fido ALLIANCE simpler stronger authentication

Fast IDentity Online (FIDO) implementation for Digital Finance

David Turner
Director of Standards Development

Dec 1 2022

> Passwords cannot meet the challenge of keeping critical information secure.

Bill Gates – RSA Conference

> There is no doubt that over time, people are going to rely less and less on passwords.

Bill Gates – RSA Conference **2004**

59%

Of employees still rely on username and password to authenticate into their accounts

(Yubico)

81%

Of hacking-related breaches use stolen or weak passwords

(Ping Identity)

24.6 Billion

Complete sets of usernames / passwords in circulation in criminal marketplaces

(Digital Shadows Photon)

54%

Of employees admit to writing down or sharing a password in the past year

(Yubico)

43%

Of people have abandoned a purchase in the past month due to forgotten passwords

(2022 FIDO Authentication Barometer)

300x

Number of times more likely the financial services sector is to be hit by a cyberattack

(Finextra / Boston Consulting Group)

39%

Of Americans experience a high degree of password fatigue or anxiety

(Beyond Identity)

$18.5 million

Average cost of cyberattack in financial services, higher than any other vertical

(Accenture)

>99.9% of breaches

(password only auth)

Hackers don’t break in. They log in.

A fundamental shift is required

From legacy, **knowledge-based** credentialing

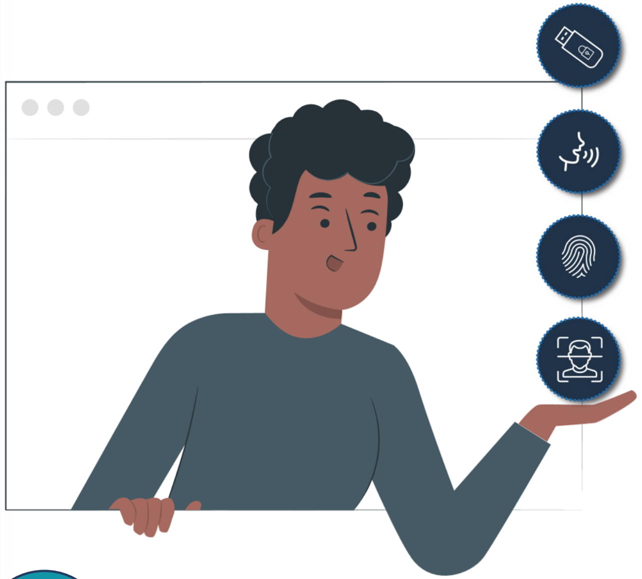
In your head (remembered)…

- Stored on a server
- SMS OTP
- KBA
- Passwords

SUSCEPTIBLE TO COMMON THREATS

…to modern, **possession-based** credentialing

In your hand

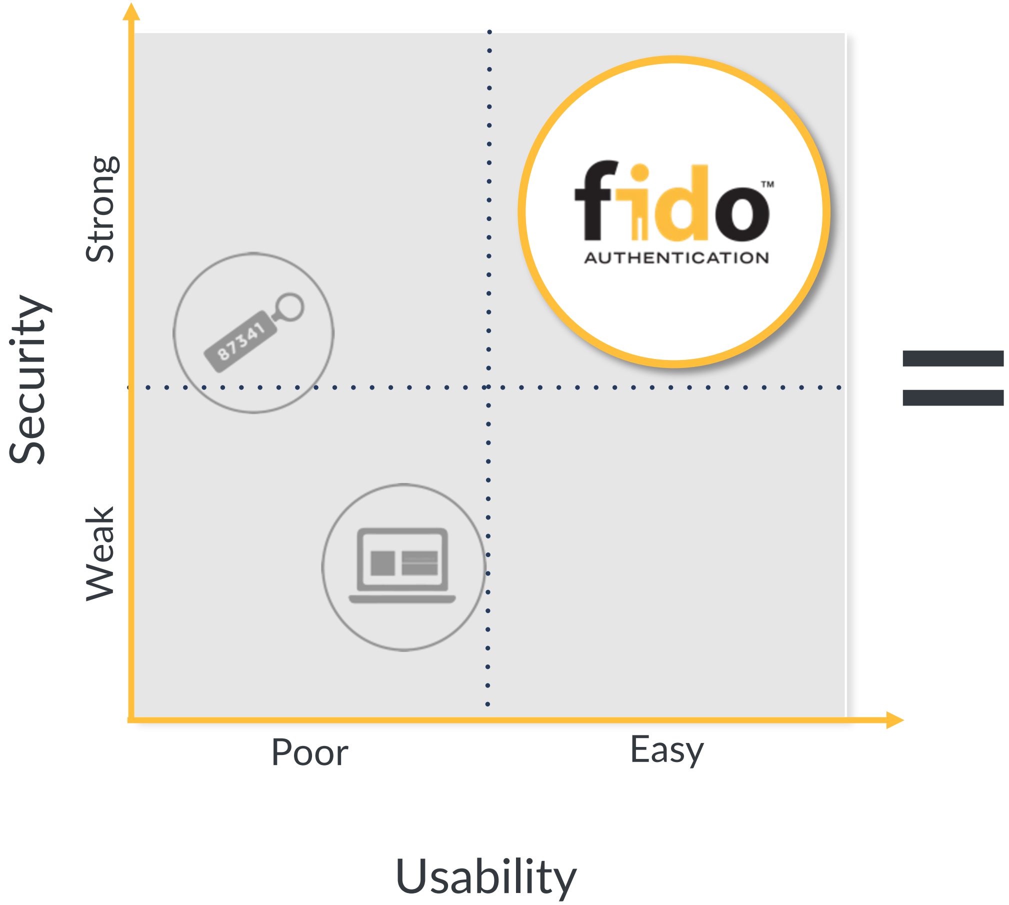


- On-device (never on a server)
- Local Biometric
- Device PIN
- “Passkeys”

PHISHING RESISTANT

(User-initiated & cryptographically secure)

Industry imperative: Simpler and stronger



=

Open standards for simpler, stronger authentication using public key cryptography

Single Gesture
Possession-based Authentication

Backed by global tech leaders

amazon

AMERICAN EXPRESS

Bank of America

CVS Health

egis Technology

FEITIAN WE BUILD SECURITY

Google

HYPR

IDEMIA

Infineon

ING

intel

JUMIO

LastPass

Lenovo

LINE

mastercard

Meta

Microsoft

nok nok

NTT docomo

OneSpan Be bold. Be secure.

onfido

PayPal

Qualcomm

RAON

RSA

SAMSUNG

Synaptics

THALES

transmit security

TRUSONA

TRUSTKEY SOLUTIONS

usbank

USAA

VISA

vmware

WELLS FARGO

YAHOO! JAPAN

yubico

+ Sponsor members

+ Associate members

+ Liaison members

+ Government members

Global market validation (partial list)

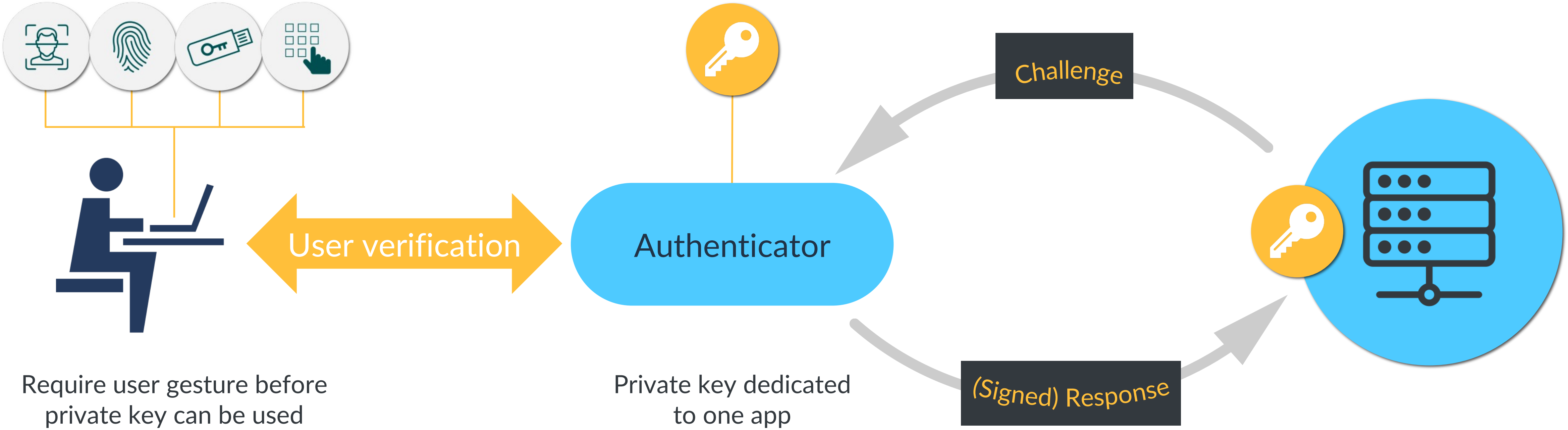
Bank of America
TARGET
中國銀行
BANK OF CHINA
f
intuit
CVS Health
Dropbox
T Mobile
SoftBank
verizon
NTT docomo
ebay
salesforce
Cigna
LOGIN.GOV
PLUS
IBM
Rakuten
twitter
MERCK
YAHOO! JAPAN

fido ALLIANCE

Now supported cross-platform

android
Hello

FIDO Authentication: How it works



User verification

Authenticator

Challenge

(Signed) Response

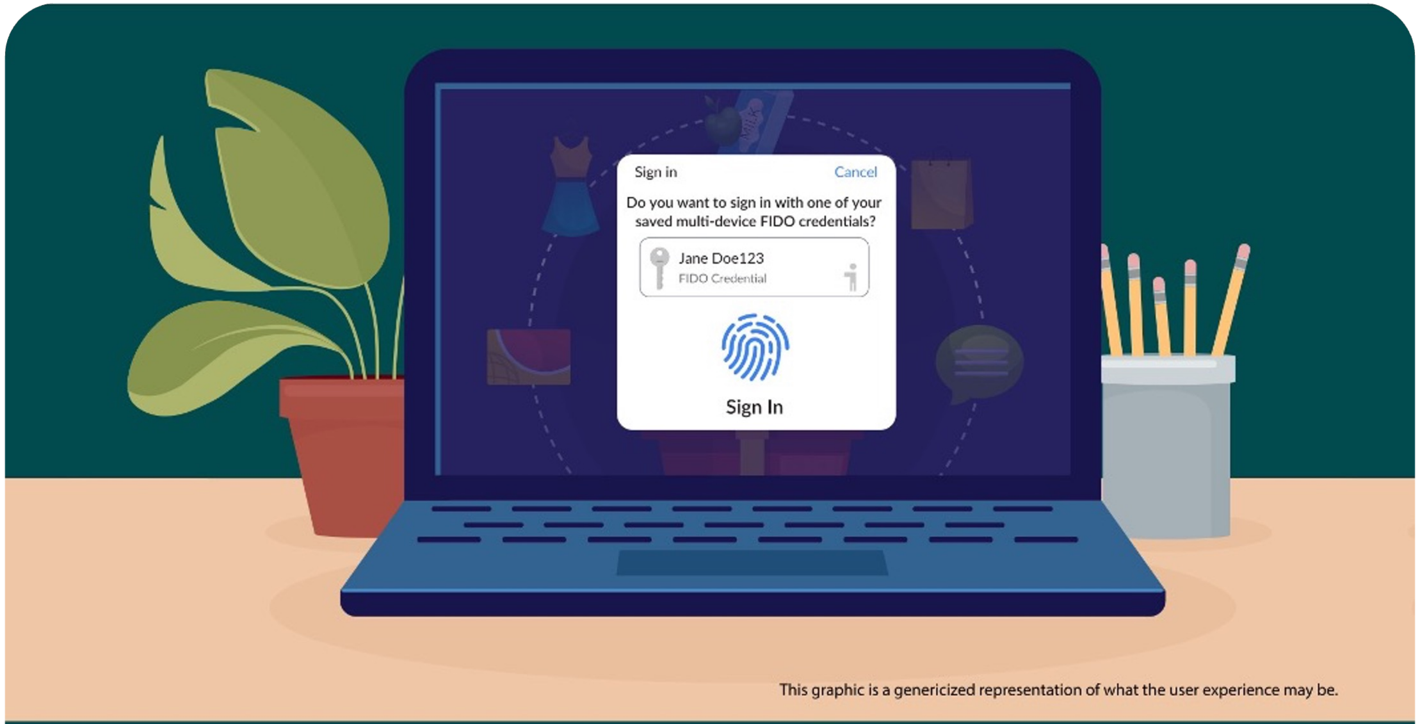
Require user gesture before private key can be used

Private key dedicated to one app

#identiverse

Multi-device FIDO credentials

AKA “passkeys”



Do you want to sign in with one of your saved multi-device FIDO credentials?

This graphic is a genericized representation of what the user experience may be.

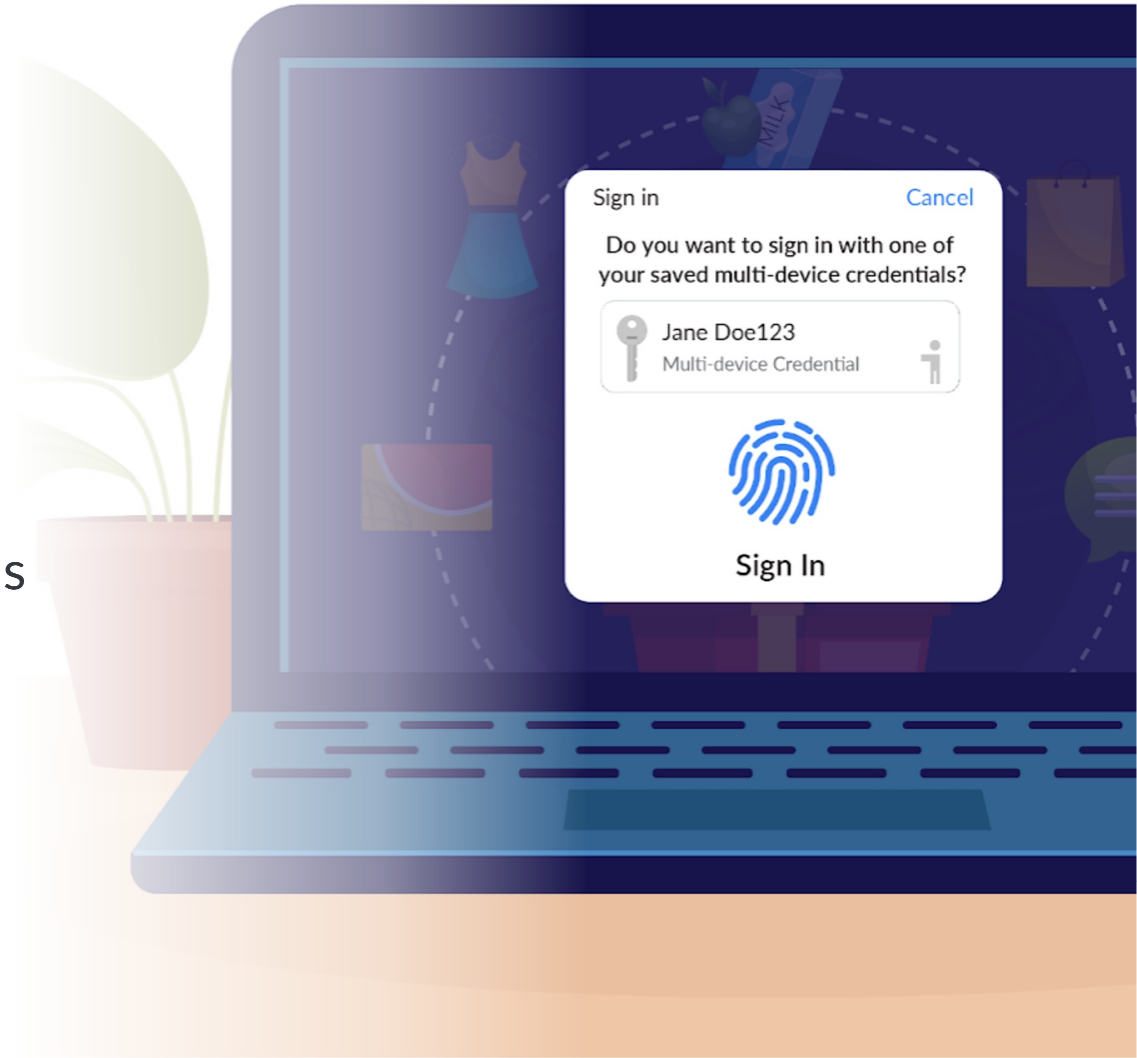
Multi-device FIDO Credentials
noun

1. *FIDO credentials that are backed up, allowing users to restore the credential to, and use it from, another device.*

CAPABILITY 1:

Sync’d FIDO credentials

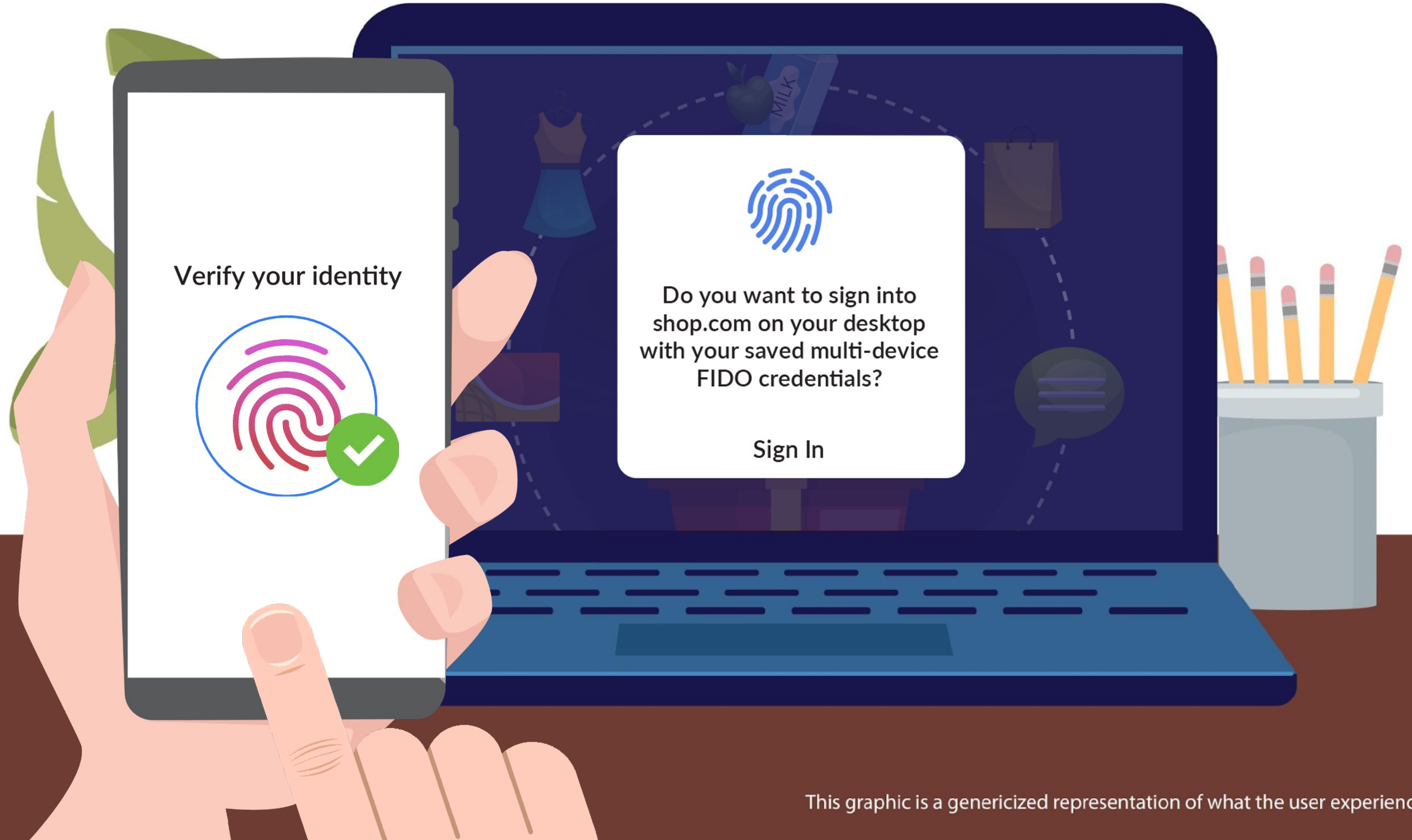
- This is the next step in the evolution of FIDO and passwordless authentication adoption
- Enables deployment of FIDO at scale to consumers moving between devices and upgrading to new ones
- Makes FIDO as ubiquitous and available as passwords
- Addresses usability AND security challenges with account recovery



Sign in
Cancel
Do you want to sign in with one of your saved multi-device credentials?
Jane Doe123
Multi-device Credential
Sign In

CAPABILITY 2:

Phone as a “roaming authenticator”


Verify your identity
Do you want to sign into shop.com on your desktop with your saved multi-device FIDO credentials?
Sign In
MILK

Proposed additions to the FIDO/WebAuthn specs define a protocol to communicate between the user’s phone (which becomes the FIDO authenticator) and the device from which the user is trying to authenticate.

This graphic is a genericized representation of what the user experience may be.

Authentication friction and excessive challenges cause abandonment and low authentication success rates

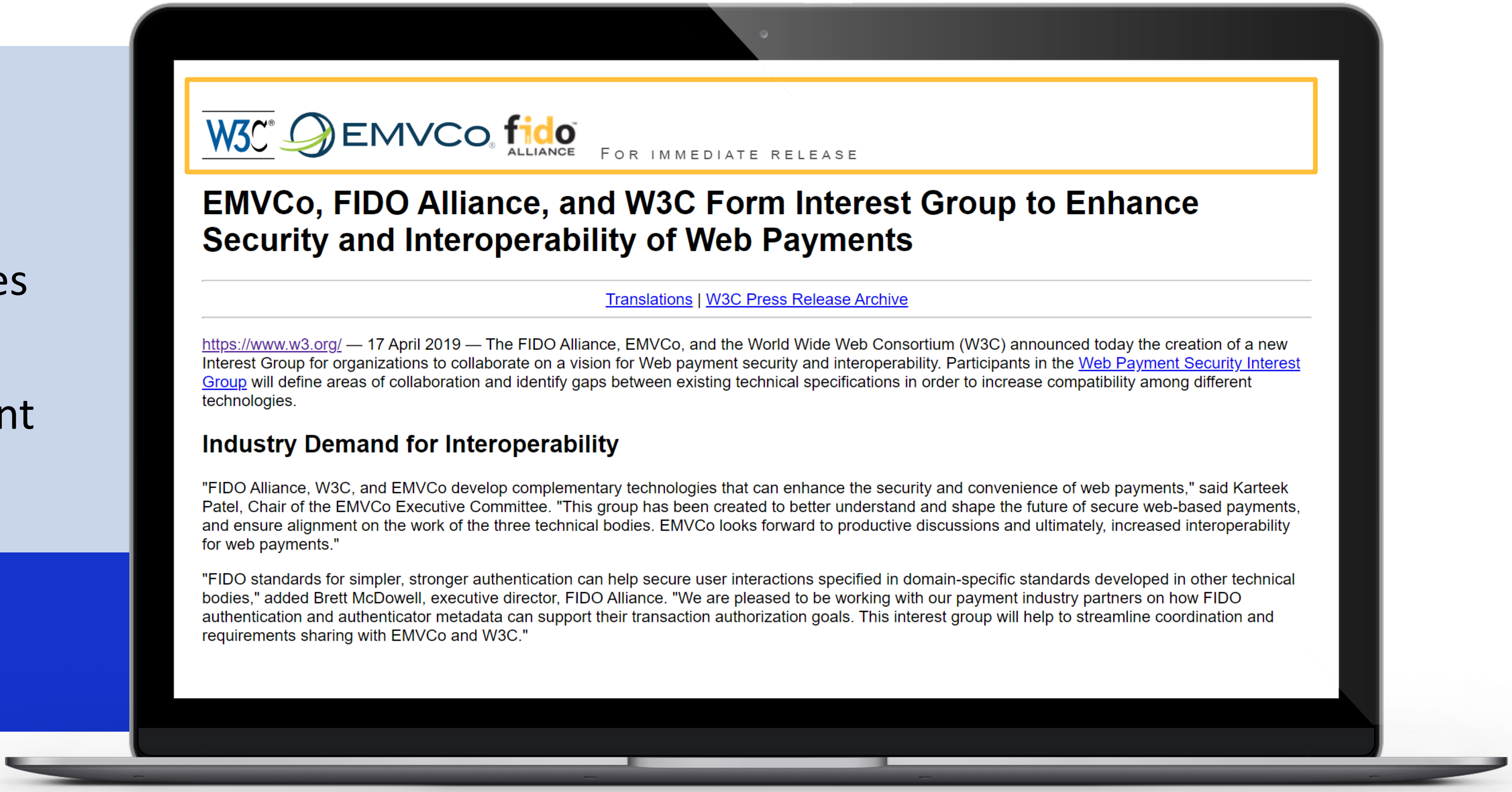
FIDO can play a key role to address these challenges

FIDO Alliance, W3C and EMVCo are collaborating to address these challenges

Key accomplishments:

- Creation of the WPSIG
- White Paper – how technologies relate
- Development of Secure Payment Confirmation

How?



EMVCo, FIDO Alliance, and W3C Form Interest Group to Enhance Security and Interoperability of Web Payments

Translations | W3C Press Release Archive

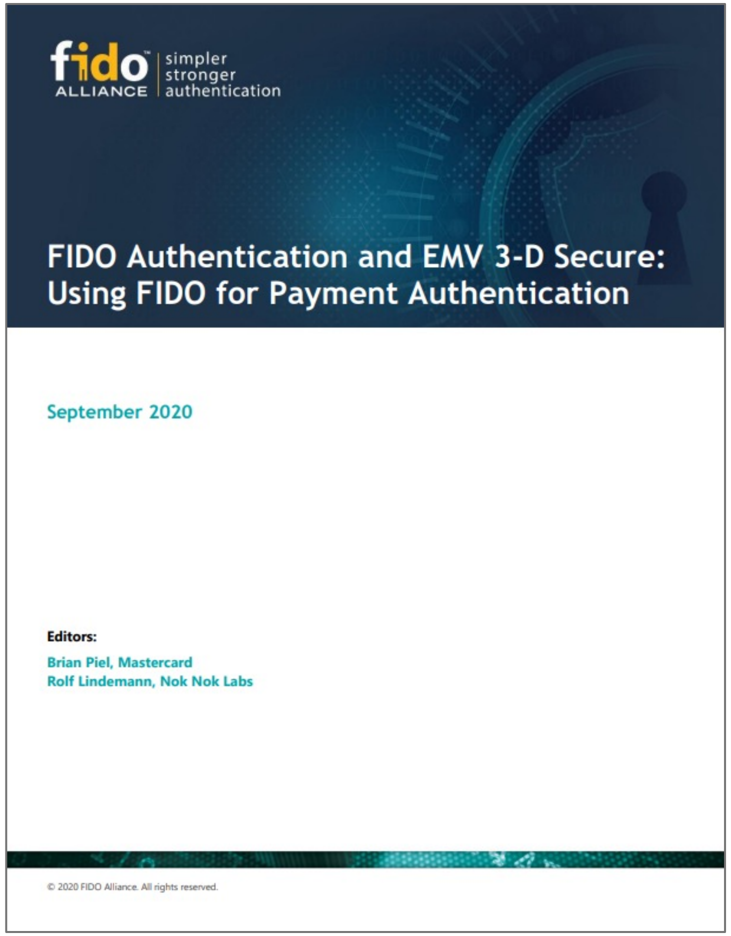
https://www.w3.org/ — 17 April 2019 — The FIDO Alliance, EMVCo, and the World Wide Web Consortium (W3C) announced today the creation of a new Interest Group for organizations to collaborate on a vision for Web payment security and interoperability. Participants in the Web Payment Security Interest Group will define areas of collaboration and identify gaps between existing technical specifications in order to increase compatibility among different technologies.

Industry Demand for Interoperability

"FIDO Alliance, W3C, and EMVCo develop complementary technologies that can enhance the security and convenience of web payments," said Karteek Patel, Chair of the EMVCo Executive Committee. "This group has been created to better understand and shape the future of secure web-based payments, and ensure alignment on the work of the three technical bodies. EMVCo looks forward to productive discussions and ultimately, increased interoperability for web payments."

"FIDO standards for simpler, stronger authentication can help secure user interactions specified in domain-specific standards developed in other technical bodies," added Brett McDowell, executive director, FIDO Alliance. "We are pleased to be working with our payment industry partners on how FIDO authentication and authenticator metadata can support their transaction authorization goals. This interest group will help to streamline coordination and requirements sharing with EMVCo and W3C."

FIDO and EMVCo White Papers



FIDO Authentication and EMV 3-D Secure: Using FIDO for Payment Authentication

September 2020

Editors:

Brian Piel, Mastercard
Rolf Lindemann, Nok Nok Labs

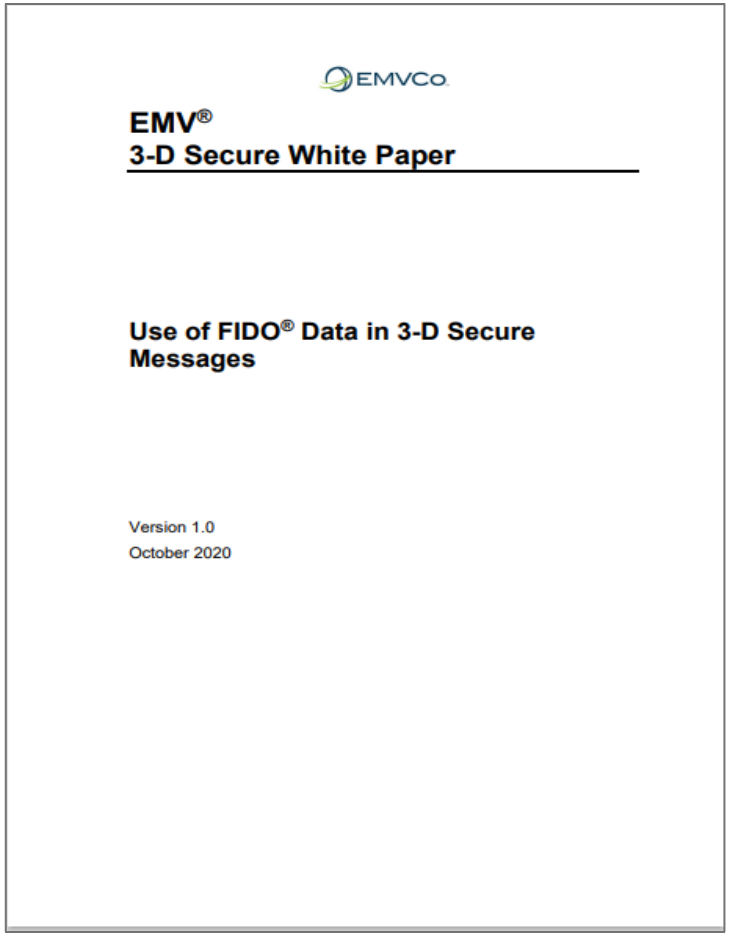
FIDO Alliance White Paper:

FIDO for SCA Delegation to Merchants or Wallet Providers

March 2021

Editors:

Jonathan Grossar, Mastercard
Alain Martin, Thales
Melanie Maier, Entersekt
Bernard Joly, OneSpan
Felix Magedanz, Hanko
Arshad Noor, StrongKey



EMV®
3-D Secure White Paper

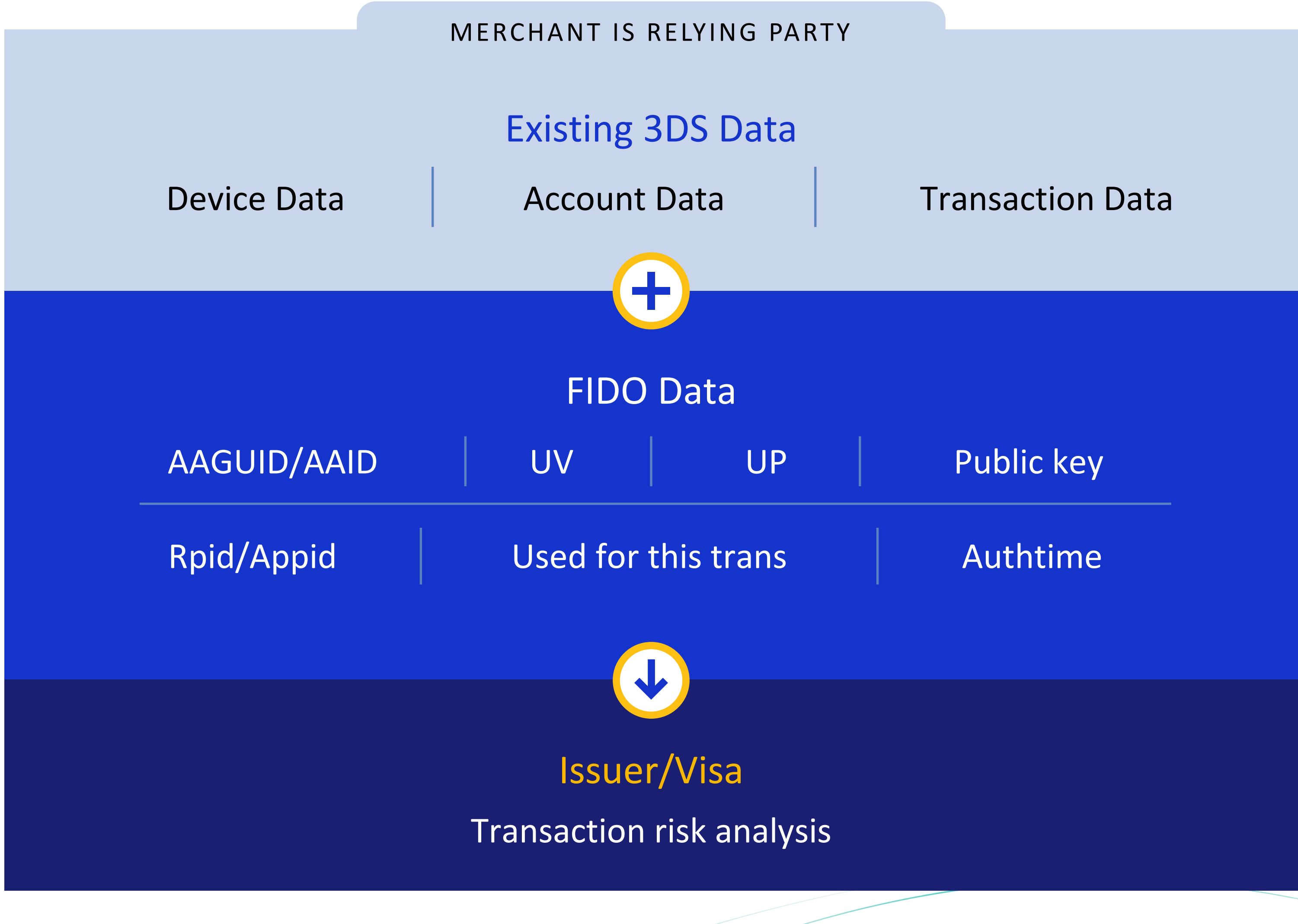
Use of FIDO® Data in 3-D Secure Messages

Version 1.0
October 2020

USE CASE # 1

FIDO-based WebAuthn invoked by merchant

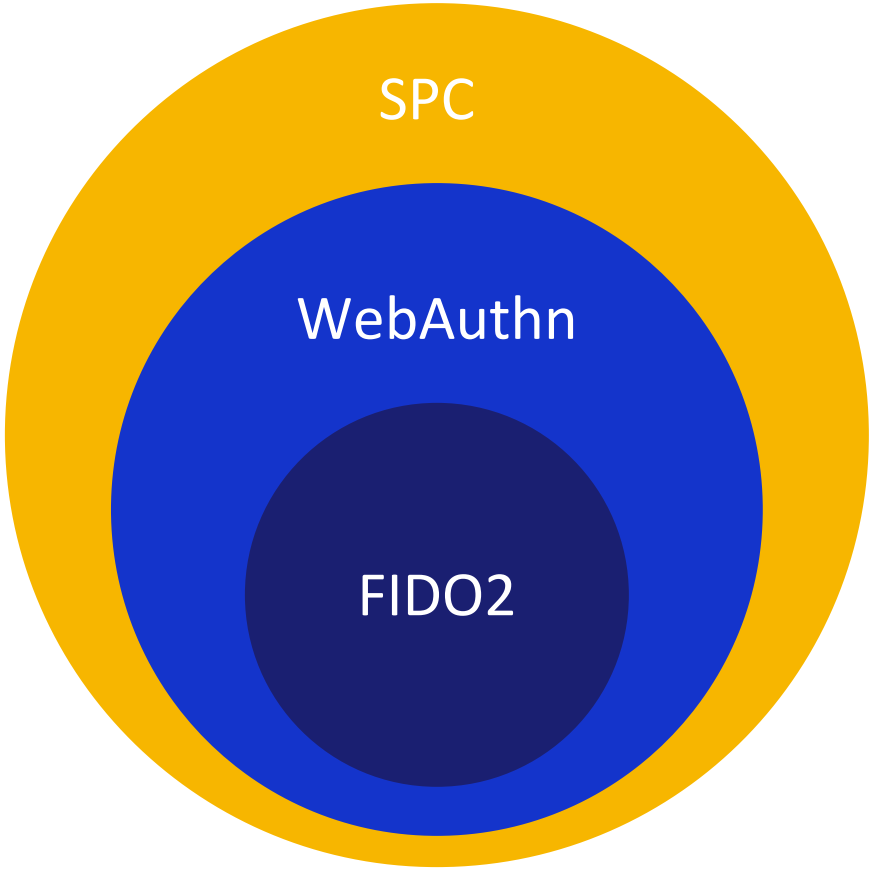
- Merchants can provide strong FIDO authentication data to enhance transaction risk analysis by the Issuer
- FIDO authentication data is communicated via existing EMV 3DS data elements
- EMVCo and FIDO Alliance defined a FIDO Alliance dataset that can be carried in 3DS messages



SPC Overview

Secure Payment Confirmation (SPC) is a web standard currently in development that is built on WebAuthn to support streamlined authentication during a payment transaction

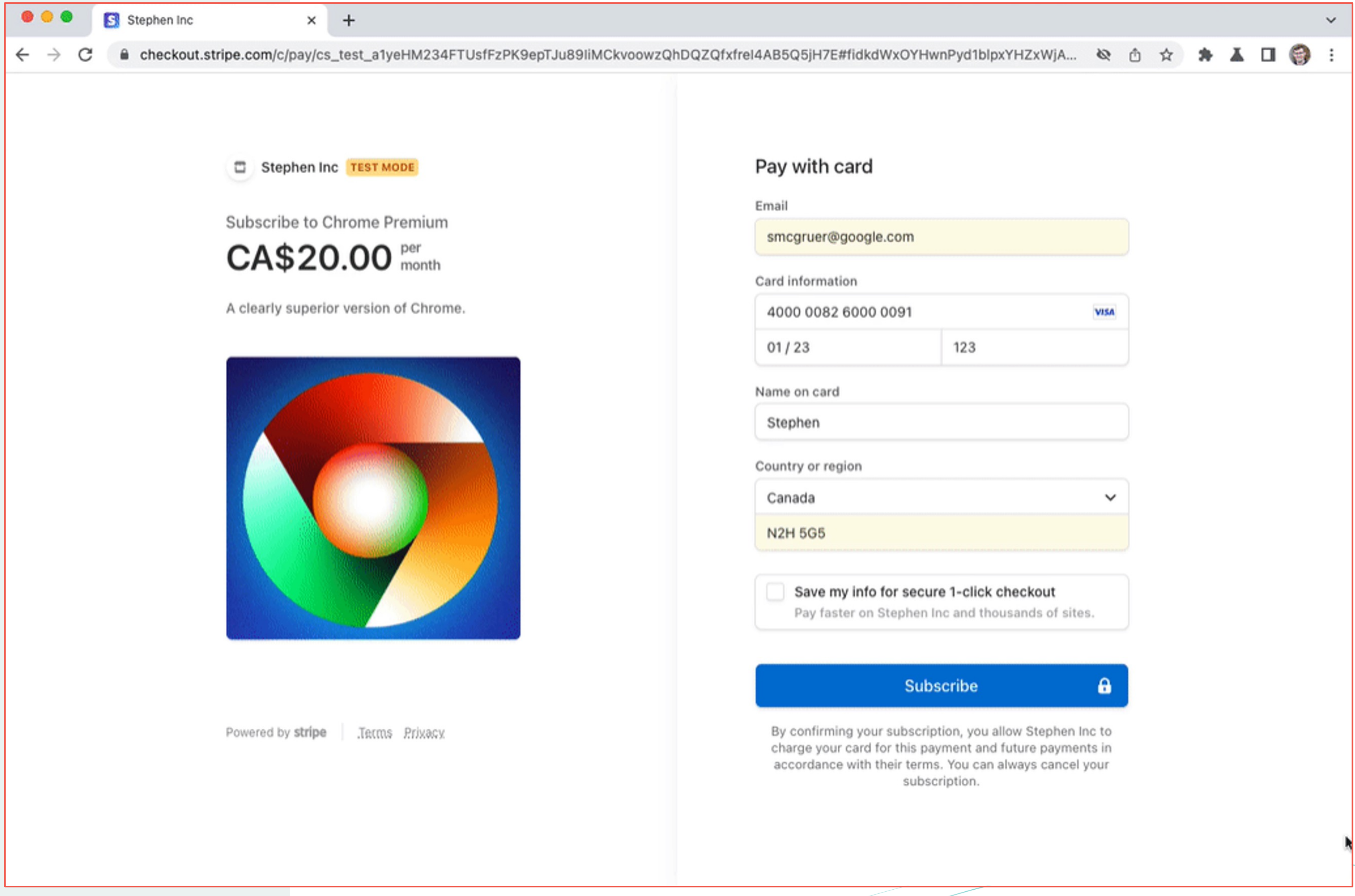
- Designed to produce cryptographic evidence that the consumer has confirmed transaction details, within a trusted platform UI, that satisfies strong authentication requirements and dynamic linking
- Increases consumer confidence with biometric verification due to the browser's ability to standardize the display and simplify the payment confirmation experience
- Cross-origin credential sharing allows any merchant supporting SPC and 3DS 2.3.1 to request a signature from the issuer's public key
- Gracefully degrades to vanilla 3DS for unenrolled users and for unsupported devices



For SPC info refer to https://www.w3.org/Payments/WG/

Secure Payment Confirmation

Seamless, FIDO-based user verification for all payment methods and all merchants.



Stephen Inc
checkout.stripe.com/c/pay/cs_test_a1yeHM234FTUsfFzPK9epTJu89IiMCkvoowzQhDQZQfxfreI4AB5Q5jH7E#fidkdWxOYHwnPyd1blpxYHZxWjA...

Stephen Inc TEST MODE

Subscribe to Chrome Premium

CA$20.00 per month

A clearly superior version of Chrome.

Powered by stripe | Terms Privacy

Pay with card

Email: smcgruer@google.com

Card information: 4000 0082 6000 0091 VISA

01 / 23 | 123

Name on card: Stephen

Country or region: Canada

N2H 5G5

□ Save my info for secure 1-click checkout
Pay faster on Stephen Inc and thousands of sites.

Subscribe

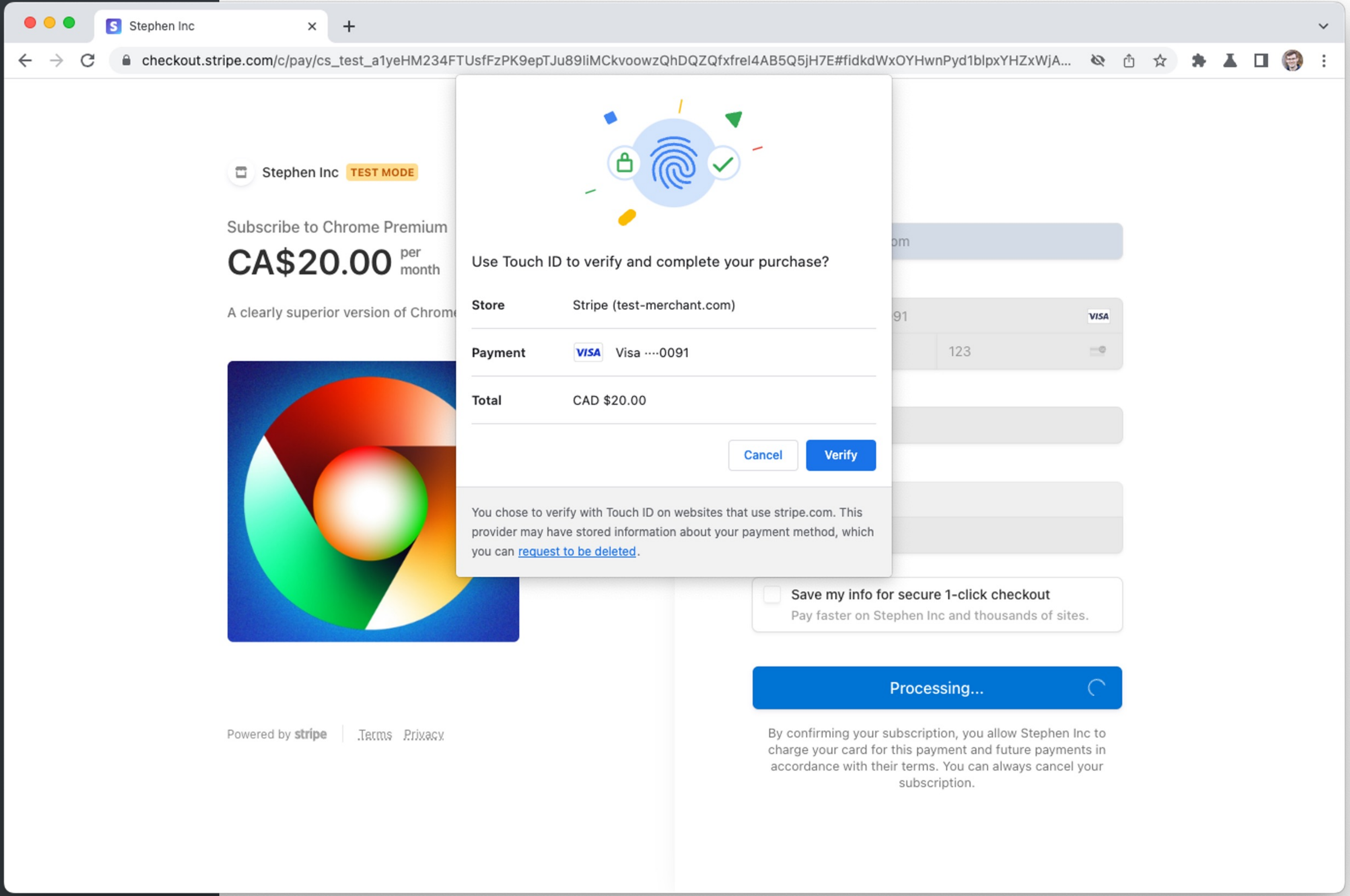
By confirming your subscription, you allow Stephen Inc to charge your card for this payment and future payments in accordance with their terms. You can always cancel your subscription.

SPC: API superpowers

Adds payments support to PublicKeyCredential

1. **Delegated exercise:** any party, not just RP, can exercise a credential[1]
2. **Dynamic linking** of transaction details into ClientDataJSON
3. **Cross-origin iframe** registration enabled

[Spec](#) [Glitch Demo](#)



Stephen Inc
checkout.stripe.com/c/pay/cs_test_a1yeHM234FTUsfFzPK9epTJu89IiMCkvoowzQhDQZQfxfrel4AB5Q5jH7E#fidkdWxOYHwnPyd1blpxYHZxWjA...

Stephen Inc TEST MODE

Subscribe to Chrome Premium

CA$20.00 per month

A clearly superior version of Chrome

Use Touch ID to verify and complete your purchase?

Store	Stripe (test-merchant.com)
Payment	VISA Visa ····0091
Total	CAD $20.00

Cancel Verify

You chose to verify with Touch ID on websites that use stripe.com. This provider may have stored information about your payment method, which you can request to be deleted.

□ Save my info for secure 1-click checkout
Pay faster on Stephen Inc and thousands of sites.

Processing...

By confirming your subscription, you allow Stephen Inc to charge your card for this payment and future payments in accordance with their terms. You can always cancel your subscription.

Powered by stripe | Terms Privacy

[1] With explicit RP opt-in during credential creation

fido ALLIANCE simpler stronger authentication

Thank you.