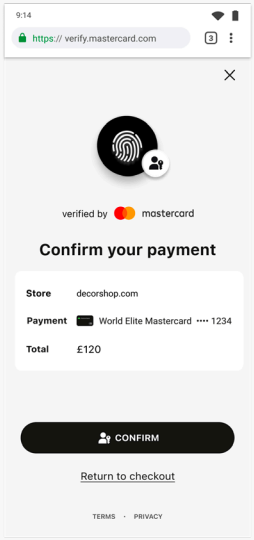
Financial losses for Issuers in case of fraud

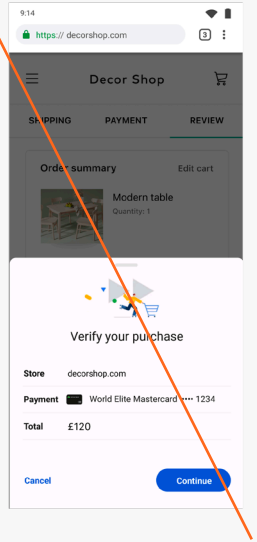
Degraded user experience

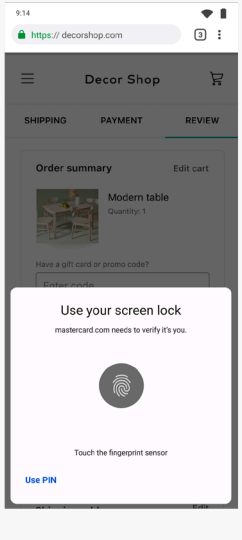
Example of risk with passkey synchronization (degraded UX)

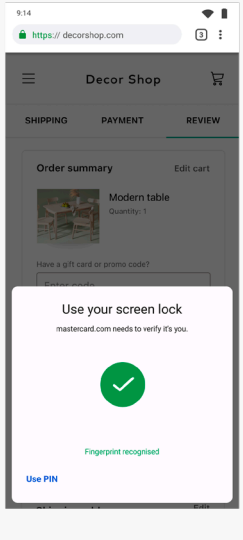


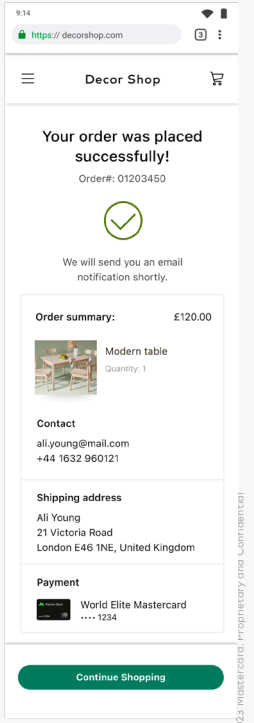






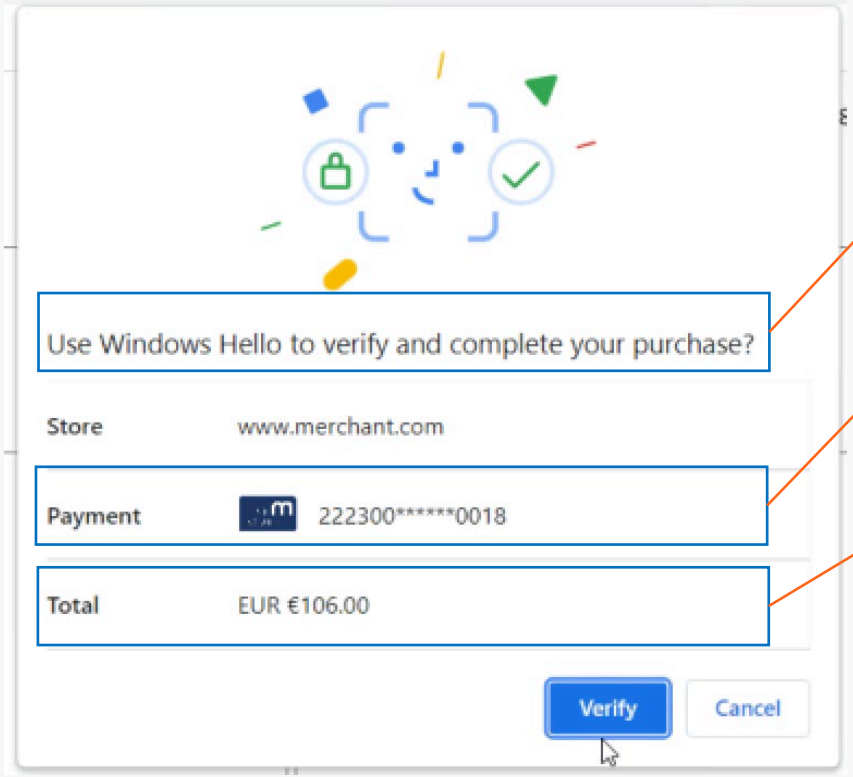






A redirect to the Relying Party (here: Mastercard) may be required to detect the consumer device e.g., when regular cookies are used – making SPC a redundant step

Possible enhancements to SPC to support consumer access to their account (i.e., outside of transaction authentication)



Examples of enhancements

Use Windows Hello to access your account

Account: e.g., Click to Pay (req.), email (opt.)

(remove)