entersekt

Entersekt Overview

Enabling Strong Authentication

GERHARD OOSTHUIZEN

2023/09/12

Important notice

Future Product Scope Disclaimer

This document and Entersekt's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at Entersekt's sole discretion. Information regarding potential future products or developments is intended to outline our general product direction and should not be relied on in making a purchasing decision.

This document is provided without a warranty of any kind, whether express or implied, and Entersekt assumes no responsibility for errors or omissions in this document. The information mentioned regarding potential future products or developments is not a commitment, promise, or legal obligation to deliver any material, code, or functionality.

Information about potential future products or developments may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remain at our sole discretion.

00

Agenda

00 Introduction

01 Demo time

02 Challenges and recommendations

entersekt

entersekt

We are the **leading** **transaction authentication provider** for **financial institutions**.

Founded in
2010

250 million +
authentications
every month

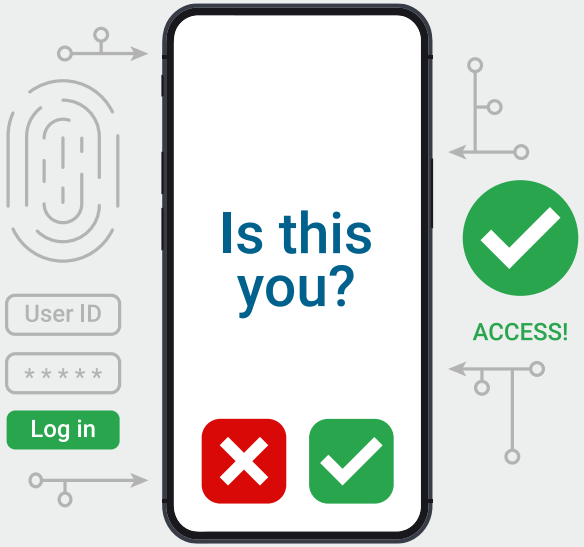
>82million
Enrolled
users

175+
banking & FI
clients

Backed by:
PAPE*funds*
AKKR
ACCEL-KKR
RMI

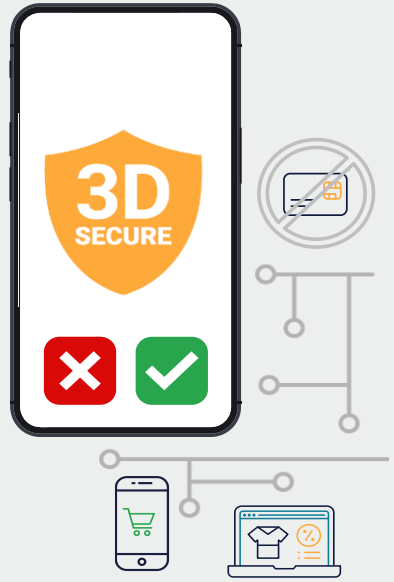
The solutions we take to market…

Foundational elements



Customer Authentication

Full-service enablement



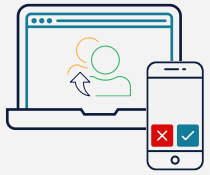
ACS (3D Secure)

Financial institutions need to protect more than just *Login*.

Access to Accounts

Login is only a small part of banking

Digital banking access
Login and set up



Open banking AISP
Strong customer Auth (SCA) for third party account access

Moving money / payments

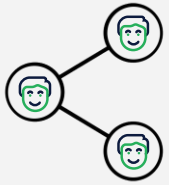
Open Banking PISP
Strong customer auth (SCA) for payments from third parties

3-D Secure
Authentication for ACS

Faster Payments
Push payments via networks or once-off payments

QR or link-based Payments

High risk events



Recovering credentials
Resetting forgotten passwords and managing phone numbers.

Linking a trusted endpoint
Enabling a mobile app and setting up biometrics

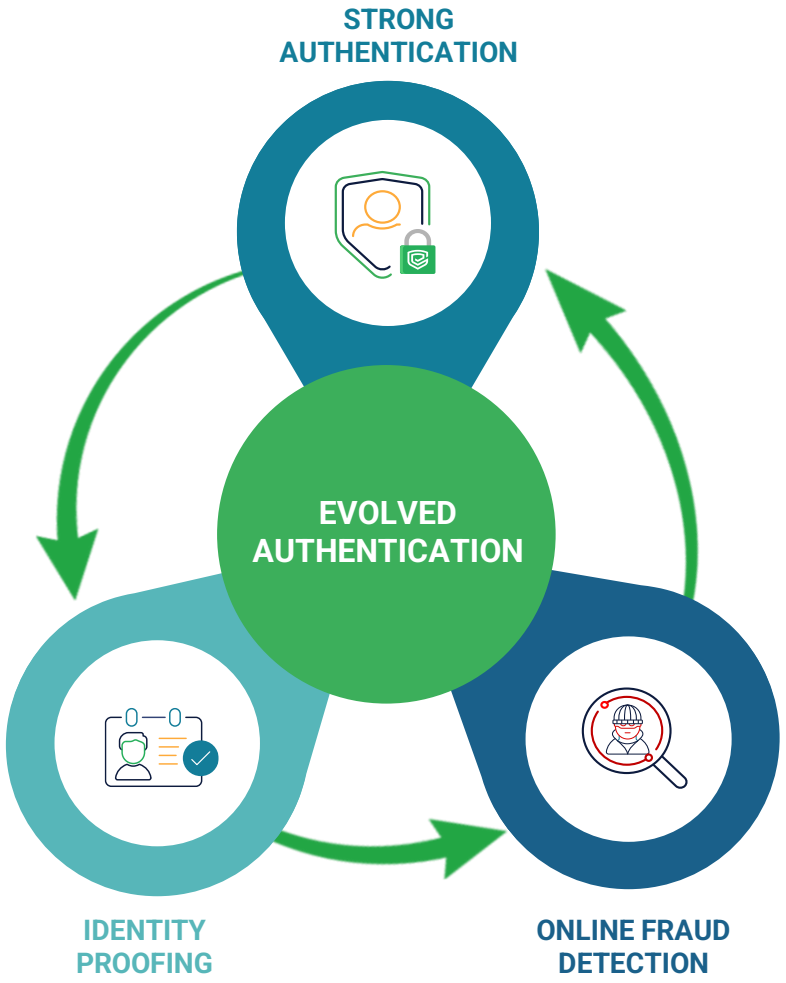
Tokenizing a card (ID&V)
Using customer consent to issue card into a wallet

Increased risk and impact...

The set of activities spans a wide range of systems and use cases, but they all require the customer's participation
Some are initiated by the customer directly, but others originate from systems

entersekt

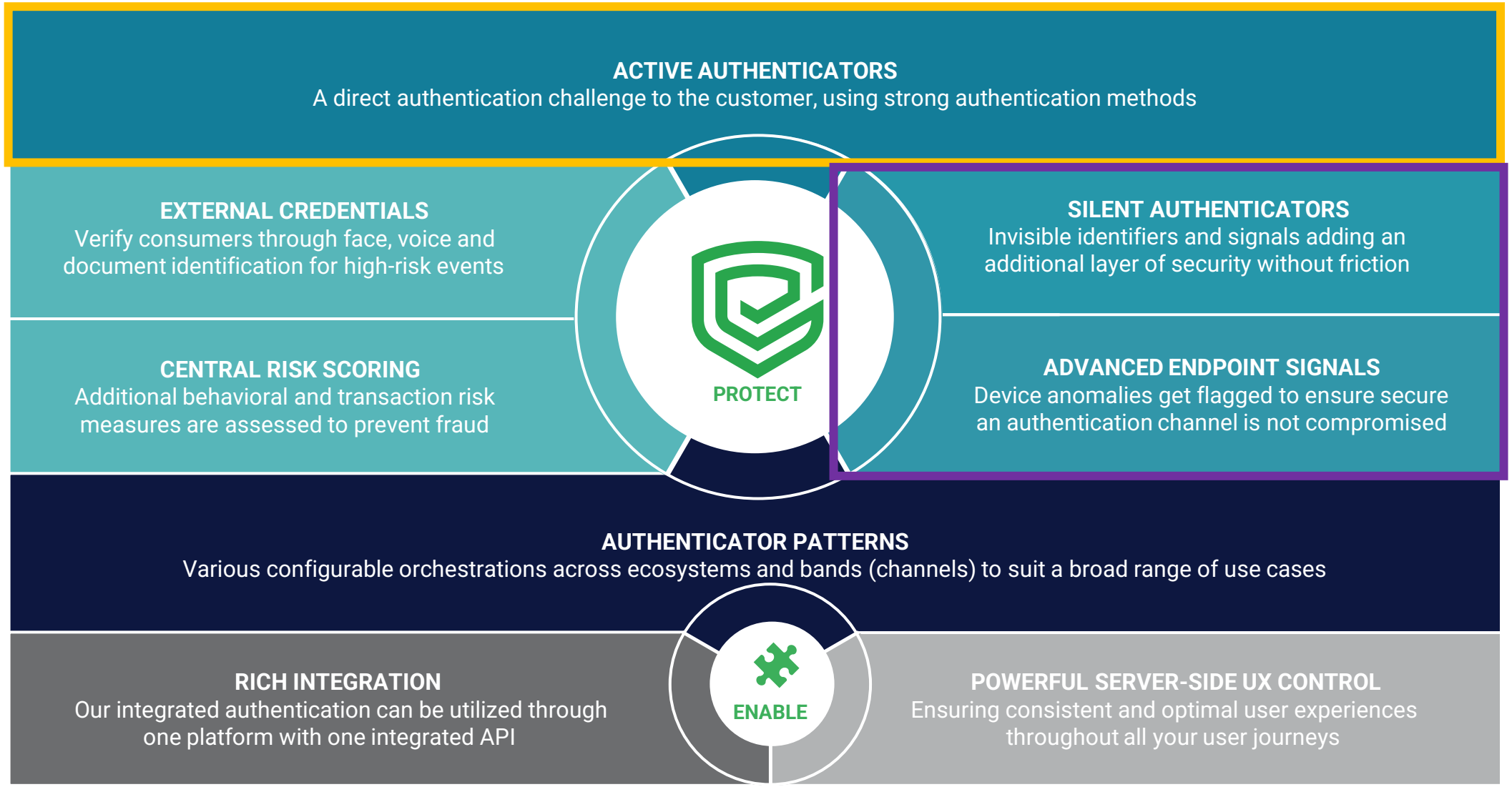
The landscape around authentication has evolved



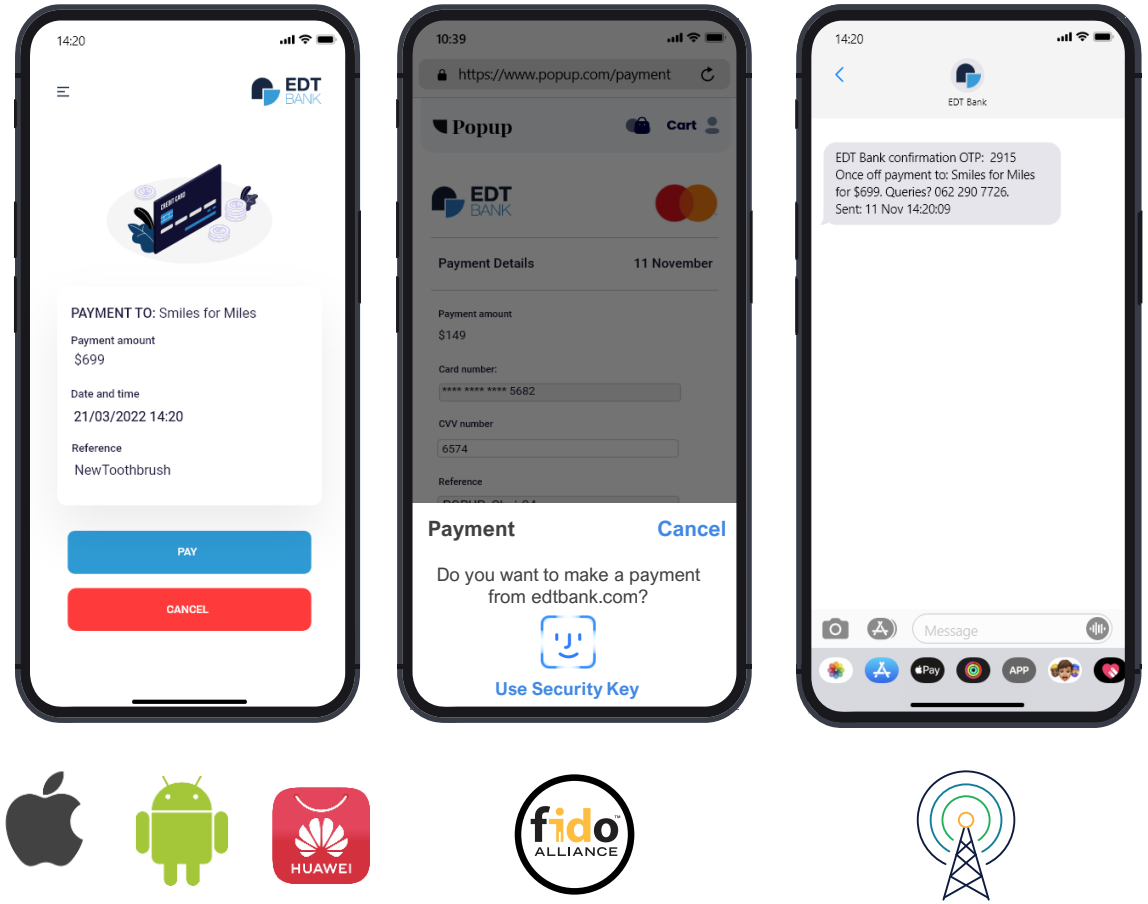
Industry convergence

- Evolved Authentication **requires convergence** across Strong Authentication, Online Fraud Detection and ID Proofing
- We've **partnered with industry experts** in these adjacent fields to bring an integrated solution offering best-of-breed value
- Entersekt has **integrated** these **into a single API** ready for clients to consume

An integrated solution to the fraud problem.



Active Authentication.



One-touch multi-factor authentication.

Stronger **security.** Better **experiences.**

Intuitive, proven UX

Fully PSD2 compliant

Mobile apps, browsers and phone numbers

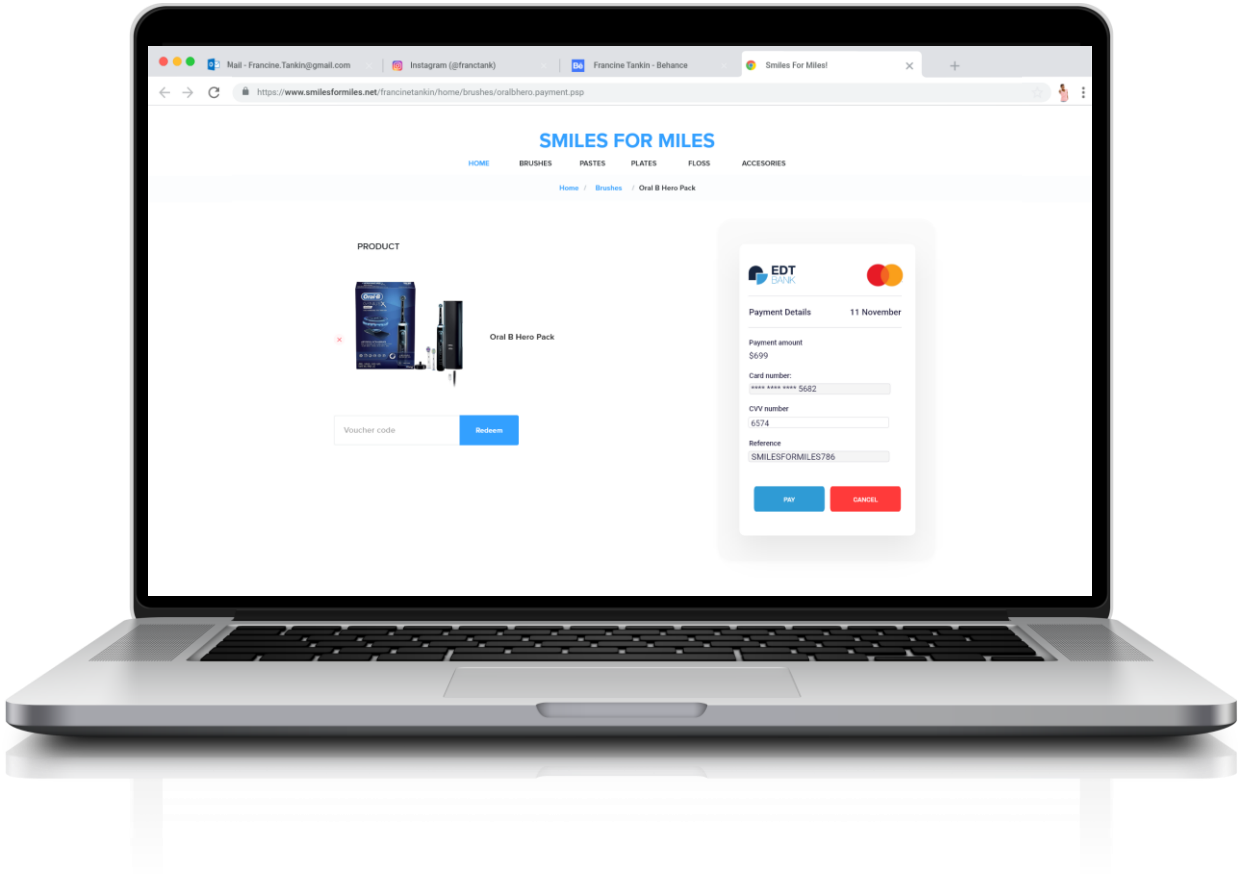
Easy integration, flexible deployment options

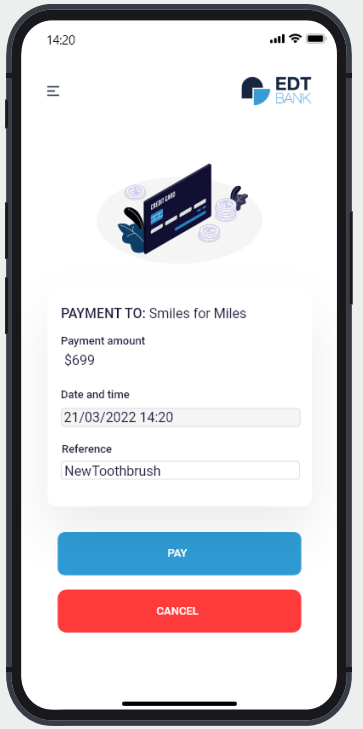
Strong roadmap with regular enhancements

International

entersekt

Online payment – 3D Secure.

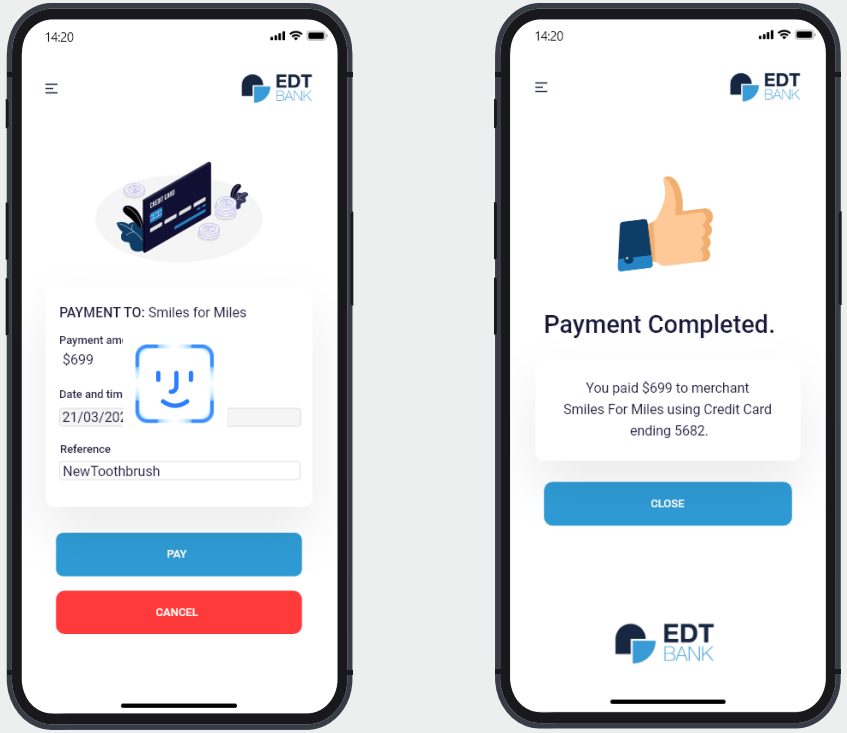


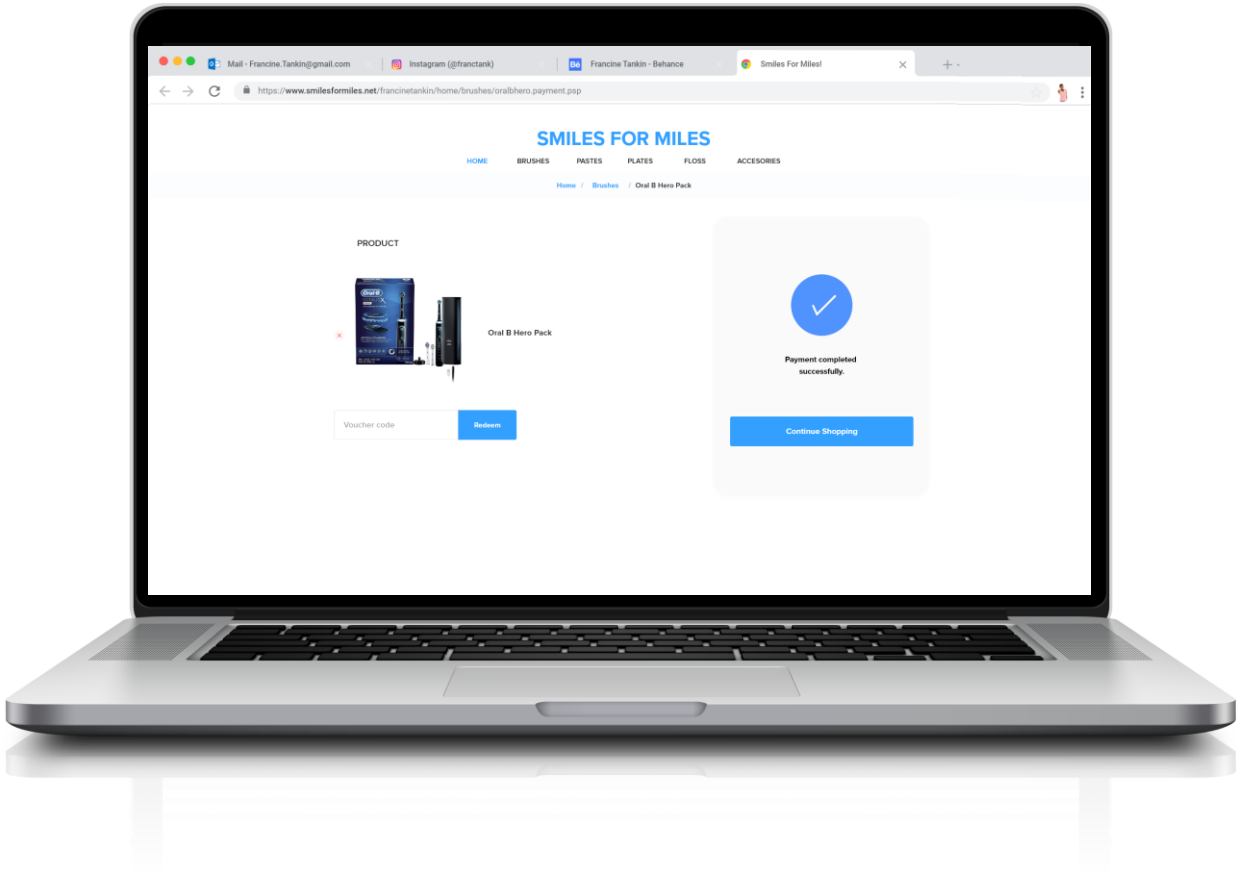


Secure online payment

Entersekt enables a secure payment using a 3D Secure push notification to the customer's registered device, using the existing bank app.

Online payment – 3D Secure.





Secure online payment

When selecting to authorize the payment, the customer is prompted to authenticate the interaction using the device's native biometrics.

01

Agenda

00 Introduction

01 Demo time

02 Challenges and recommendations

entersekt

SPC’s unique benefits

Payment display	Cryptographic proof	Cross-domain control
Payment information shown to customer natively in browser	Transaction details signed into cryptogram on the device using hardware backed storage	Merchant or PSP can use Issuer’s credentials for on the merchant page (no re-direct required)

Demo setup for this session…

We will generate a URL for each of these flows. Clients integrate that into their customer journey

Three Authenticators

Windows 10
(Platform Authenticator)

Android
(Platform Authenticator)

iOS 16
(Platform Authenticator)

Five Environments

Windows 10 with Chrome

Samsung with Chrome

iPhone 12 with Chrome

iPhone 12 with Safari

Windows 10 with Edge

Two Transactions

Login

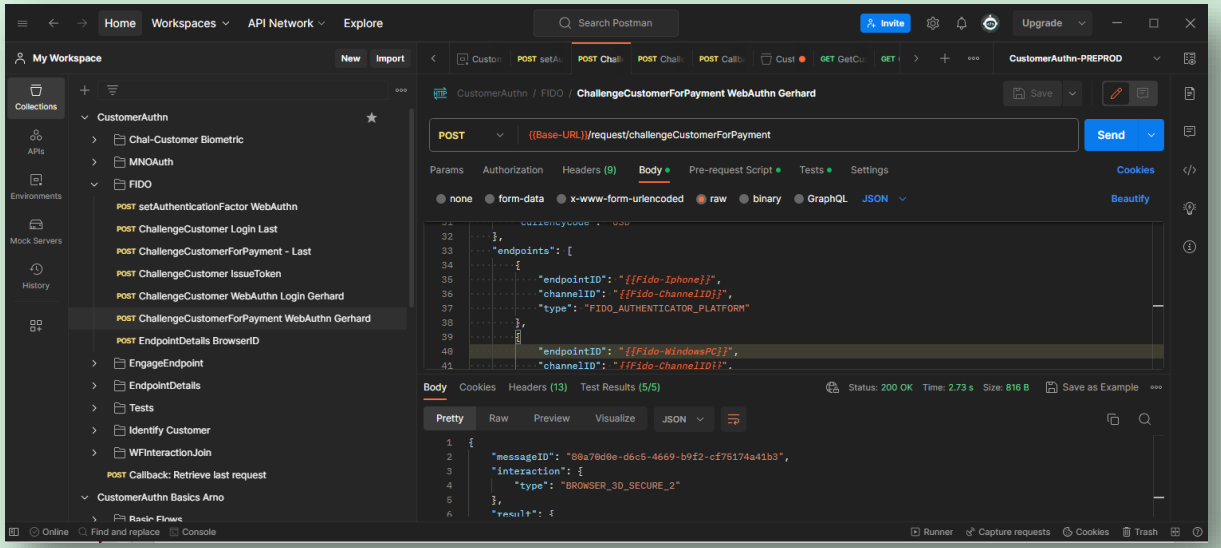
eCommerce Payment

Demo notes

I'm using
PostMan to demo,
showing the back-end API's.

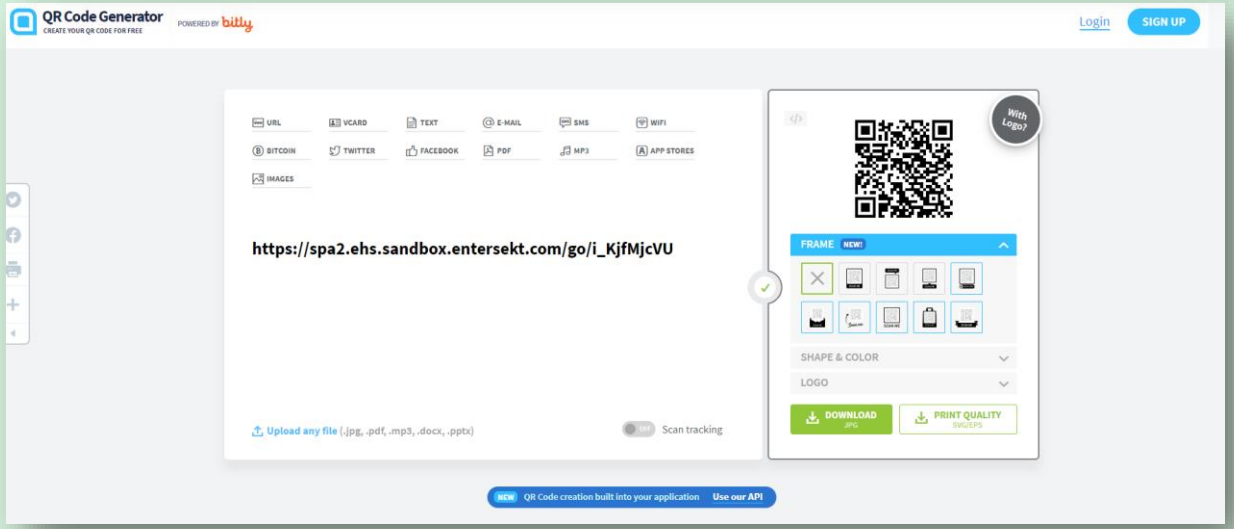
API's call requests a URL, which the client will redirect to from their browser.

There are many other ways to use these API's, but we're not demoing the API's today…



I'm using a
QR viewer to transfer links
to my test phones.

In practice the client does a web redirect to this page from their device and redirects back once completed.



Some notes on our integration.

Best possible technique becomes available

- Our clients do not want to worry about the specific mechanism employed.
- They want to get the job done in the best way – selecting SPC when it's available is our job.

We always enable fido tokens to be able to perform payments

- There is no need to not-enable it and then later wishing you wanted it.
- If the client does not want to use it, they should not call the instruction

Demo setup for this session…

Three Authenticators

Android
(Platform Authenticator)

iOS 16
(Platform Authenticator)

Windows 10
(Platform Authenticator)

Five Environments

Samsung with Chrome

Windows 10 with Chrome

Windows 10 with Edge

iPhone 12 with Chrome

iPhone 12 with Safari

Two Transactions

Login

eCommerce Payment

Demo setup for this session…

Three Authenticators

Android
(Platform Authenticator)

iOS 16
(Platform Authenticator)

Windows 10
(Platform Authenticator issued in Chrome)

Five Environments

Samsung with Chrome

Windows 10 with Chrome

Windows 10 with Edge

iPhone 12 with Chrome

iPhone 12 with Safari

Two Transactions

Login

eCommerce Payment

Demo setup for this session…

Three Authenticators

Android
(Platform Authenticator)

iOS 16
(Platform Authenticator)

Windows 10
(Platform Authenticator)

Five Environments

Samsung with Chrome

Windows 10 with Chrome

Windows 10 with Edge

iPhone 12 with Chrome

iPhone 12 with Safari

Two Transactions

Login

eCommerce Payment

Demo setup for this session…

Three Authenticators

Android
(Platform Authenticator)

iOS 16
(Platform Authenticator)

Windows 10
(Platform Authenticator)

Five Environments

Samsung with Chrome

Windows 10 with Chrome

Windows 10 with Edge

iPhone 12 with Chrome

iPhone 12 with Safari

Two Transactions

Login

eCommerce Payment

Exploring failure journeys

Three Authenticators

Another device
(Platform Authenticator)

Five Environments

Samsung with Chrome

Windows 10 with Chrome

Windows 10 with Edge

iPhone 12 with Chrome

iPhone 12 with Safari

Two Transactions

Login

eCommerce Payment

Demonstration Notes

Windows
Chrome | Edge

- Edge requires multiple fallback steps. It work on WebAuthn eventually.
- The inverse would have happened in Chrome if the token was issued on Edge

Chrome
Android | Windows

- Different Action buttons (Verify vs Continue)
- Chrome on Android shows USD after, and on windows before
- Payment display not kept visible on Android but stays visible on Windows.

iOS
Chrome | Safari

- Cross browser works due to Safari Webkit underneath.
- SPC obviously does not work. The payment is followed by a “Sign in” request.

02

Agenda

00 Introduction

01 Demo time

02 Challenges and recommendations

entersekt

Challenges to adoption

Some new observations…

User activity required on new page (e.g. after redirect)

- Activating SPC and WebAuthn directly requires a user interaction (although that's being addressed)
- This causes and extra user action being enforced… So we're up to 3 actions if biometric (and more if there is only PIN)…

Inconsistencies across browsers on same OS

- MacOS: WebAuthn did not work across browsers on the same Mac. It worked on iOS.
- Windows: WebAuthn worked and SPC worked, but only on the browser it was created on.

When can we use fido?

- The inability to control the browser flow. This is a real challenge – we need predictability.
- When you guess wrong, you confuse the user. The friction is perhaps worse than OTP.
- Everyone's going to implementing workarounds (e.g. Cookies, fingerprinting) and still get it wrong…

Lack of PSD2 clarity for Passkeys

- Full support for 'Device Signature' to separate Passkeys across devices (European regulators not happy without this)

Perceived challenges to adoption

Some new observations…

Fallback journeys are clumsy

- Inconsistent and confusing to the user. We need to find a better way…

Friction remains high

- SPC requires and additional action (Verify and WebAuthn and Biometric)
- Single confirmation would be awesome!

Limited UX control…

- E.g. very small card icon, domain name limited.

Wider coverage

- Would be great to get need than than just Chrome & Edge. It can work however if these predictability…
- For payments, we'll need OS Level based changes too (ux & universal device binding).

Some ideas of how to increase adoption

Sorry – some of them are not new…

Offer a browser only journey

- The Browser + OS combination is still clunky and leads to many inconsistencies.
- Can we bootstrap it with a browser only control, and allow the relying party to choose?
- This is a consumer use-case. Removing the OS dependency might allow us to experiment faster initially.

The industry is asking for lower friction (trusted browser)

- Some markets, such as the USA, will not accept extra friction at every transaction.
- Anything is better than device fingerprinting with SMS OTP – can find a balance with privacy here?
- E.g. enabling a customer to ‘trust this browser’ and not having to challenge every time…

Enabling SPC for passkeys (OS synch and over BLE)

- Actual OS level support (not requiring browser caching of SPC activity).
- Device specific attestation for regulatory clarify
- Enabling us to leverage SPC for passkeys (synch and BLE) would further increase chances of success.

entersekt

www.entersekt.com