



FIDO Deployment Deep Dive Mobile Payments

Dr. Rolf Lindemann, Nok Nok

Background

- **About Dr. Rolf Lindemann**

- Author & contributing editor of multiple FIDO specifications
- Frequent speaker at industry events
- Helped regulators across the globe with modern authentication
- VP Products at Nok Nok

- **About Nok Nok**

- **Deep domain expertise in FIDO next-generation authentication**
 - Original inventor of FIDO and co-founder the FIDO Alliance
 - Thought leader in customer authentication with proven track record
- **Proven deployed B2C passwordless solution**
 - 100s of millions of deployed users
 - Billions of authentications
- **Proven technology with innovations based on the real world**
 - Servers deployed globally at scale



Session Overview

Objective: Demonstrate why and how FIDO-based payments lead to *increased conversion* and *reduced fraud*

Agenda:

- The Problems with Online Payments Today
- Legacy vs. Modern (FIDO) Authentication Approaches
- Payment Scenarios Leveraging FIDO
 - 3DS “challenge flow”
 - Delegated Authentication

Current Issues with Online Payments

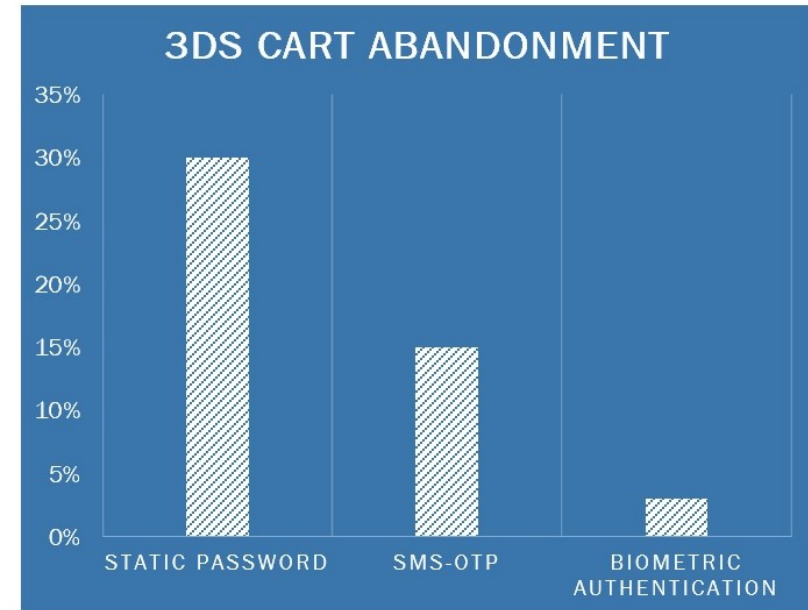
1

Conversion

Legacy Step-Up Auth Leads to High Cart Abandonment

Biometric Authentication Reduces Cart Abandonment

- Biometrics simplify checkout
- 80% reduction in cart abandonment over passwords or SMS OTP
- Less Friction is a business enabler



Source: Mastercard Study

Current Issues with Online Payments

1

Conversion

False-declines

OTP not received

Phone not in reach

Forgotten PIN

Waiting time too long

Unpredictable UX

Current Issues with Online Payments

1

Conversion

- False-declines
- OTP not received
- Phone not in reach
- Forgotten PIN
- Waiting time too long
- Unpredictable UX

2

Fraud

CNP Fraud 3X More than Card Present

Offline Card Present (CP)



Online Card Not Present (CNP)

- 3x more fraud than Card Present
- 1.8% revenue lost to fraud globally

Enter card details

Card number



Accepted credit and debit card types

Expiry date

For example, 10/20

Month Year

 /

Name on card

Card security code

The last 3 digits on the back of the card



Current Issues with Online Payments

1

Conversion

False-declines
OTP not received
Phone not in reach
Forgotten PIN
Waiting time too long
Unpredictable UX

2

Fraud

- ★ **Identity theft:** stolen cards, ...
Friendly fraud: never ordered or delivered
- ★ **Clean fraud:** variation of identity theft
Affiliate fraud: fake traffic via affiliates
Triangulation fraud: “fake shops”

Current Issues with Online Payments

1

Conversion

Example

eCommerce revenue = \$10m

Payment conversion: 78%

Revenue lost: \$2.2m

Gross Margin: 40%

Money lost: \$880k

2

Fraud

Example

eCommerce revenue = \$10m

Online payment fraud: 1.8%

Payments lost: \$180k

Add'l. loss per \$1 chargeback: \$2.94

Money lost: \$180k + \$529k = \$709k

Current Issues with Online Payments

1

Conversion

2

Fraud

Both issues have similar relevance
(for merchants)!

Current Issues with Online Payments

1

Conversion

2

Fraud

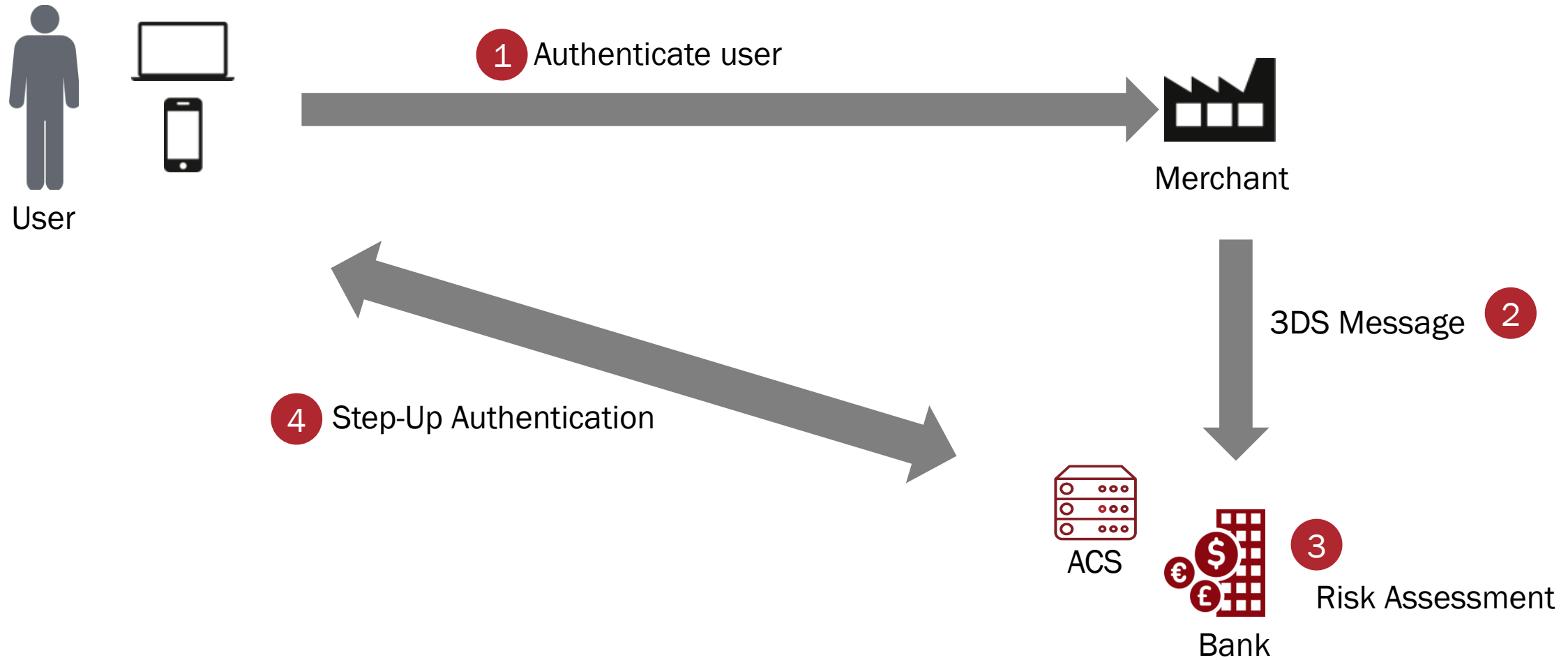
Both issues have similar relevance
(for merchants)!

Focus on
Payment
Auth UX

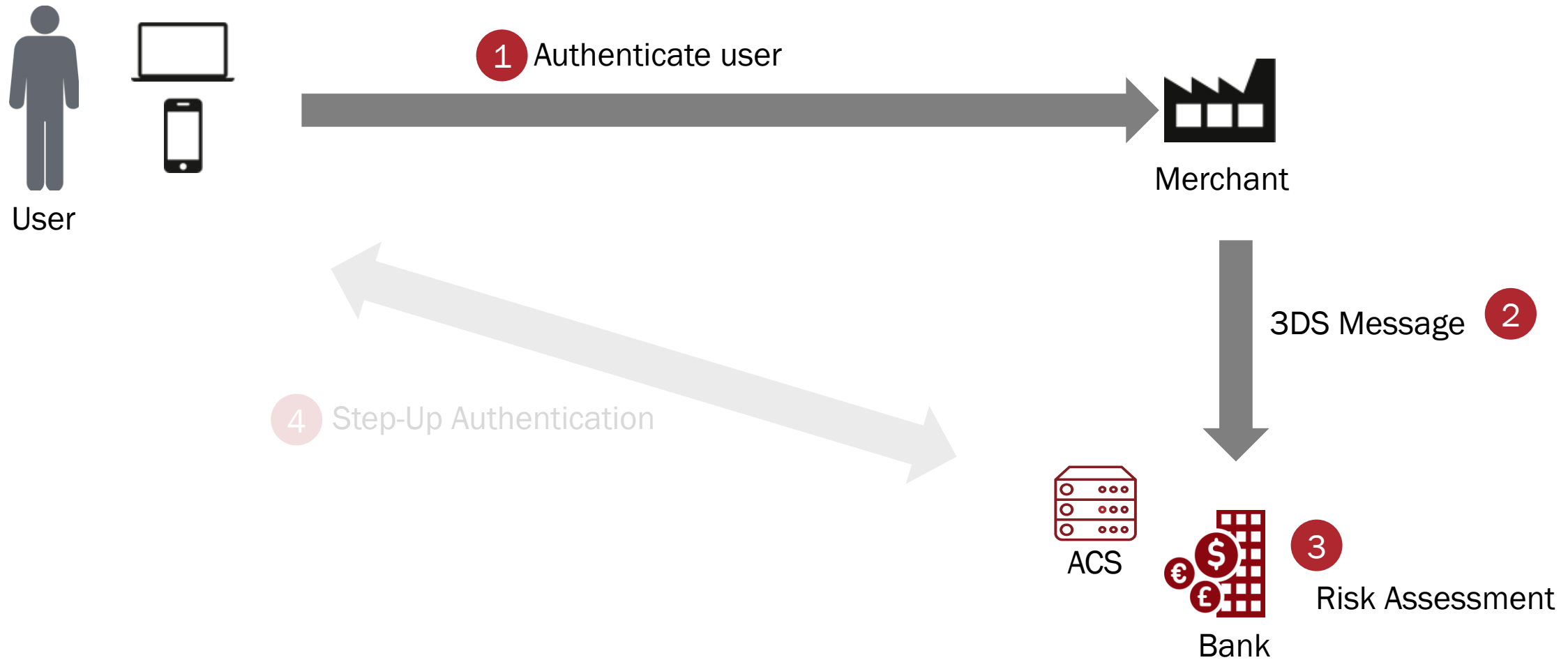
Focus on
CNP Specific
Fraud

Legacy vs. Modern (FIDO) Approaches

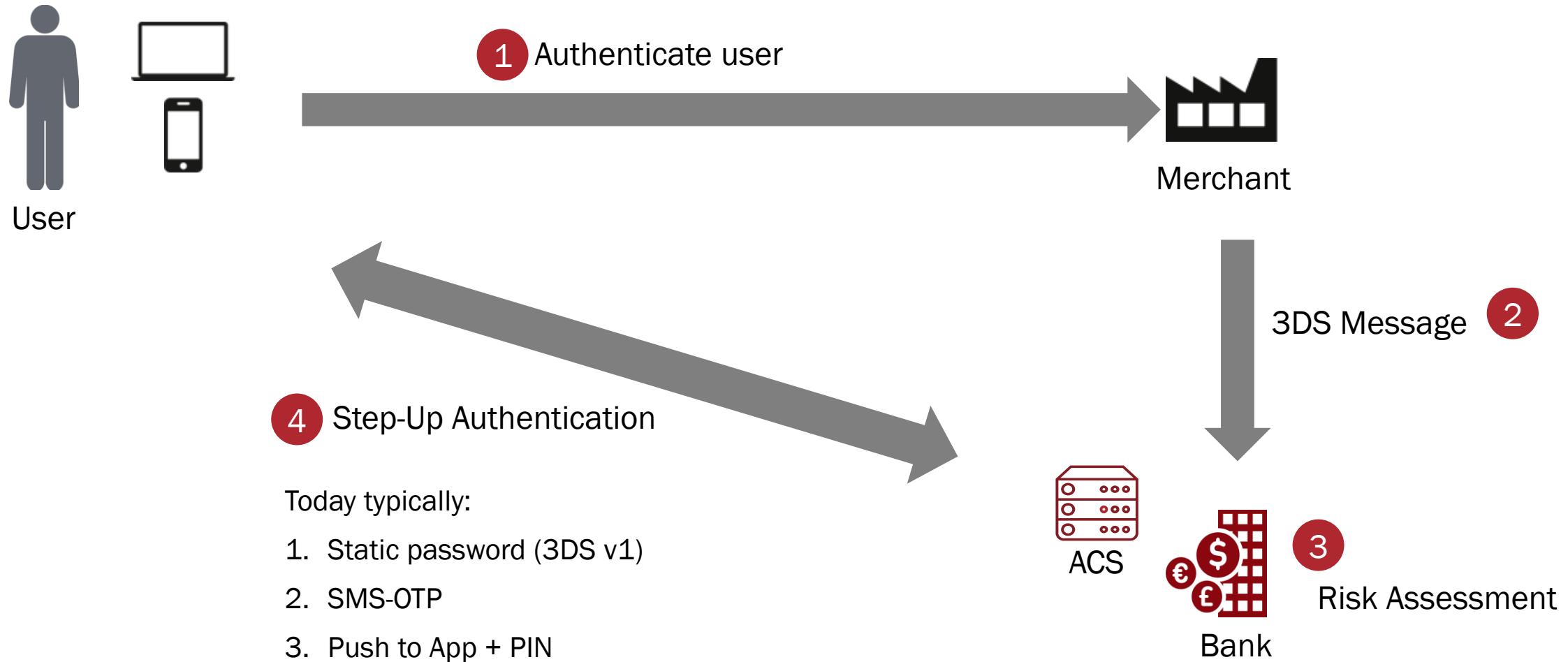
3DS Overview



3DS Overview



3DS Overview



Legacy Methods: Under the Hood

Password

OTP

Device Data

ONLINE CONNECTION

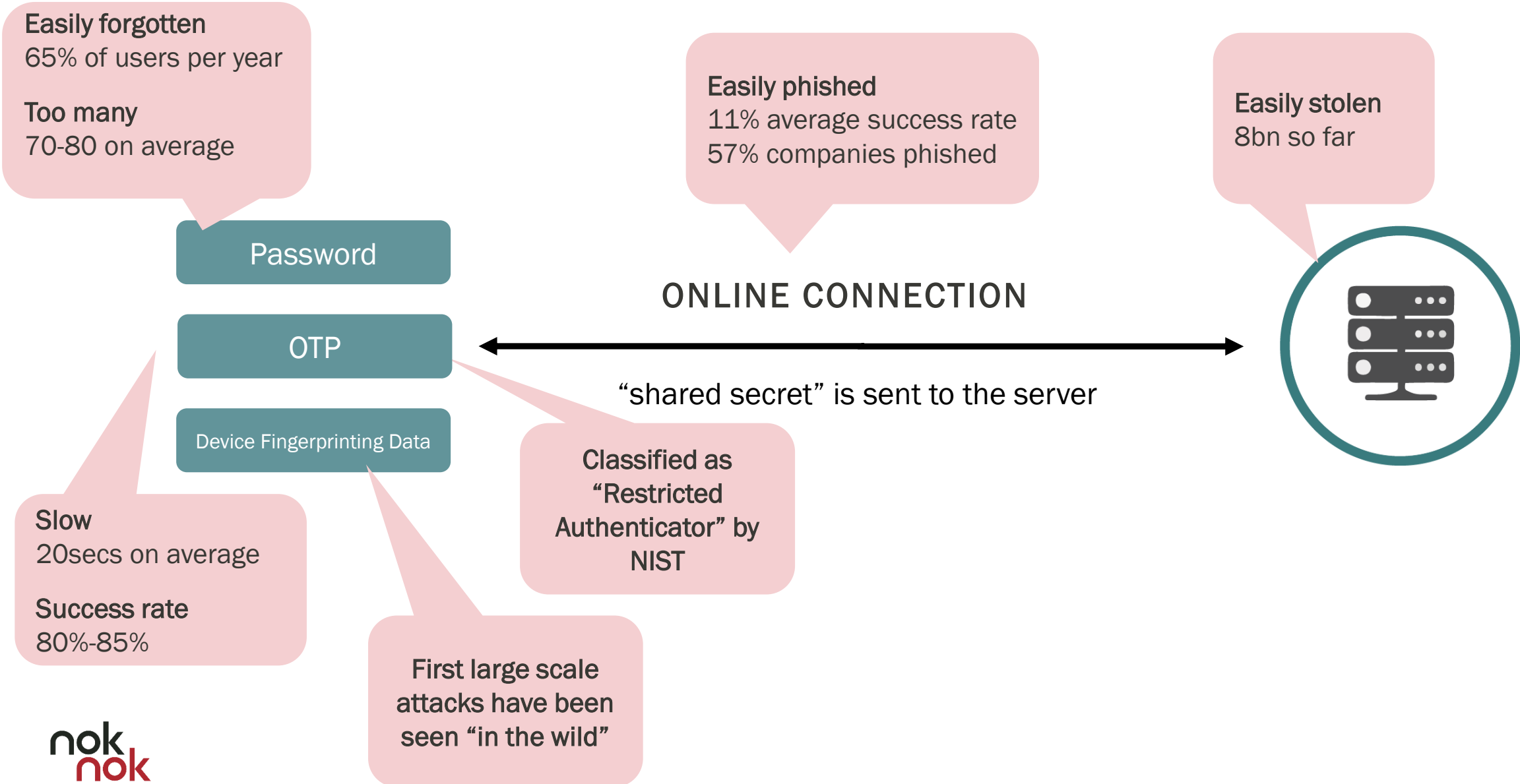


“shared secret” is sent to the server

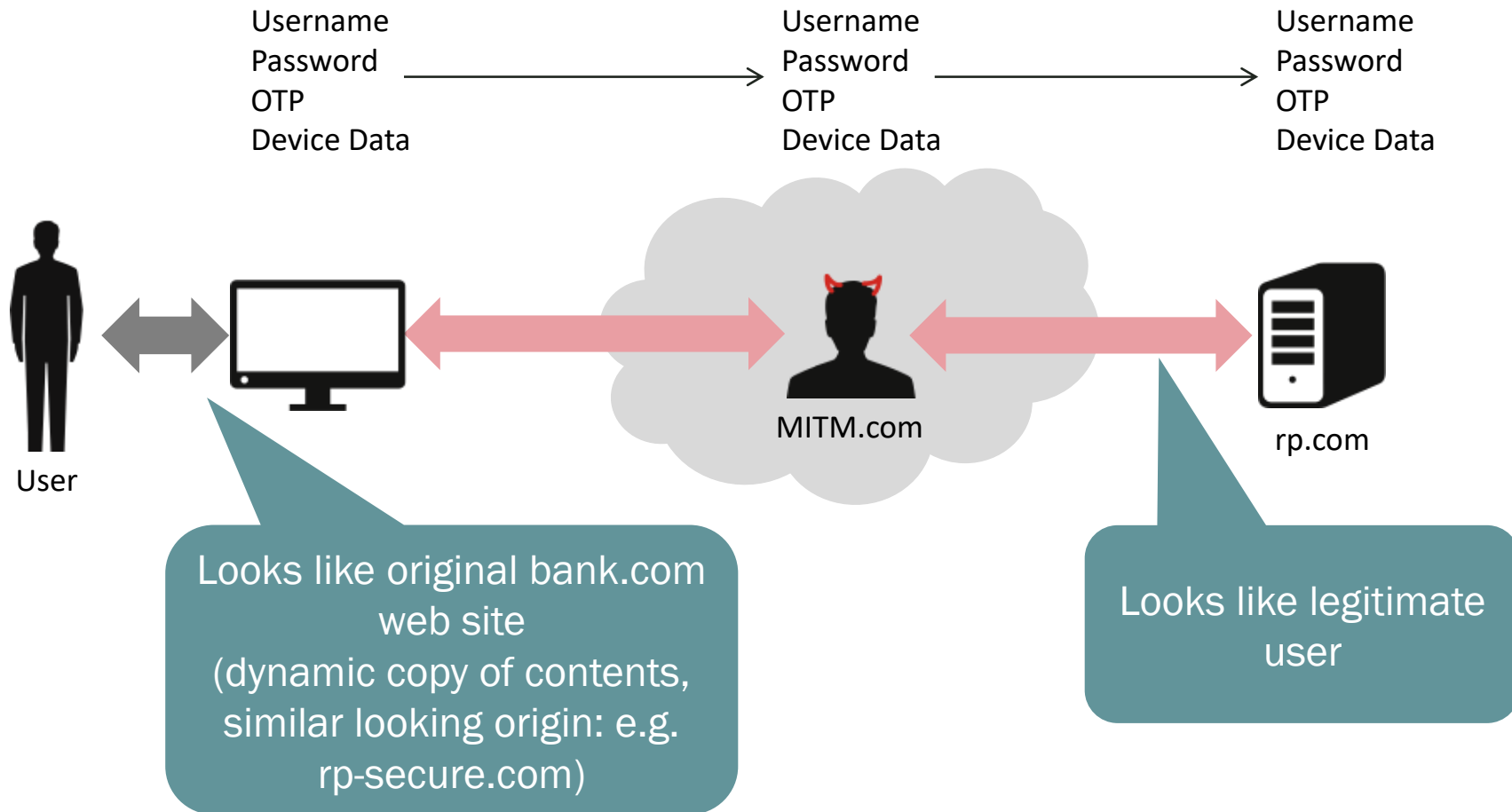
Centrally Stored Passwords



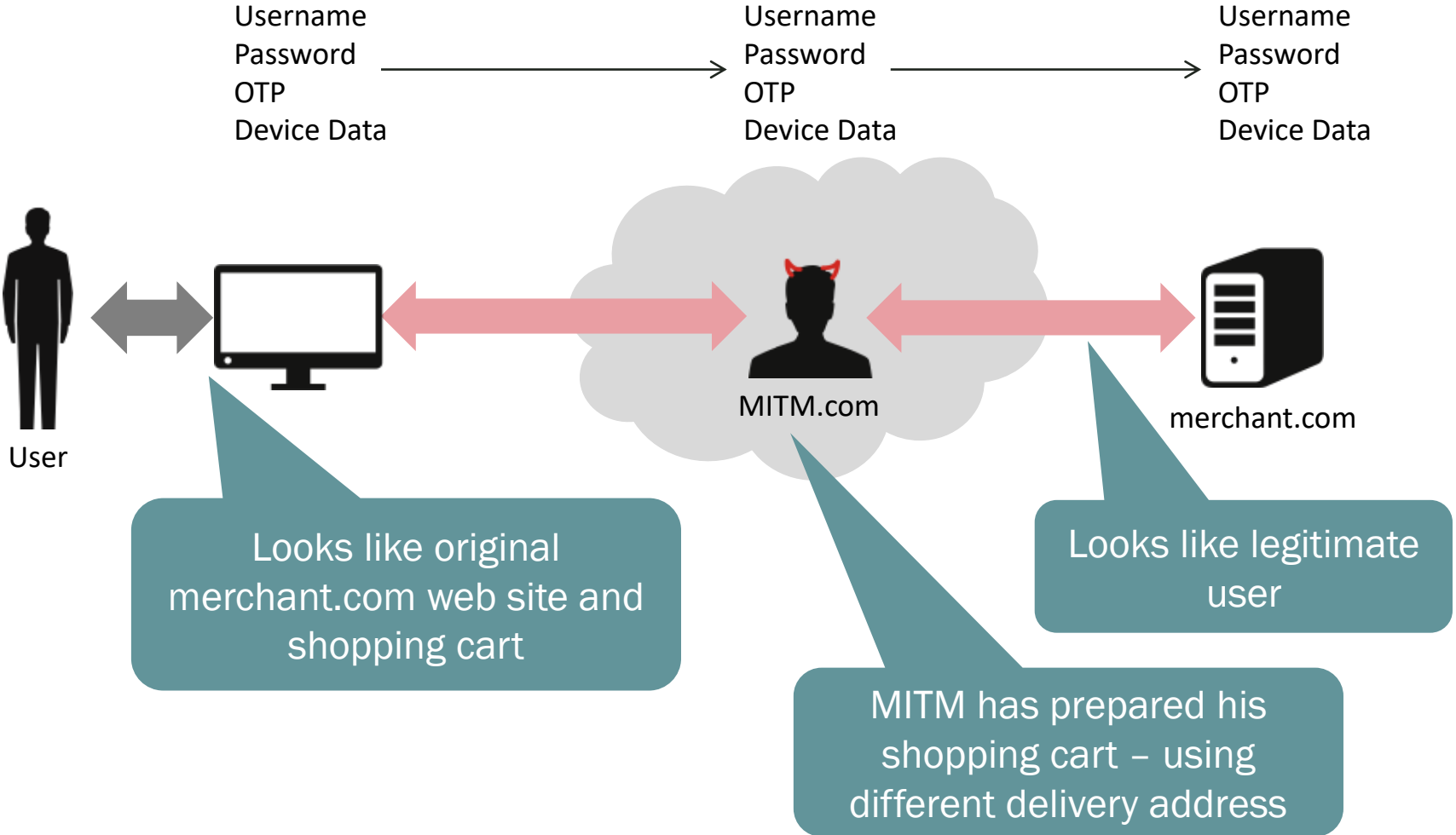
Legacy Methods: Under the Hood



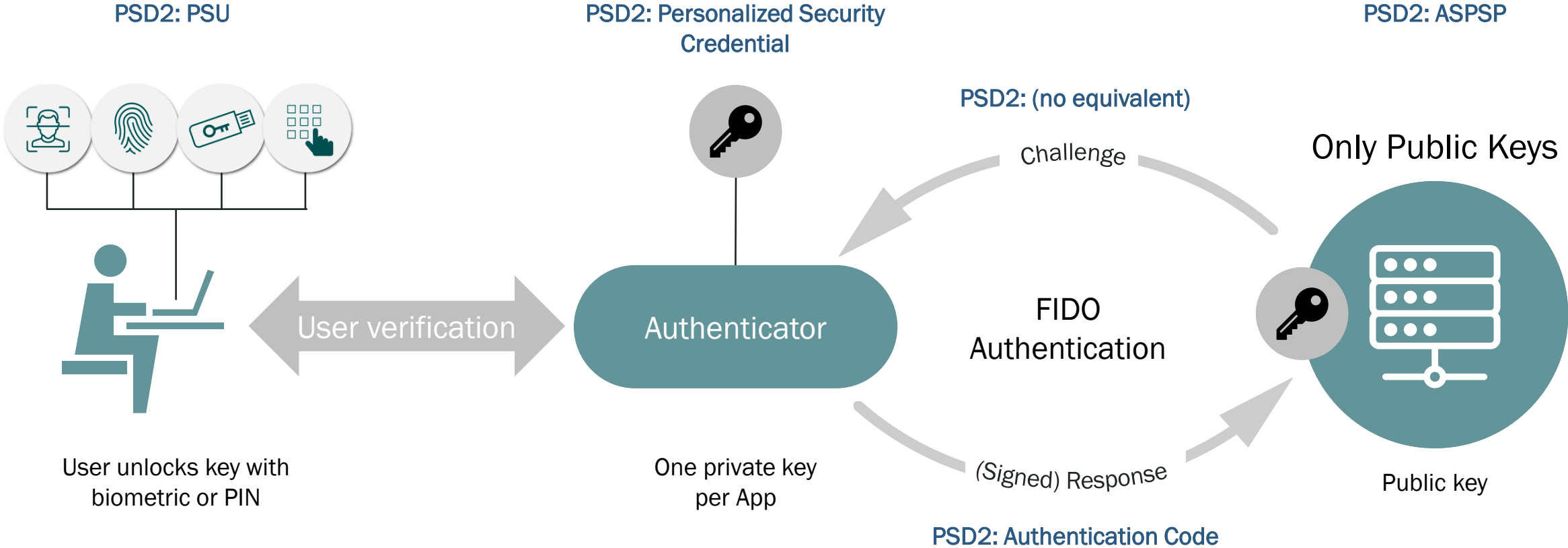
Bearer Tokens Vulnerable to MITM Attacks



Example for MITM Attack on Shopping

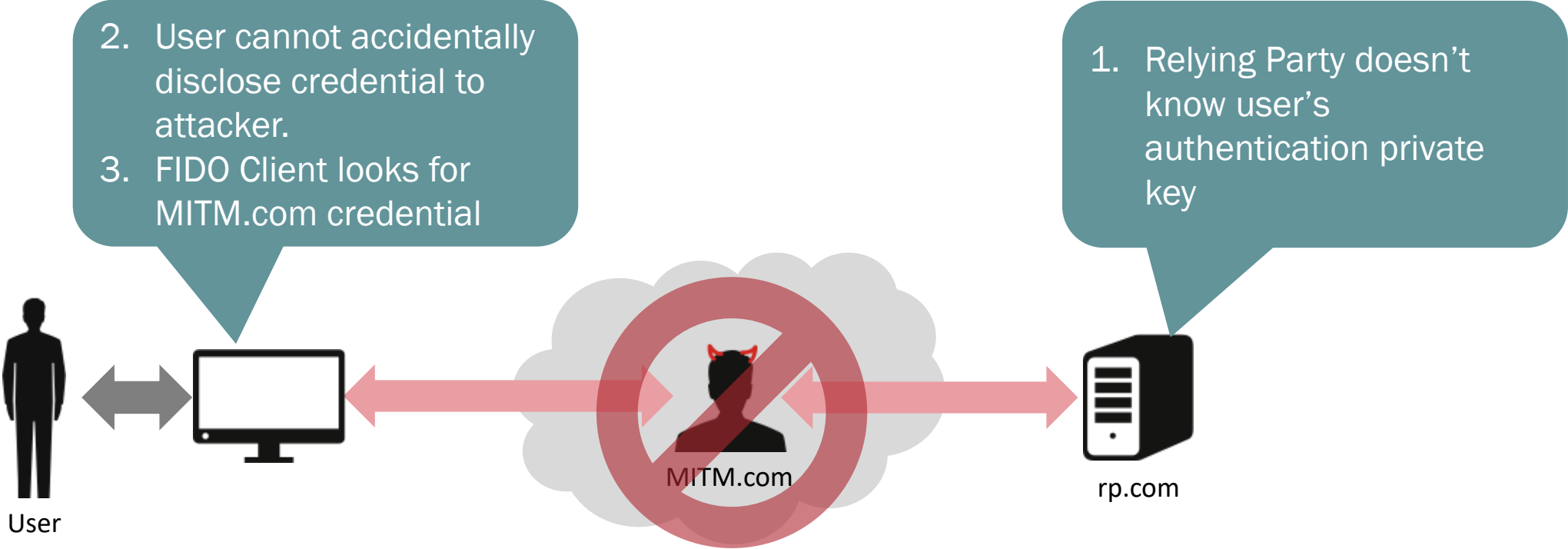


FIDO: Under the Hood

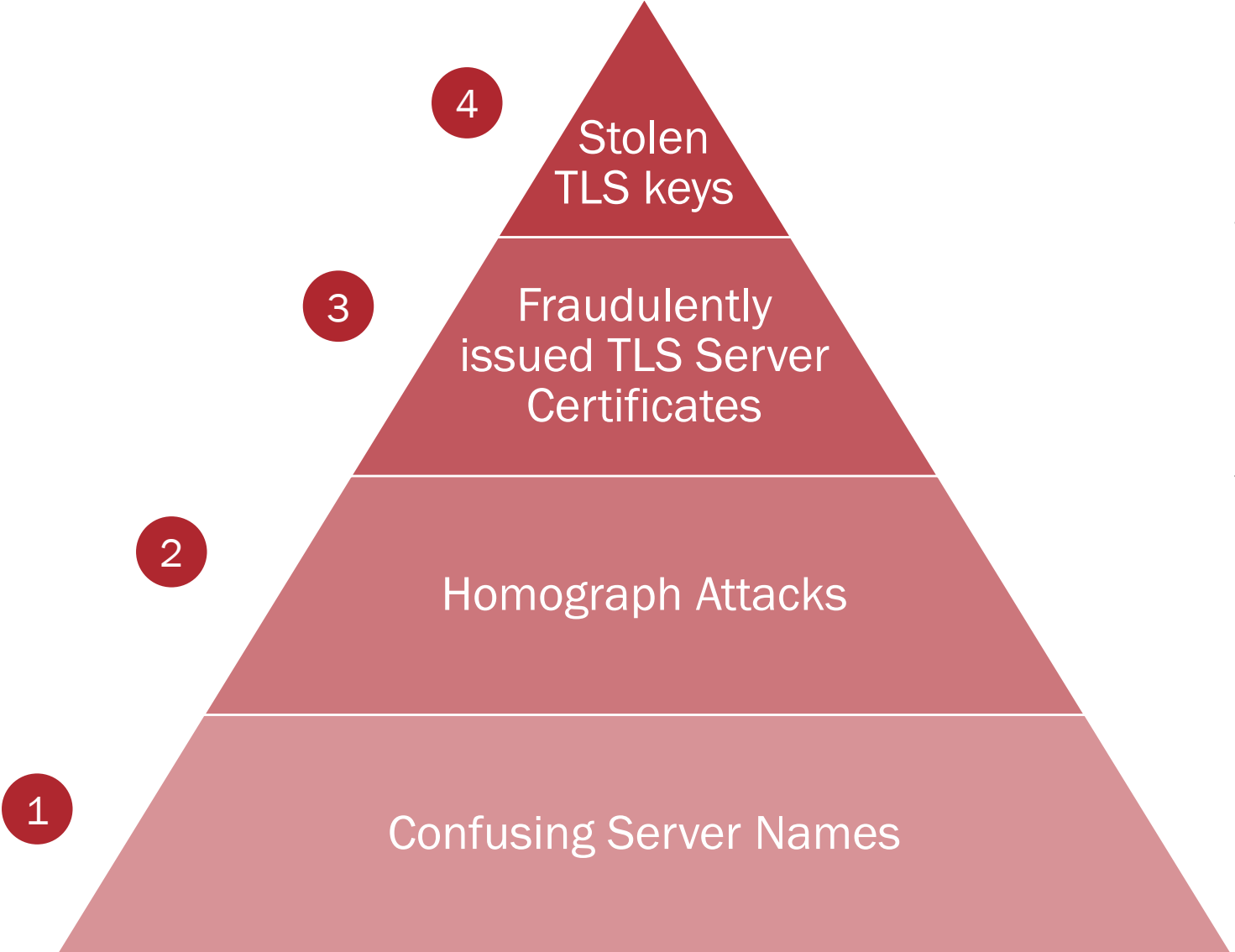


Key Pairs replace legacy shared secrets

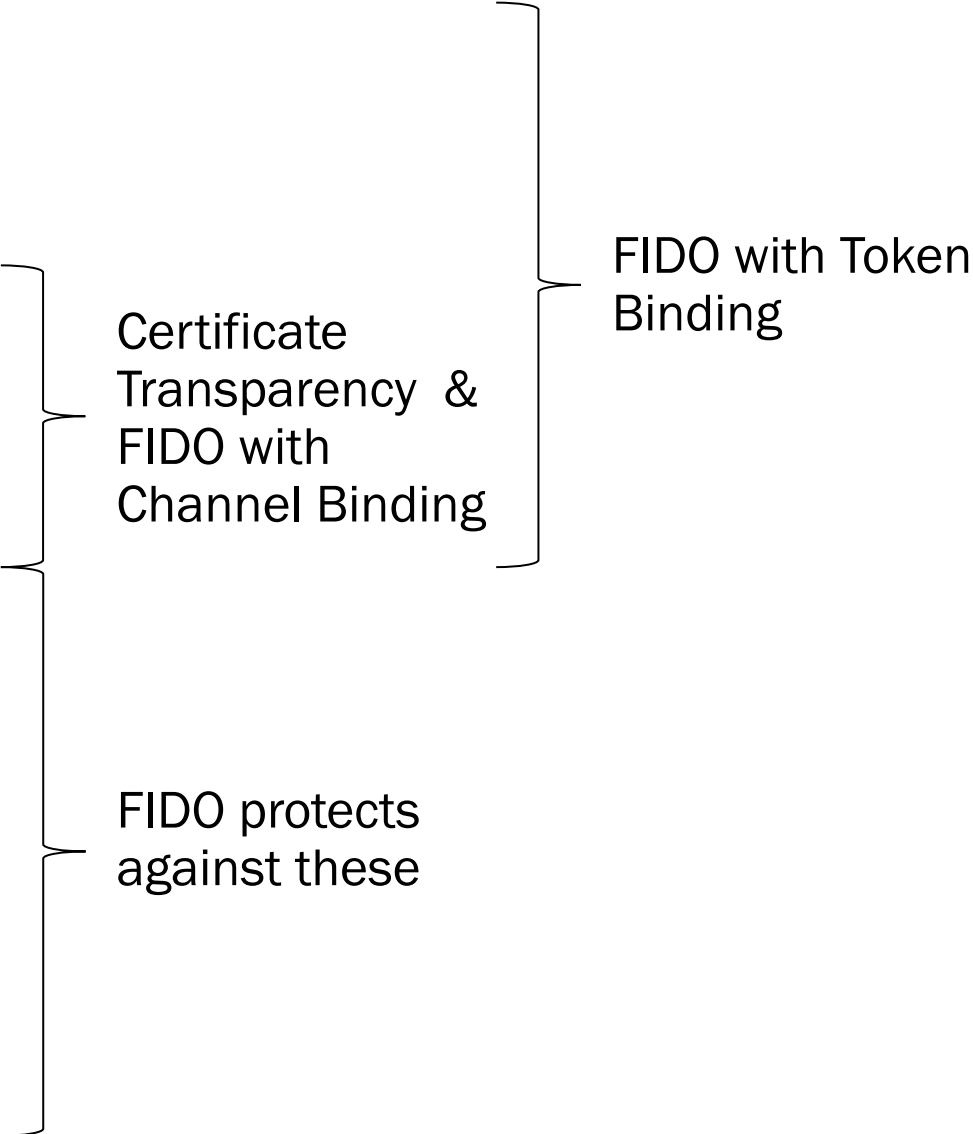
FIDO Protects Against MITM attacks



MITM Attack Levels



Counter-Measures



A person in a dark suit and tie is holding a tablet computer. The tablet screen displays a glowing blue globe with white data lines and a red-to-blue gradient background. The person is standing in front of a city skyline at dusk or dawn.

Payment Scenarios Leveraging FIDO

Authenticator Form Factors

Typical Modalities

Platform Authenticators

Authenticator is an integral part of a multi-functional device



Roaming Authenticators

Authenticator is a dedicated security device – typically supporting USB, NFC and/or BLE.



Payment Scenarios

- **3DS with Biometric Challenge Flow**

1. Browser and Push-OOB to smartphone App
2. Browser WebAuthn (cross-origin-iframe)
3. Secure Payment Confirmation (SPC)

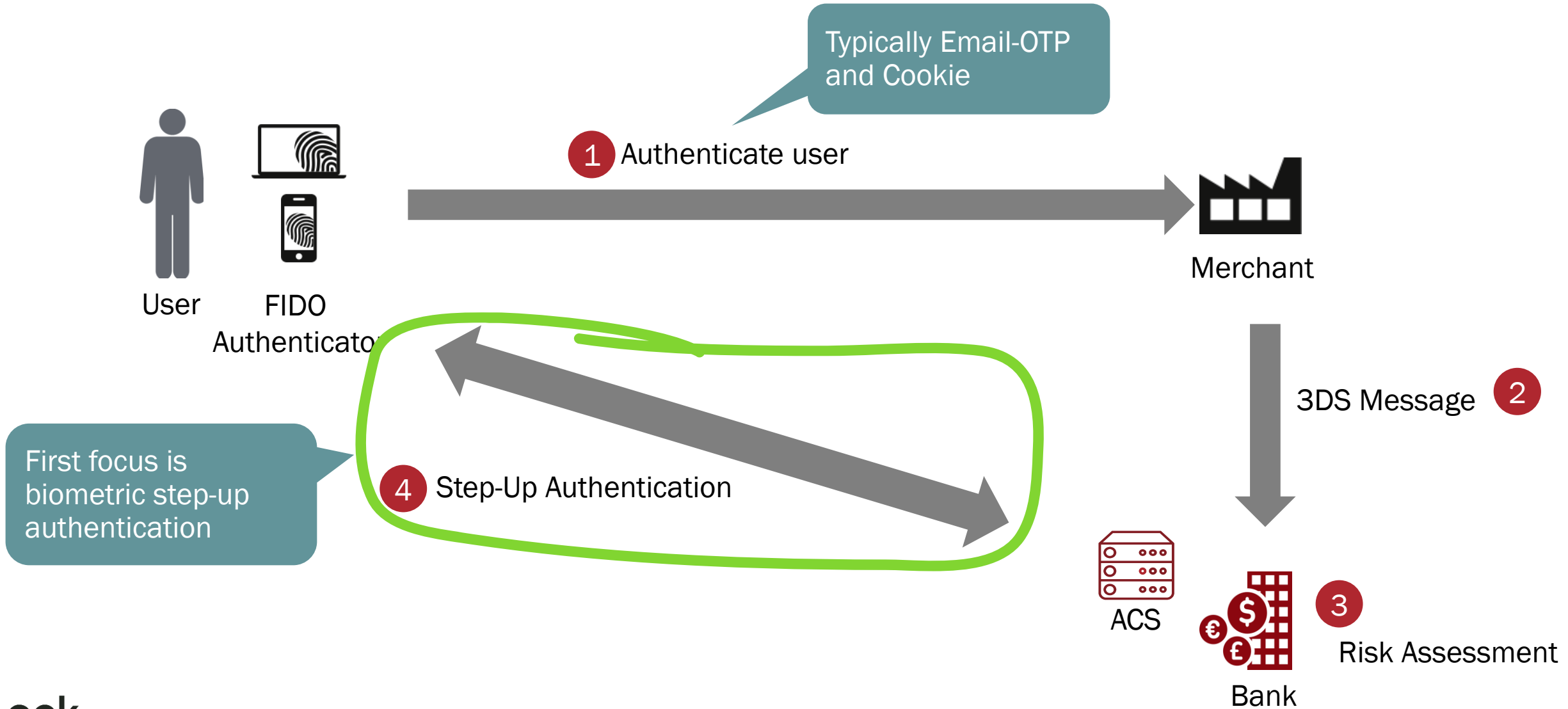
- **Delegated Authentication**

0. Enablement
1. First Purchase
2. Second Purchase
 1. Browser WebAuthn
 2. Secure Payment Confirmation (SPC)



Using FIDO authentication

3DS with Biometric Challenge Flow






1. Browser and Push-OOB to App

ShopAuth x +

← ↻ 🔒 https://shopauth.noknokdemo.com 🔊 ★ ⚙️ 📦 👤 ⋮

☰ **nok nok** 🔍 🛒 [Sign In](#)




Drone 1 The Best

★★★★★ 523

\$ 750.00

Free shipping on orders over \$199

[Details](#)




Droney 23 Take Me

★★★★ 69

\$ 199.00

Free shipping on orders over \$199

[Details](#)



Drohne 7 Heavyliifter

★★★★★ 307

\$ 530.00


Free shipping on orders over \$199

[Details](#)

ShopAuth x +

https://shopauth.noknokdemo.com/details.html

☰ nok nok 🔍 🛒 Sign In



Drone 1 The Best

BLUE & WHITE

★★★★★ 523


\$750.00

[ADD TO CART](#)

Hyperloop delivery from San Francisco

Description


This is the drone you've been waiting for. This drone is fully loaded with high-performance automations like Auto Launch, Auto Hover, and Auto Land. Eliminate the learning curve and fly like a Pro right out of the box! The



ShopAuth x +

← ↻ 🔒 https://shopauth.noknokdemo.com/details.html 🔊 ☆ ⌵ 🗑️ 👤 ⋮

☰ **nok nok** 🔍 🛒 1 [Sign In](#)



Drone 1 The Best

BLUE & WHITE

★★★★★ 523


\$750.00

[ADD TO CART](#)

Hyperloop delivery from San Francisco

Description

This is the drone you've been waiting for. This drone is fully loaded with high-performance automations like Auto Launch, Auto Hover, and Auto Land. Eliminate the learning curve and fly like a Pro right out of the box! The



ShopAuth x +

https://shopauth.noknokdemo.com/cart.html

Sign In

Double check your order details

Shipping Information

Elena Molinero

Calle Puente Grau 300, Arequipa 04000 Peru

3439875075651058

[Save Payment Information](#)

Enables Delegated Authentication

Item(s) total	\$750.00
Shipping	\$0
Sales tax	67.50
Order total (1 item)	\$817.50

[Place your order](#)

By clicking Place your order, you agree to Dronz' Shop Terms of Use and Privacy Policy

The screenshot shows a web browser window with the following details:

- Browser tab: ShopAuth
- Address bar: <https://shopauth.noknokdemo.com/cart.html>
- Page header: noknok logo, search icon, cart icon, and Sign In link.
- Main heading: Double check your order details
- Section: Shipping Information
- Payment modal: A white dialog box with the text "Authorize \$817.50 payment?" and two red buttons labeled "Authorize" and "Decline".
- Order summary table:

Item(s) total	Price
Item(s) total	\$750.00
Element	\$0
Call	67.50
Order total (1 item)	\$817.50

Below the table, there is a blue button labeled "Save Payment Information" with the text "Enables Delegated Authentication" underneath it. To the right, there is a yellow button labeled "Place your order" with the text "By clicking Place your order, you agree to Dronz' Shop Terms of Use and Privacy Policy" below it.

The screenshot shows a web browser window with the following details:

- Browser Tab:** ShopAuth
- Address Bar:** <https://shopauth.noknokdemo.com/cart.html>
- Page Header:** Includes the 'nok nok' logo, a search icon, a shopping cart icon, and a 'Sign In' link.
- Main Content:**
 - Section Header:** Double check your order details
 - Shipping Information:** A form with a text input containing '3439875075651058' and a 'Save Payment Information' button. Below the button is the text 'Enables Delegated Authentication'.
 - Order Summary:**

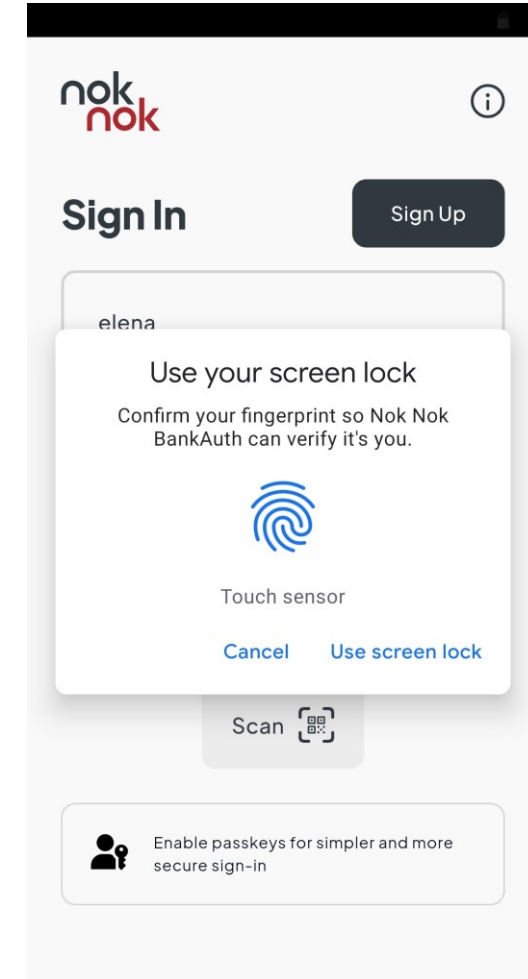
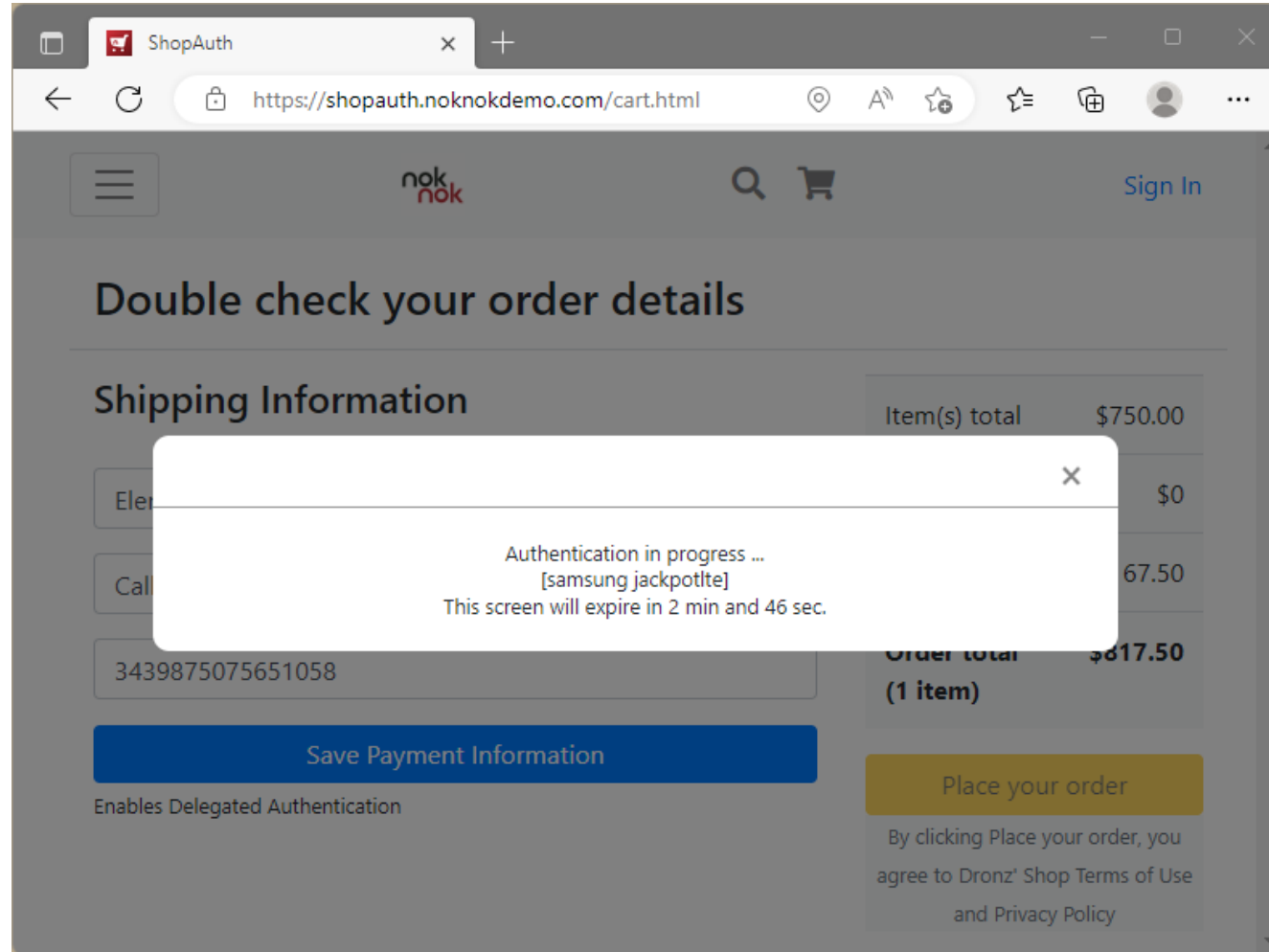
Item(s) total	\$750.00
Element	\$0
Call	67.50
Order total (1 item)	\$817.50
 - Buttons:** A blue 'Save Payment Information' button and a gold 'Place your order' button.
 - Disclaimer:** Below the 'Place your order' button, it says: 'By clicking Place your order, you agree to Dronz' Shop Terms of Use and Privacy Policy'.

Authentication Overlay: A white modal box is centered on the screen with the following text:
Authentication in progress ...
[samsung jackpotlte]
This screen will expire in 2 min and 46 sec.

The screenshot shows a web browser window with the address bar displaying `https://shopauth.noknokdemo.com/cart.html`. The page header includes the 'nok nok' logo, a search icon, a shopping cart icon, and a 'Sign In' link. The main content area features the heading 'Double check your order details' and a 'Shipping Information' section. A white modal overlay is centered on the screen, containing the text: 'Authentication in progress ... [samsung jackpotlte] This screen will expire in 2 min and 46 sec.' The background page shows a table of items with a total of \$817.50 and a 'Place your order' button.

Item(s) total	Price
Item(s) total	\$750.00
Element	\$0
Call	67.50
Order total (1 item)	\$817.50

The screenshot shows a mobile banking app interface. At the top, the status bar displays the time 13:37 and various icons. The app header is 'Nok Nok BankAuth'. The main content area displays the text 'Authorize \$817.50 payment?'. At the bottom, there are two orange buttons: 'Authorize' and 'Decline'. The bottom of the screen shows the standard Android navigation bar with three icons.



ShopAuth x +

← ↻ 🔒 https://shopauth.noknokdemo.com/order-complete.html 🔍 ☆ ⌘ 👤 ⋮

☰ **nok nok** 🔍 🛒 [Sign In](#)

Thank you for shopping with us, Elena Molinero.
We hope to see you again soon!

Order No.	#10723
-----------	--------

Total:	\$817.50
--------	----------

Shipping to

Calle Puente Grau 300, Arequipa
04000 Peru

Scenario Summary – Browser & Push-OOB

Transaction display	FIDO Client (embedded in App) – privileged to use credential
Transaction detail linked ¹ to authentication code ²	Transaction text hash is part of assertion signature (FIDO UAF Transaction Confirmation)
Credential type	Single device credential – cannot be exported from device
Authentication factors ³	Possession of authenticator (TEE backed) + user verification
Transaction text appearance	Text and / or image – up to full screen
Devices required	2
MITM protection	Yes, if user verifies transaction text
Additional user interaction	Use second (OOB) device
Notes	Requires native mobile app, broadest device coverage

¹ See PSD2 RTS Article 9 “Independence of Elements”

² PSD2 term for the FIDO assertion is “authentication code”

³ See PSD2 RTS Article 5 “dynamic linking”



2. Browser (iframe)

ShopAuth x +

https://shopauth.noknokdemo.com/cart.html

Sign In

Double check your order details

Shipping Information

Elena Molinero

Calle Puente Grau 300, Arequipa 04000 Peru

3439875075651058

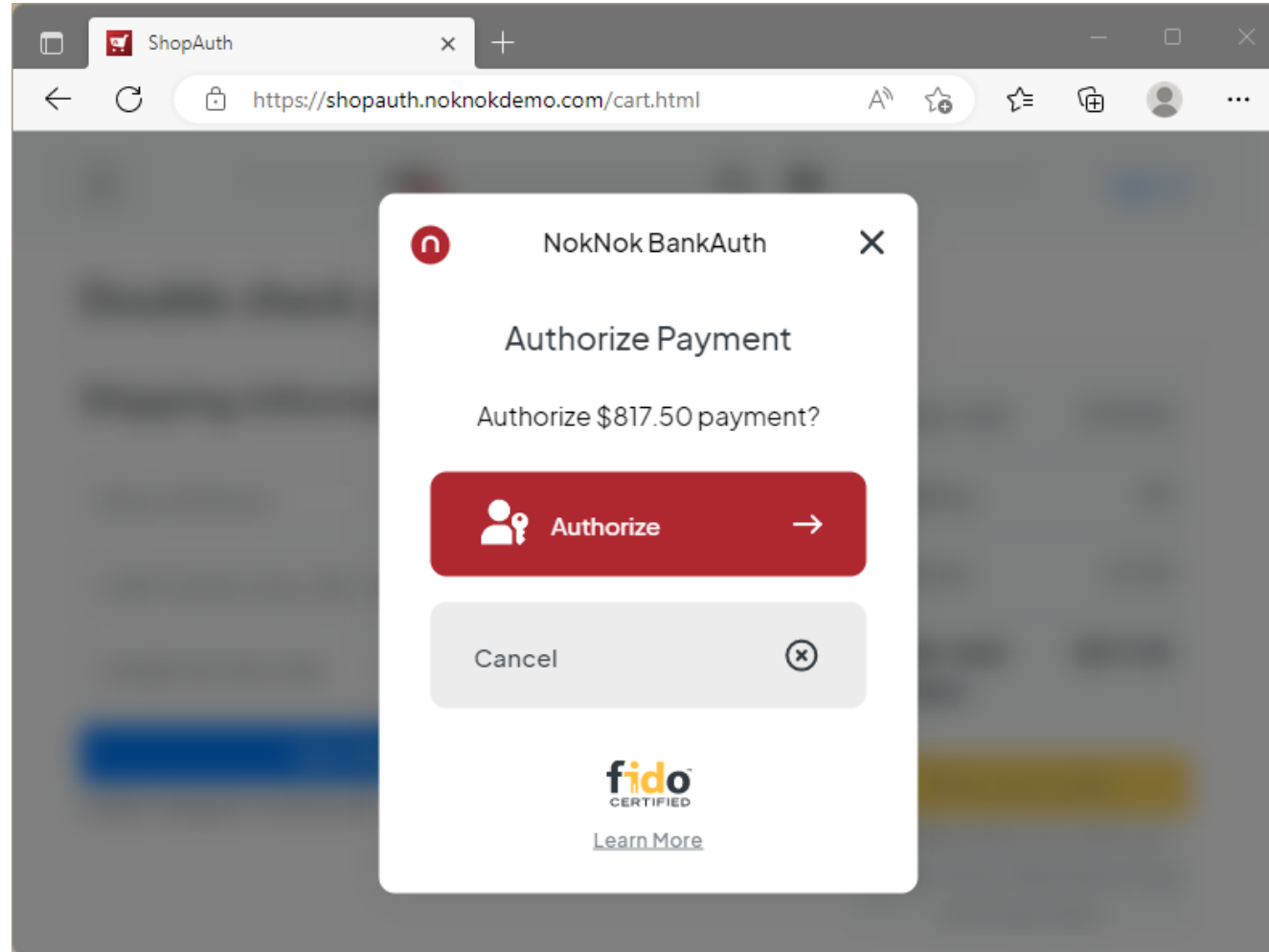
[Save Payment Information](#)

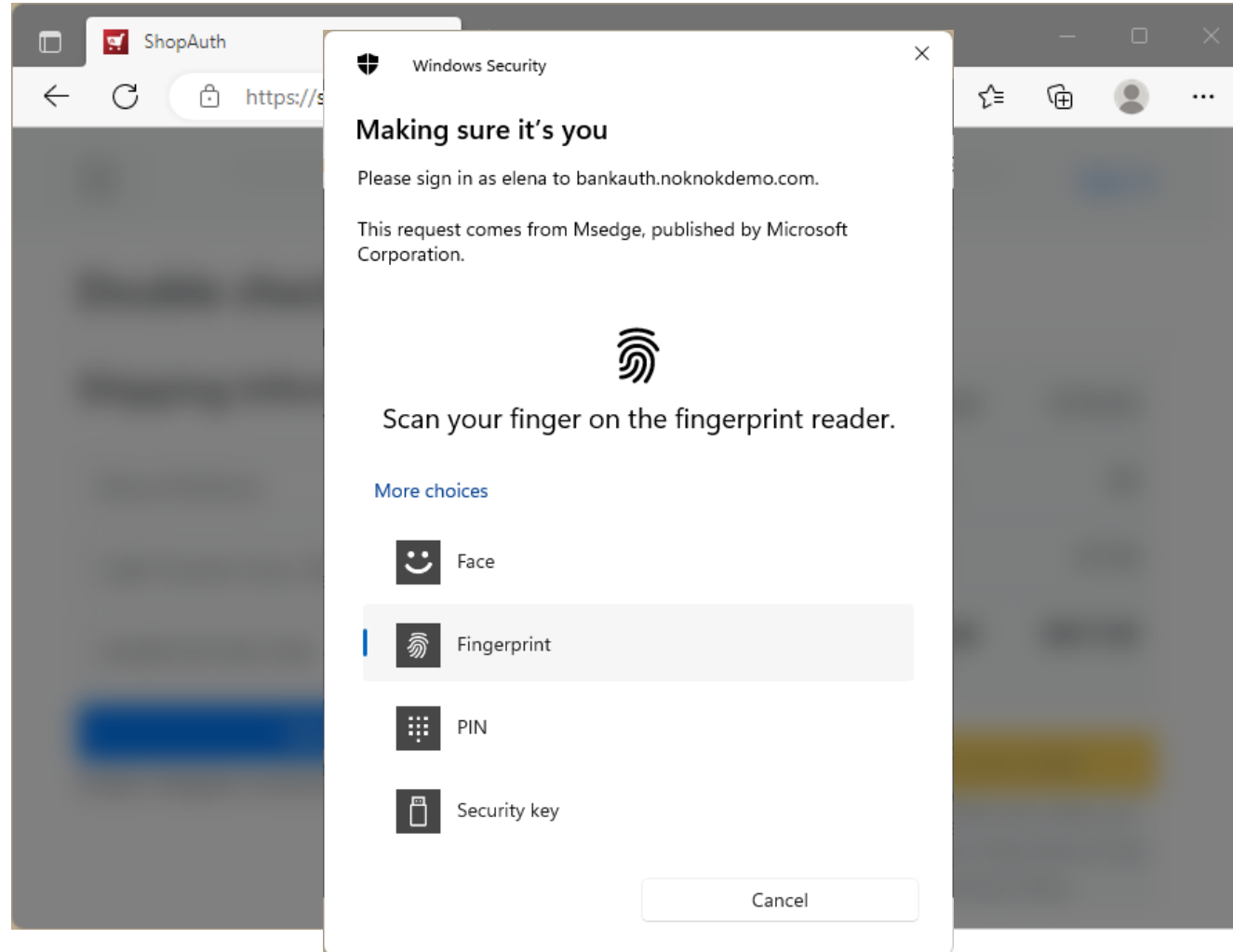
Enables Delegated Authentication

Item(s) total	\$750.00
Shipping	\$0
Sales tax	67.50
Order total (1 item)	\$817.50

[Place your order](#)

By clicking Place your order, you agree to Dronz' Shop Terms of Use and Privacy Policy





ShopAuth x +

← ↻ 🔒 https://shopauth.noknokdemo.com/order-complete.html 🔍 ☆ ⌘ 👤 ⋮

☰ **nok nok** 🔍 🛒 [Sign In](#)

Thank you for shopping with us, Elena Molinero.

We hope to see you again soon!

Order No.	#10723
-----------	--------

Total:	\$817.50
--------	----------

Shipping to

Calle Puente Grau 300, Arequipa
04000 Peru

15:08



oknokdemo.com

Shipping Information

Elena Molinero

Calle Puente Grau 300, Arequipa 04000 Per

3439875075651058

Save Payment Information

Enables Delegated Authentication

Item(s) total	\$750.00
Shipping	\$0
Sales tax	67.50
Order total (1 item)	\$817.50

Place your order

By clicking Place your order, you agree to Dronz' Shop



15:08



oknokdemo.com

NokNok BankAuth X

Authorize Payment

Authorize \$817.50 payment?

Authorize →

Cancel ⊗

fido
CERTIFIED

[Learn More](#)



15:08



oknokdemo.com

Shipping Information

Elena Molinero

Use your screen lock

Confirm your fingerprint so bankauth.noknokdemo.com can verify it's you.



Touch sensor

Cancel Use screen lock

Sales tax 67.50

Order total (1 item) \$817.50

Place your order

By clicking Place your order, you agree to Dronz' Shop

**Thank you for
shopping with us,
Elena Molinero.**

**We hope to see you again
soon!**

Order No.

#10723

Total:

\$817.50

Shipping to

Calle Puente Grau 300, Arequipa
04000 Peru

Scenario Summary – Browser (iframe)

Transaction display	Bank web app (HTML & JS) – privileged to use credential
Transaction detail linked ¹ to authentication code ²	The FIDO assertion includes a server challenge derived from a cryptographic hash of the transaction text
Credential type	Depends on authenticator/device – single device credential or multi-device credential
Authentication factors ³	Possession of authenticator + user verification
Transaction text appearance	HTML – up to full screen
Devices required	1
MITM protection	Yes, if user verifies transaction text
Additional user interaction	None
Notes	Requires cross-origin-iframe WebAuthn support in Browser (Chrome, Edge, Samsung Internet, Safari 16+), needs JS injection protection

¹ See PSD2 RTS Article 9 “Independence of Elements”

² PSD2 term for the FIDO assertion is “authentication code”



³ See PSD2 RTS Article 5 “dynamic linking”



3. Secure Payment Confirmation (SPC)

ShopAuth x +

shopauth.noknokdemo.com/cart.html

nok nok DRONES DRONE COMPONENTS CALL US: 650.433.1300   Sign In

Double check your order details

Shipping Information

Elena Molinero

Calle Puente Grau 300, Arequipa 04000 Peru


3439875075651058

Save Payment Information Enables Delegated Authentication

Item(s) total	\$750.00
Shipping	\$0
Sales tax	67.50
Order total (1 item)	\$817.50

Place your order

By clicking Place your order, you agree to Dronz' Shop Terms of Use and Privacy Policy



Drone 1 The Best
Free Shipping. Ready for delivery.

Quantity: 1

This order is a gift


Choose a shipping method

Hyperloop instant delivery
Free


USPS Priority Mail Express
\$12.50

ShopAuth

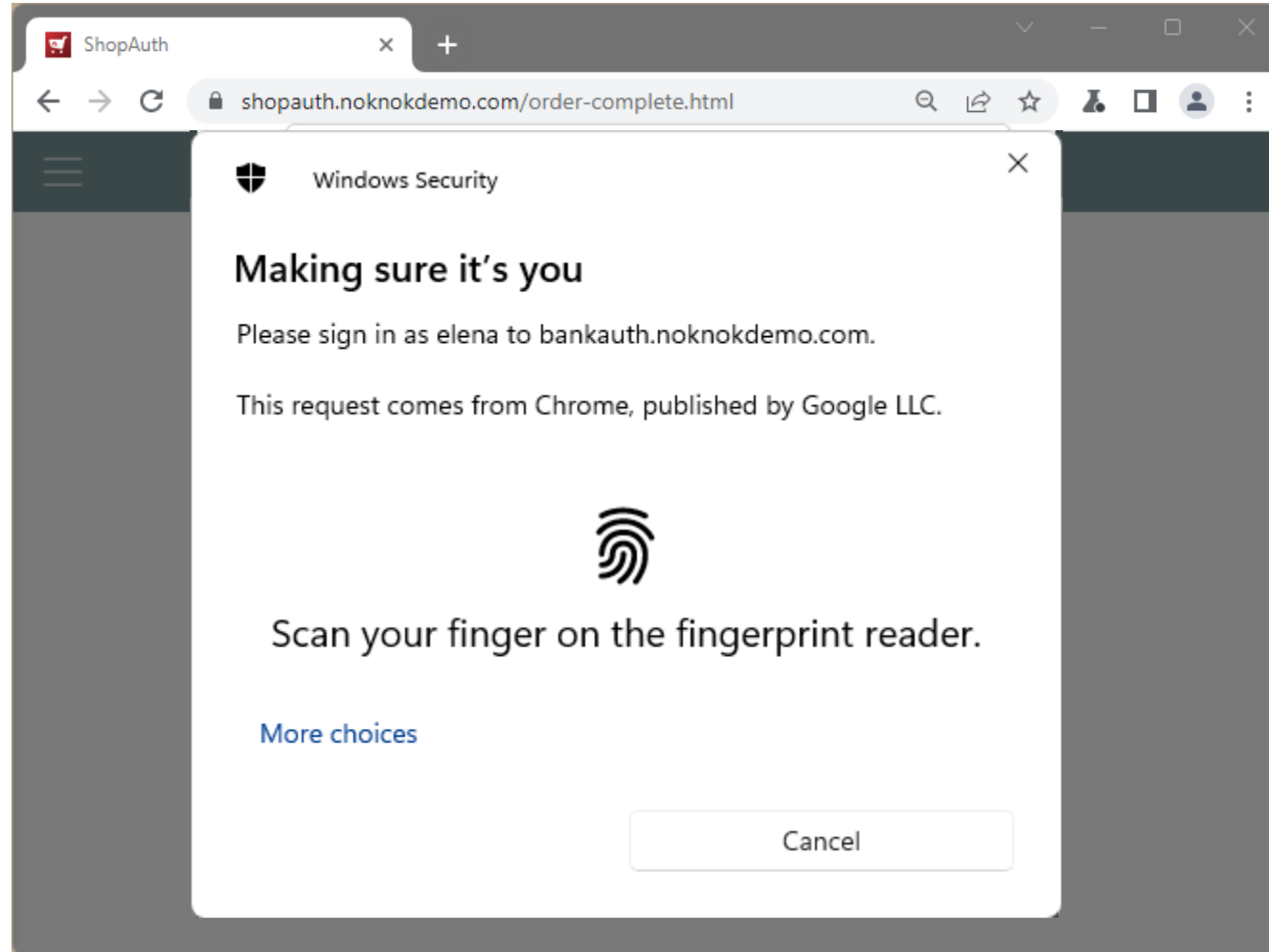
shopauth.noknokdemo.com/order-complete.html



Use Windows Hello to verify and complete your purchase?

Store	ShopAuth (shopauth.noknokdemo.com)
Payment	 BankAuth... 1058
Total	USD \$817.50

Verify Cancel



ShopAuth

shopauth.noknokdemo.com/order-complete.html

nok nok DRONES DRONE COMPONENTS CALL US: 650.433.1300

Search Cart Sign In

Thank you for shopping with us, Elena Molinero.
We hope to see you again soon!

Order No. #10723

Total: \$817.50

Shipping to
Calle Puente Grau 300, Arequipa 04000 Peru

Sign up now for our Newsletter and get a 10% rebate on your first order.

COMPANY SERVICE ORDERS & RETURNS PAYMENTS ACCEPTED

Scenario Summary – Issuer-SPC

Transaction display	FIDO Client (Web Browser) – privileged to use credential
Transaction detail linked ¹ to authentication code ²	The FIDO assertion includes a cryptographic hash of the structured transaction details.
Credential type	Depends on authenticator/device – single device credential or multi-device credential
Authentication factors ³	Possession of authenticator + user verification
Transaction text appearance	Browser-specific visual representation
Devices required	1
MITM protection	Yes, if user verifies transaction text
Additional user interaction	None
Notes	Supported in Chrome only, no roaming authenticator support (yet)

¹ See PSD2 RTS Article 9 “Independence of Elements”

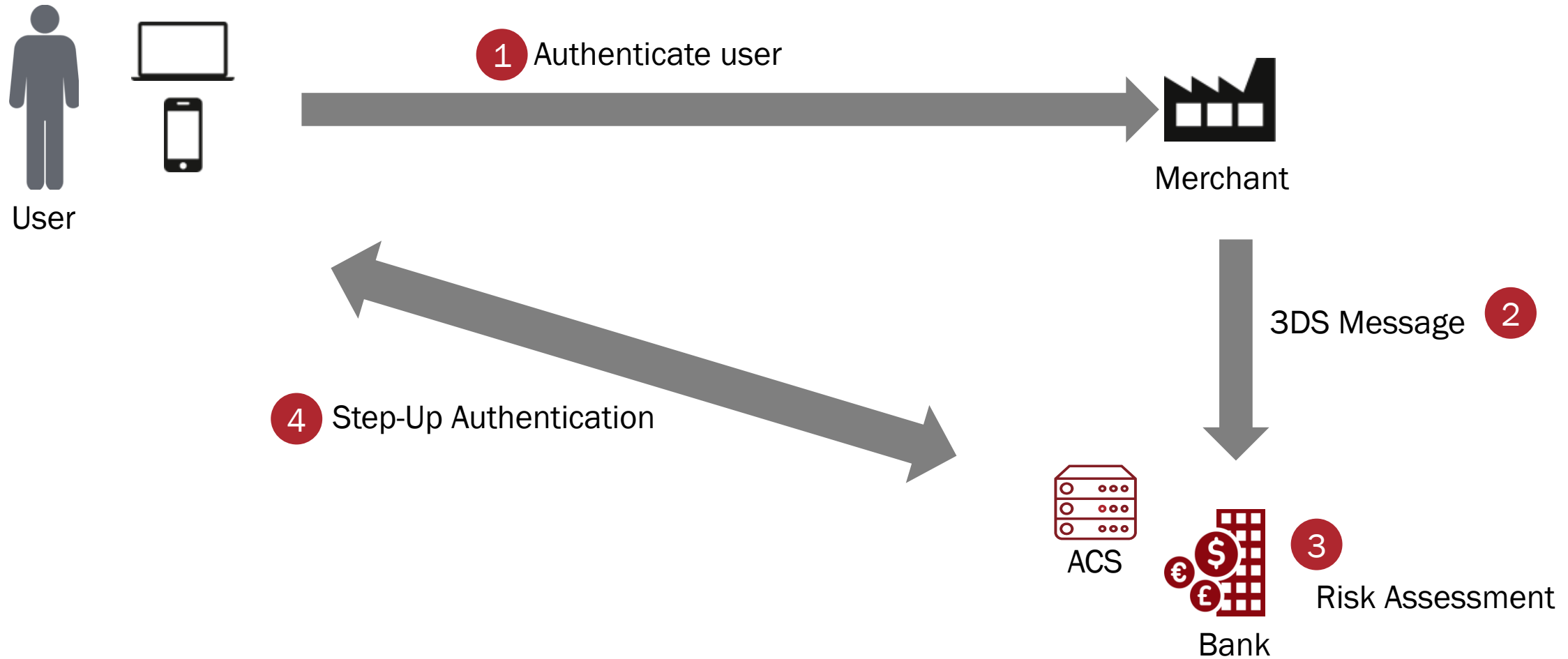
² PSD2 term for the FIDO assertion is “authentication code”

³ See PSD2 RTS Article 5 “dynamic linking”

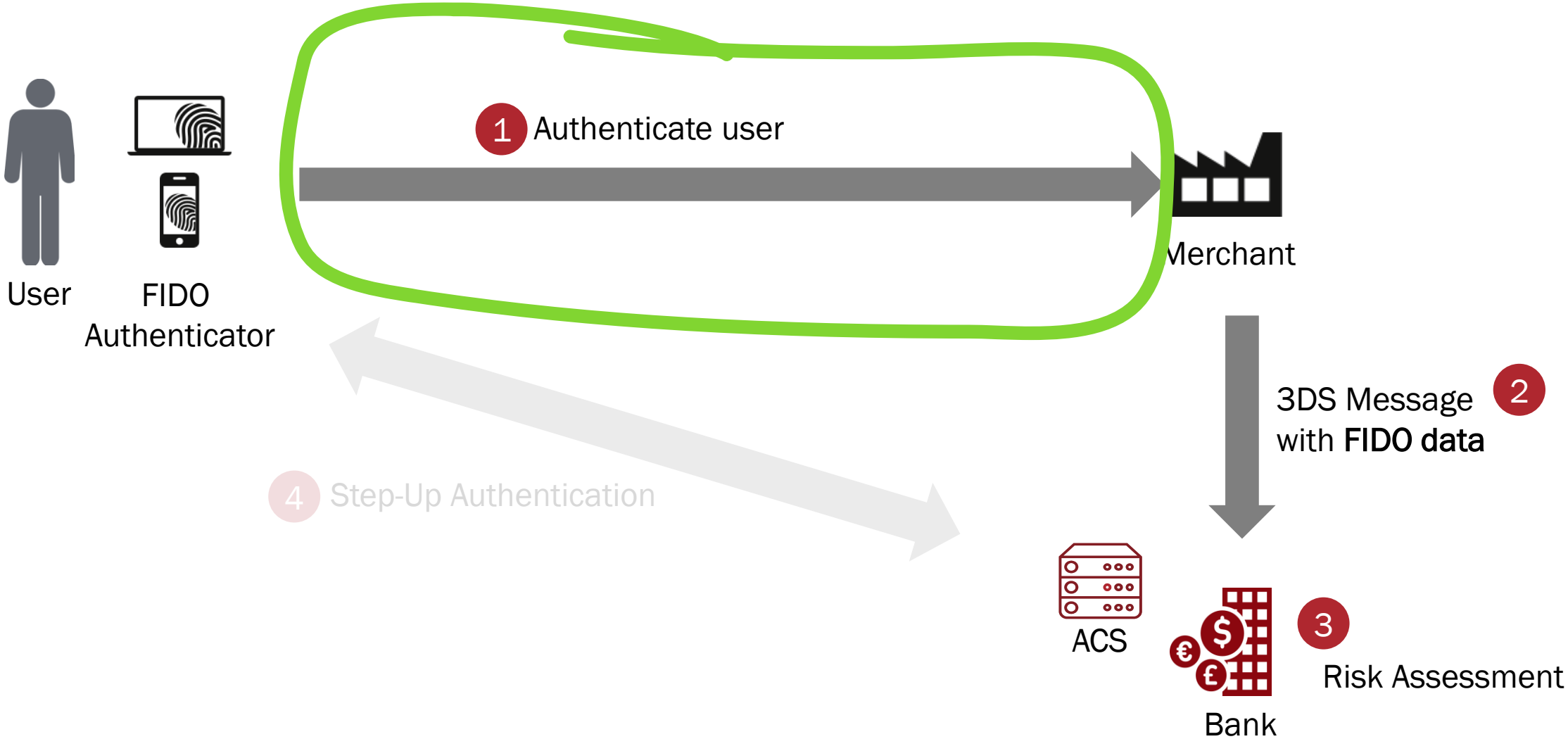


Delegated Authentication

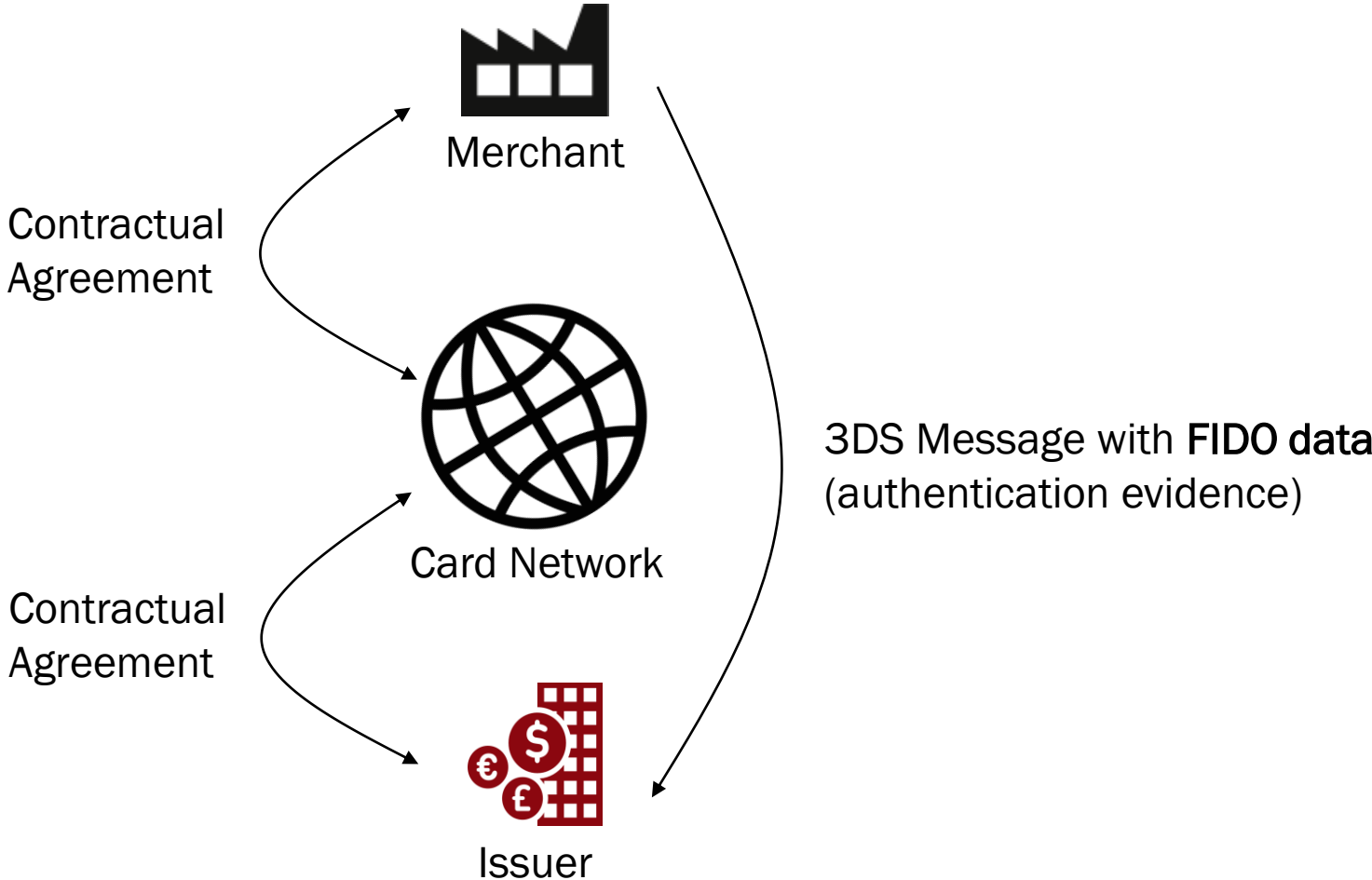
3DS Overview



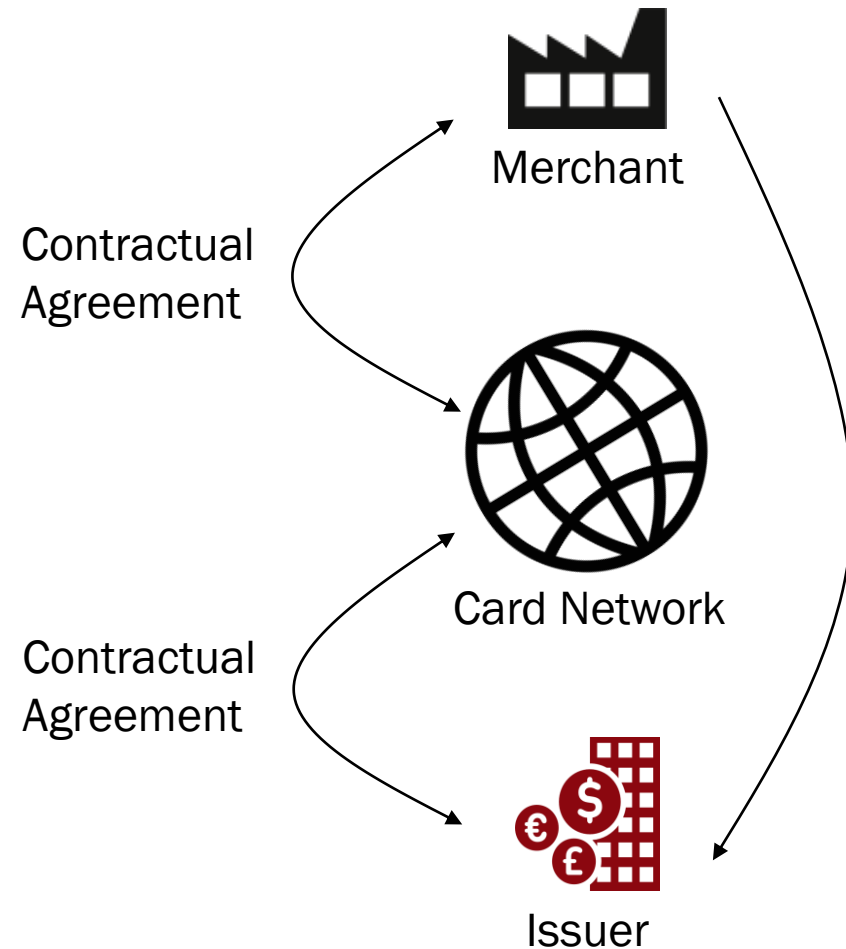
Delegated Authentication



Delegated Authentication



Delegated Authentication



A.7.3 3DS Requestor Authentication Information

The 3DS Requestor Authentication Information contains optional information about how the cardholder authenticated during login to their 3DS Requestor account. The detailed data elements are outlined in Table A.10.

Table A.10: 3DS Requestor Authentication Information

Data Element/Field Name	Description	Length/Format/Values
3DS Requestor Authentication Data Field Name: <code>threeDSReqAuthData</code>	Data that documents and supports a specific authentication process. In the current version of the specification, this data element is not defined in detail, however the intention is that for each 3DS Requestor Authentication Method, this field carry data that the ACS can use to verify the authentication process. For example, if the 3DS Requestor Authentication Method is: <ul style="list-style-type: none"> 03, then this element can carry information about the provider of the federated ID and related information. 06, then this element can carry the FIDO attestation data (including the signature). 07, then this element can carry FIDO Attestation data with the FIDO assurance data signed. 08, then this element can carry the SRC assurance data. 	Length: maximum 20,000 characters JSON Data Type: String

3DS Message with FIDO data (authentication evidence)

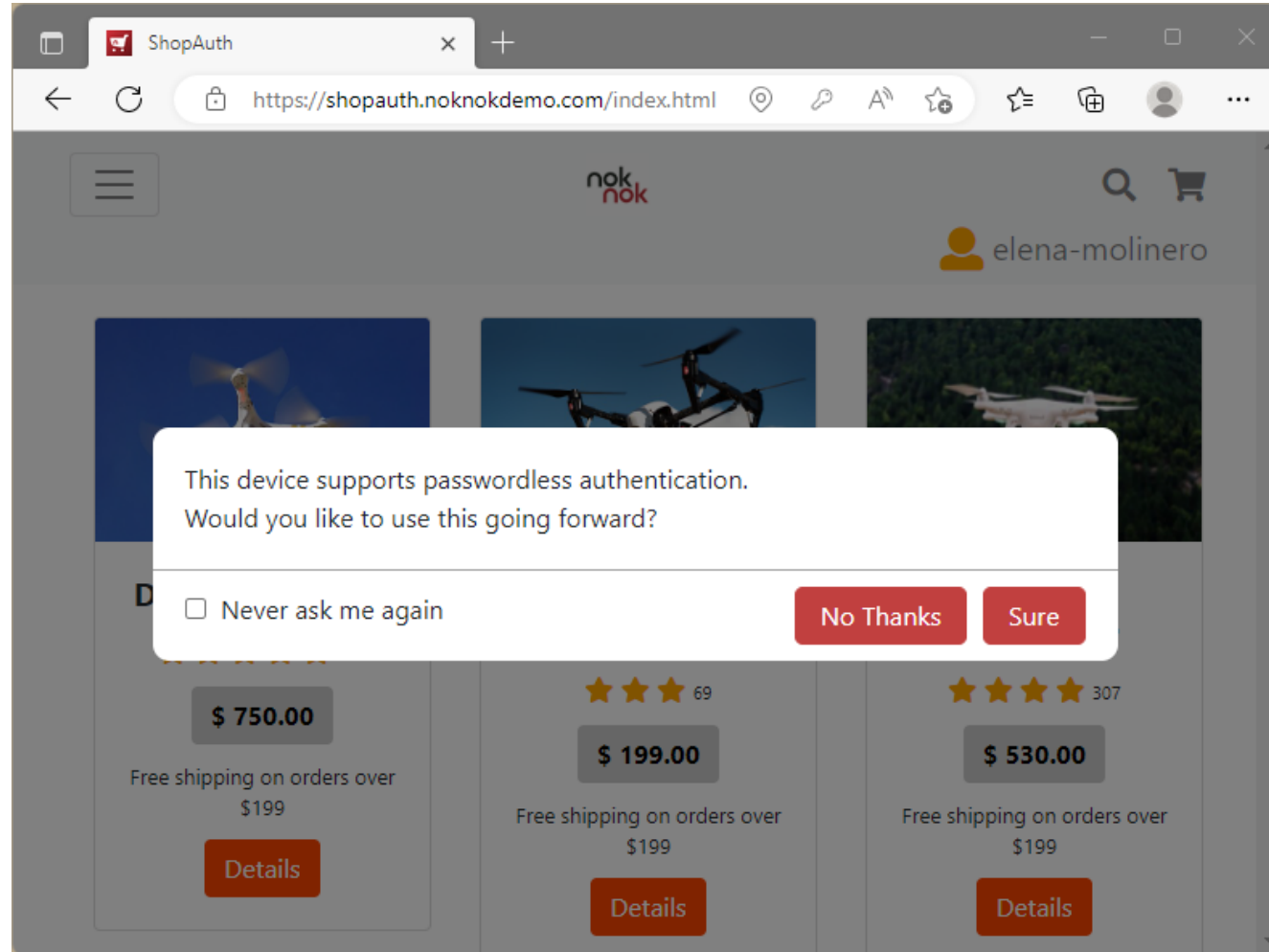
```

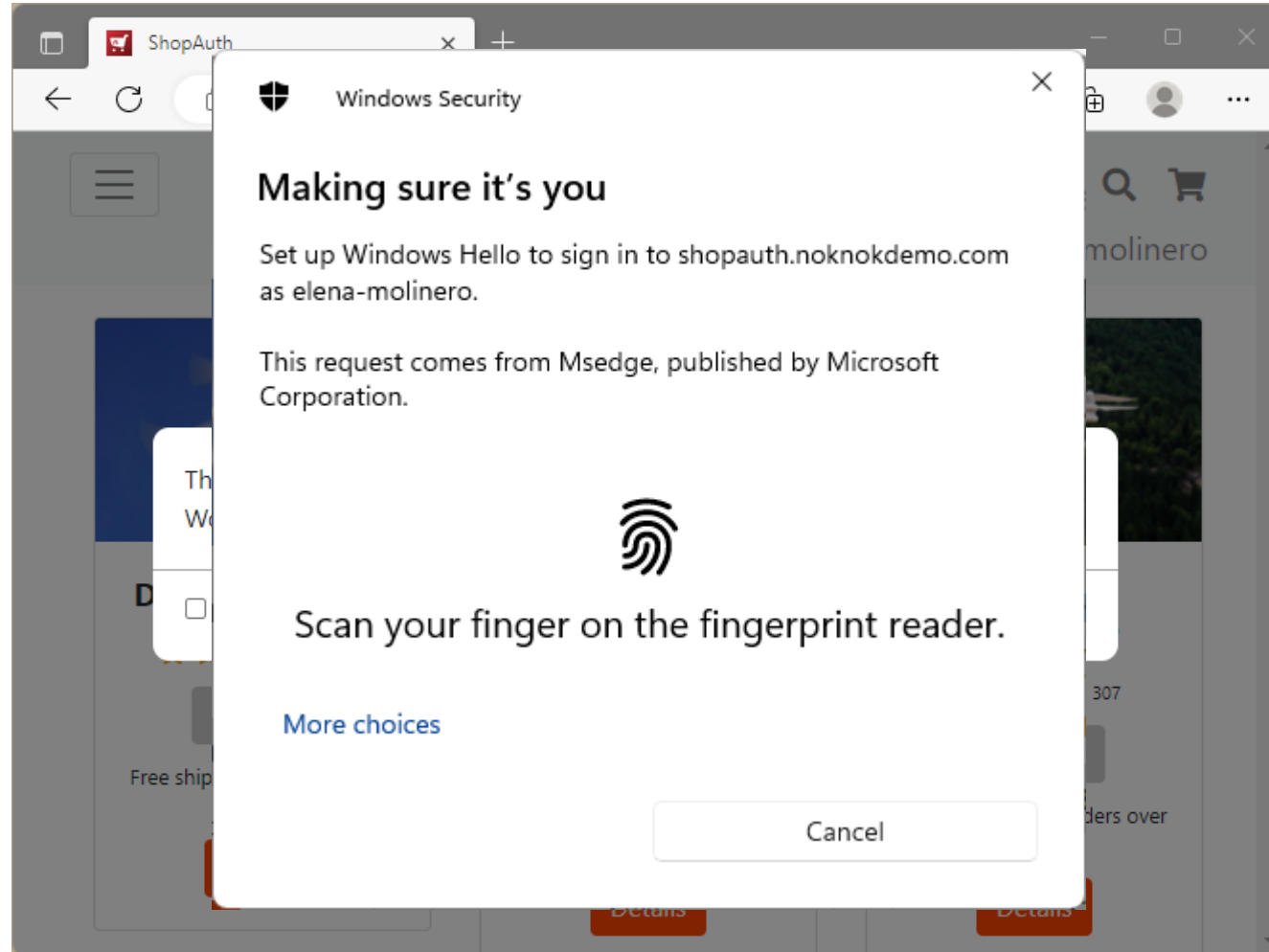
"fidodata": {
  "rpId": "https://shopauth.noknokdemo.com",
  "authTime": "2022-06-08T07:42:17Z",
  "fidoAuthenticatorReferences": [
    { "publicKey":
      "A401030339010020590100C7CA21EA2DC465DC6338E5D3404A174493E42173EE4188412E542300364C82CA647
      AC641752DFAD2787911ABBCDD484B5C33DD63F10DBF102154F2D45FB4B1147971287D119C93CD3BB4EBD076048
      D6EA32ED999419A0490546BEE6C79E056F396D5717AFE710CE735230C08E98BF5A378797844D06CF2B9E1A1CD44
      09C1989C4EBC60E0B37AE3244D89517AE77E80CC1849DDB21A62FE163739AD92FF1F64C2552C440A1EFACC5736
      EB31E62B773105F6FF01679F9A84B157BC0D2A5A0B983149C990768E8E1EF43899B4967AA58EA285B695A239D6
      A204685D2417DE5581D564C78B008F4E0729AA1B1B1883D57AC51B2BE9258DF6572E061A00774C180AEA121430
      10001",
      "aaguid": "0132d110-bf4e-4208-a403-ab4f5f12efe5",
      "uv": true,
      "up": true,
      "usedForThisTransaction": true
    }
  ]
}
    
```

See <https://fidoalliance.org/technical-note-fido-authentication-and-emv-3-d-secure-using-fido-for-payment-authentication/>



0. Enablement








1. First Purchase

ShopAuth x +

https://shopauth.noknokdemo.com/index.html

☰ nok nok 🔍 🛒

👤 elena-molinero




Drone 1 The Best

★★★★★ 523

\$ 750.00

Free shipping on orders over \$199

[Details](#)




Droney 23 Take Me

★★★★ 69

\$ 199.00

Free shipping on orders over \$199

[Details](#)



Drohne 7 Heavyliifter

★★★★★ 307

\$ 530.00

Free shipping on orders over \$199


[Details](#)

ShopAuth x +

← ↻ 🔒 https://shopauth.noknokdemo.com/details.html 🔊 ☆ ⌵ 🗑️ 👤 ⋮

☰ **nok nok** 🔍 🛒

👤 elena-molinerero



Drone 1 The Best

BLUE & WHITE

★★★★★ 523


\$750.00

[ADD TO CART](#)

Hyperloop delivery from San Francisco

Description

This is the drone you've been waiting for. This drone is fully loaded with high-performance automations like Auto Launch, Auto Hover, and Auto Land. Eliminate the learning curve




ShopAuth x +

← ↻ 🔒 https://shopauth.noknokdemo.com/details.html 🔊 ☆ ⌵ 📁 👤 ⋮

☰ **nok nok** 🔍 🛒 1

👤 elena-moliner



Drone 1 The Best

BLUE & WHITE

★★★★★ 523


\$750.00

[ADD TO CART](#)

Hyperloop delivery from San Francisco

Description

This is the drone you've been waiting for. This drone is fully loaded with high-performance automations like Auto Launch, Auto Hover, and Auto Land. Eliminate the learning curve



ShopAuth x +

https://shopauth.noknokdemo.com/cart.html

nok nok

elena-molinero

Double check your order details

Shipping Information

Elena Molinero

Calle Puente Grau 300, Arequipa 04000 Peru

3439875075651058

[Remove Payment Information](#)

Enables Delegated Authentication

Item(s) total	\$750.00
Shipping	\$0
Sales tax	67.50
Order total (1 item)	\$817.50

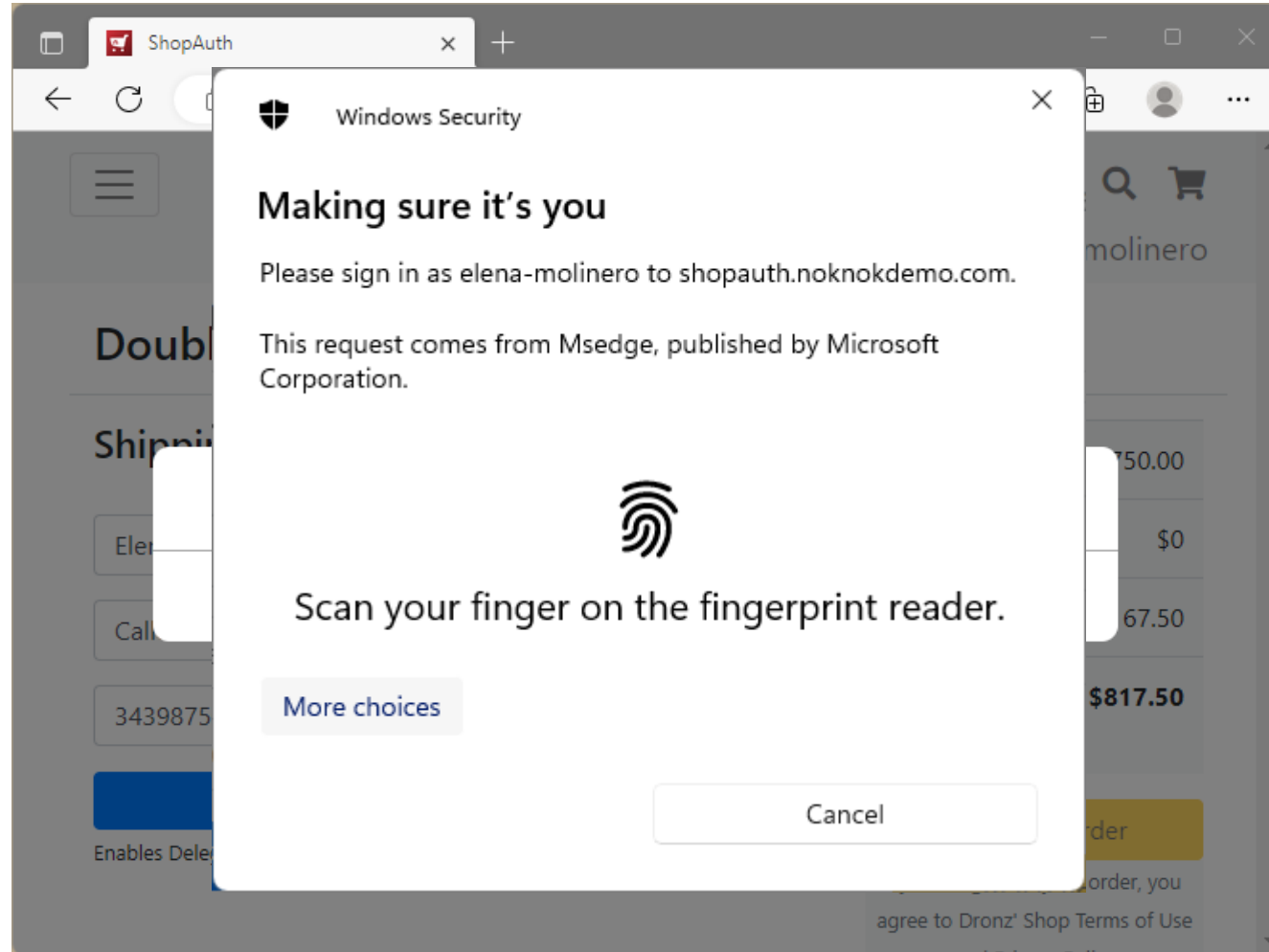
[Place your order](#)

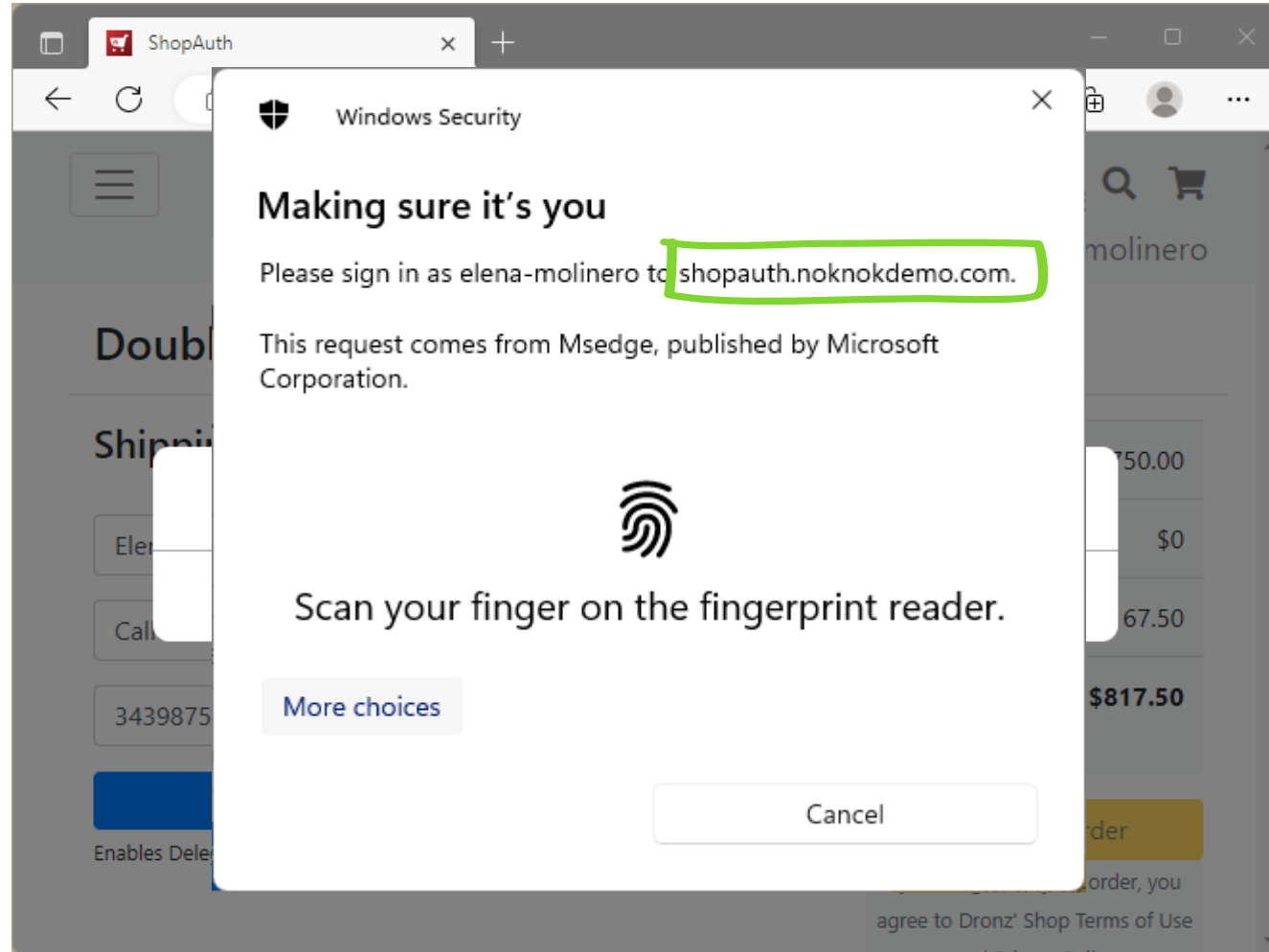
By clicking Place your order, you agree to Dronz' Shop Terms of Use

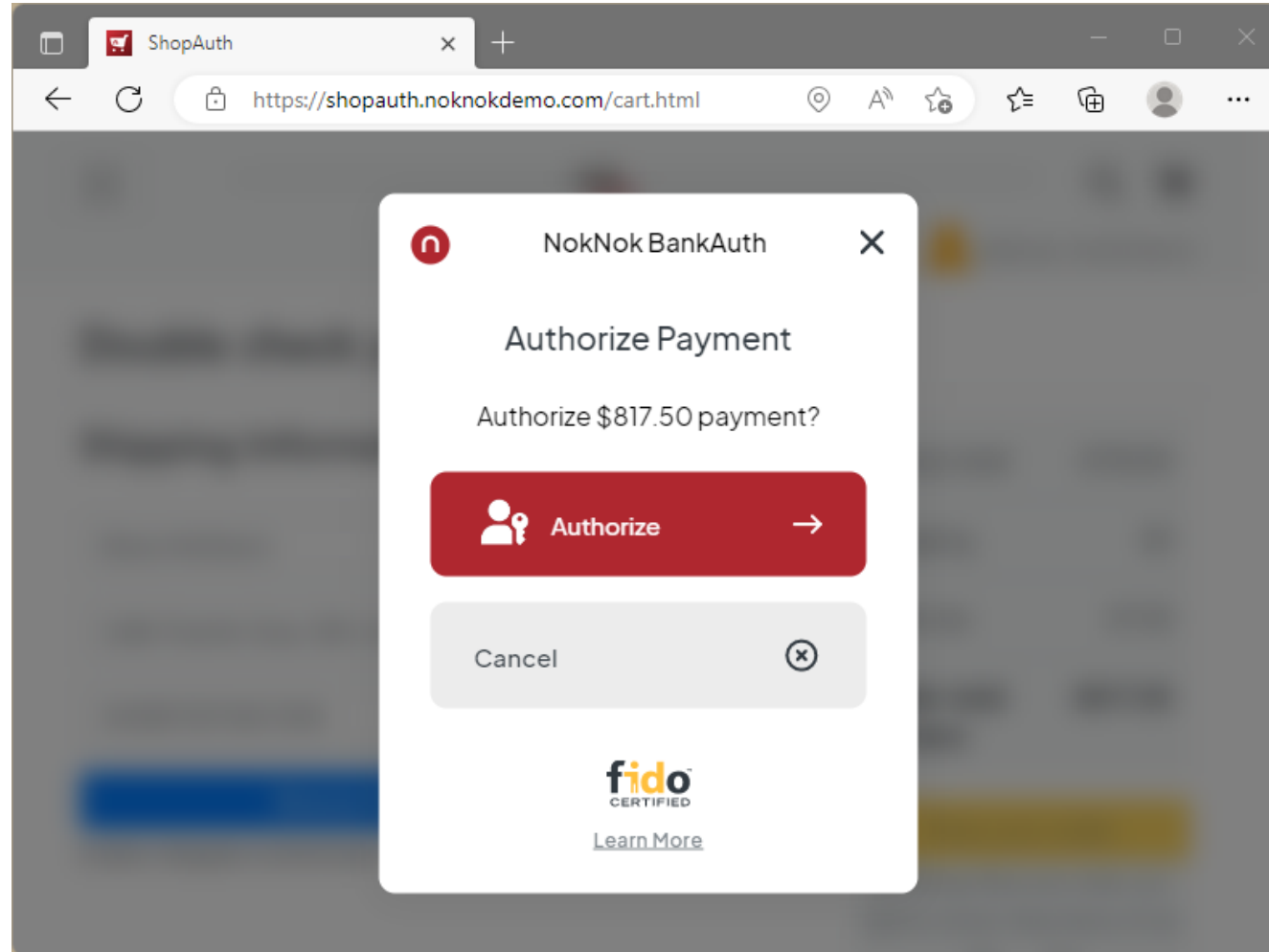
The screenshot shows a web browser window with the following details:

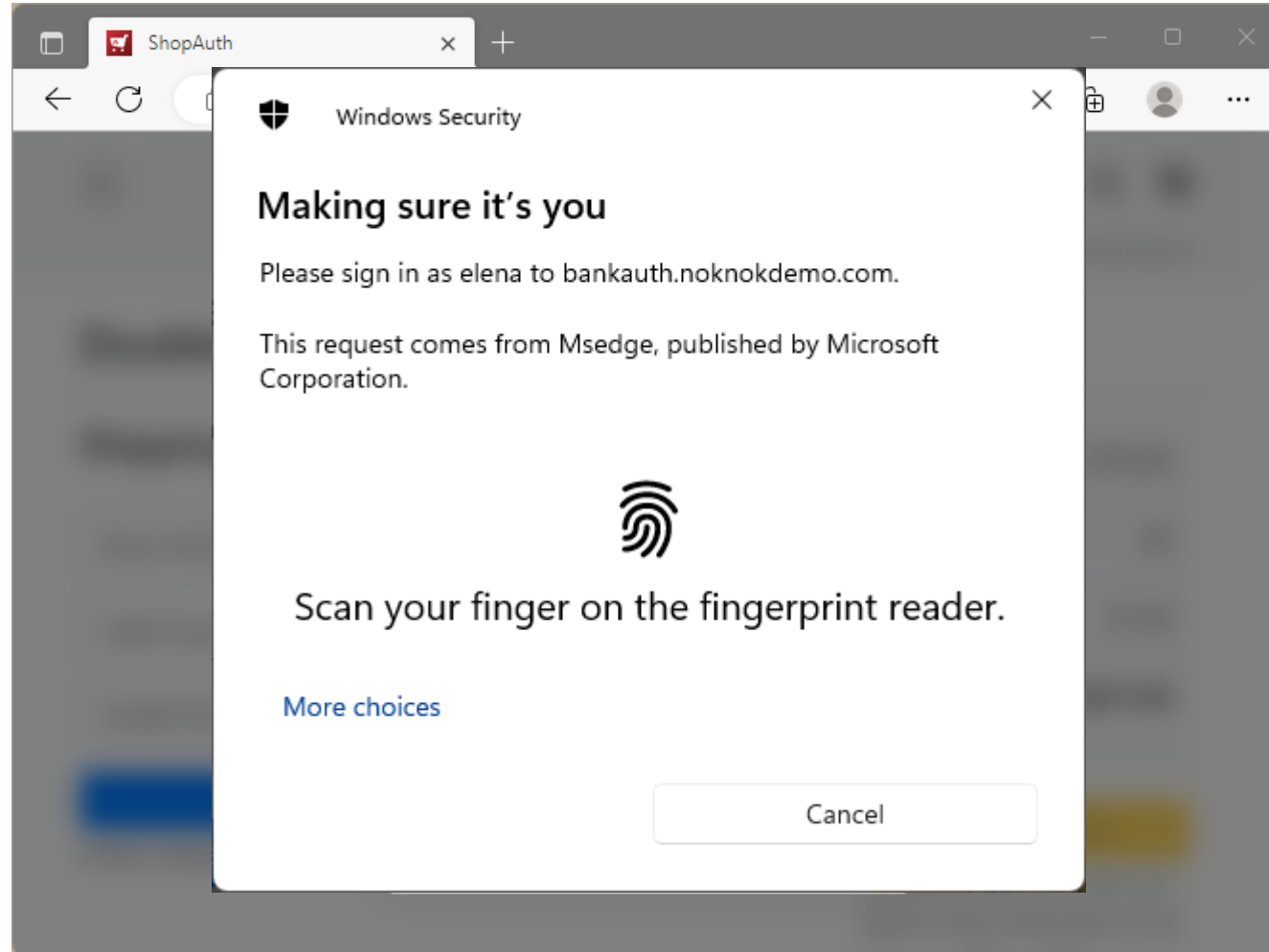
- Browser Tab:** ShopAuth
- Address Bar:** <https://shopauth.noknokdemo.com/cart.html>
- Page Header:** noknok logo, search icon, shopping cart icon, and user profile "elena-molinero".
- Main Content:** "Double check your order details" section with "Shipping Information" and a table of items.
- Payment Dialog:** A white modal box with the text "Authorize \$817.50 payment?" and two red buttons: "Authorize" and "Decline".
- Order Summary:** "Order total (1 item) \$817.50".
- Buttons:** "Remove Payment Information" (blue) and "Place your order" (olive green).

Item	Price
Electronics	\$750.00
Shipping	\$0
Call	\$67.50
Order total (1 item)	\$817.50









ShopAuth x +

← ↻ 🔒 https://shopauth.noknokdemo.com/order-complete.html 🔍 ⭐ 📁 👤 ⋮

☰ **nok nok** 🔍 🛒

👤 elena-molinero

Thank you for shopping with us, Elena Molinero.

We hope to see you again soon!

Order No. #10723

Total: \$817.50

Shipping to

Calle Puente Grau 300, Arequipa
04000 Peru




2. Second and Subsequent Purchases

ShopAuth x +

← → ↻ https://shopauth.noknokdemo.com/index.html 🔍 ⭐ 📌 👤 ⋮

☰ **nok nok** 🔍 🛒

👤 elena-molinero




Drone 1 The Best

★★★★★ 523

\$ 750.00

Free shipping on orders over \$199

[Details](#)




Droney 23 Take Me

★★★★ 69

\$ 199.00

Free shipping on orders over \$199

[Details](#)



Drohne 7 Heavyliifter

★★★★★ 307

\$ 530.00

Free shipping on orders over \$199


[Details](#)

ShopAuth x +

← ↻ 🔒 https://shopauth.noknokdemo.com/details2.html 🔊 ☆ ⌵ 📁 👤 ⋮

☰ **nok nok** 🔍 🛒

👤 elena-molinero



Droney 23 Take Me

BLACK & WHITE

★★★★ 69


\$199.00

[ADD TO CART](#)

Hyperloop delivery from San Francisco

Description

This drone is fully loaded with high-performance automations like Auto Launch, Auto Hover, and Auto Land. Eliminate the



ShopAuth x +


← ↻ 🔒 https://shopauth.noknokdemo.com/details2.html 🔊 ☆ ⌵ 🗑️ 👤 ⋮

☰

**nok
nok**

🔍 🛒 1

👤 elena-molinero



Droney 23 Take Me

BLACK & WHITE

★★★★ 69





\$199.00

ADD TO CART

Hyperloop delivery from San Francisco

Description

This drone is fully loaded with high-performance automations like Auto Launch, Auto Hover, and Auto Land. Eliminate the



ShopAuth x +

← ↻ 🔒 https://shopauth.noknokdemo.com/cart.html 🔍 ⭐ ⚙️ 🛒 👤 ⋮

☰ **nok nok** 🔍 🛒

👤 elena-molinero

Double check your order details

Shipping Information

Elena Molinero

Calle Puente Grau 300, Arequipa 04000 Peru

3439875075651058

[Remove Payment Information](#)

Enables Delegated Authentication

Item(s) total	\$199.00
Shipping	\$0
Sales tax	17.91
Order total (1 item)	\$216.91

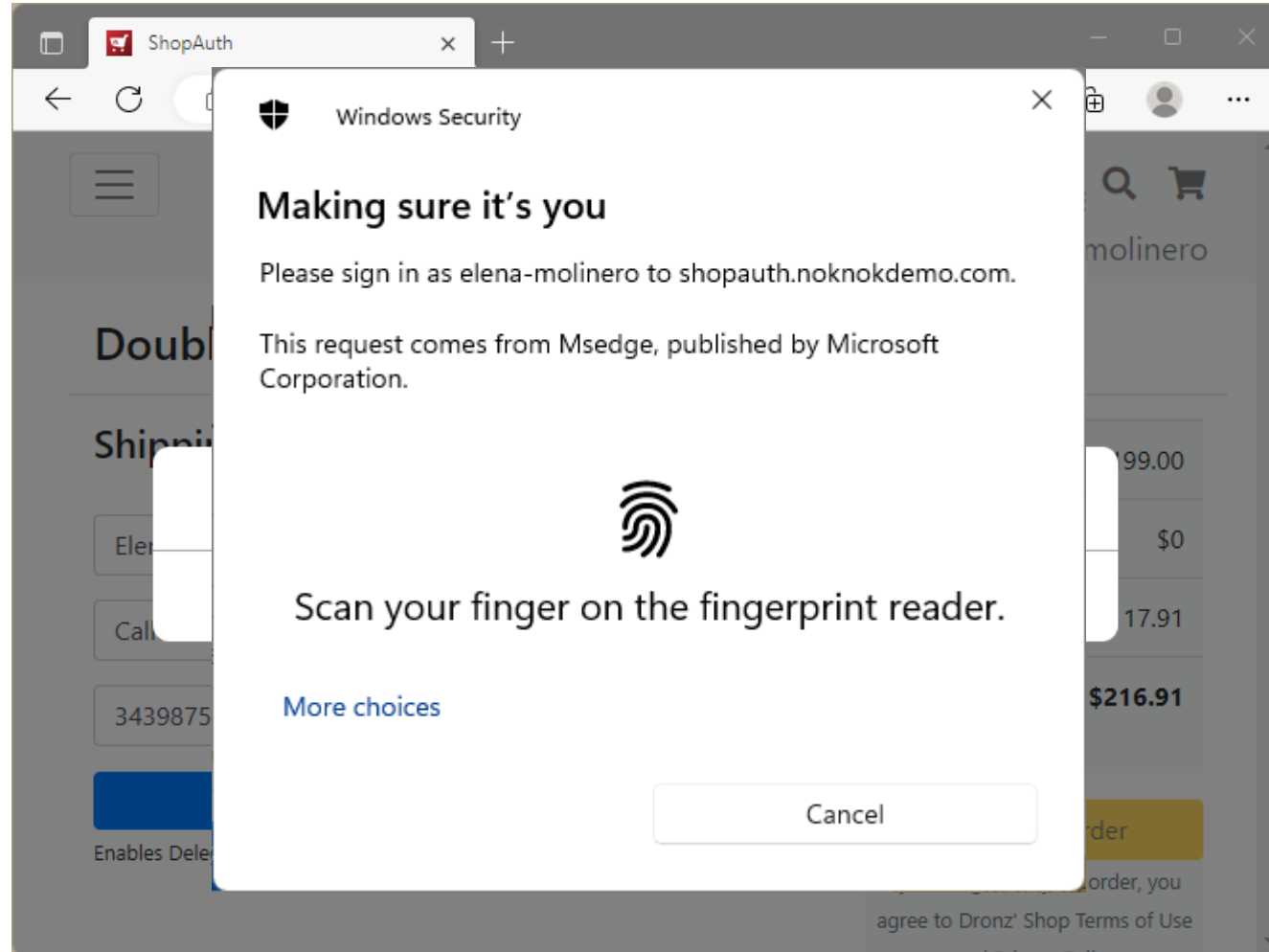
[Place your order](#)

By clicking Place your order, you agree to Dronz' Shop Terms of Use

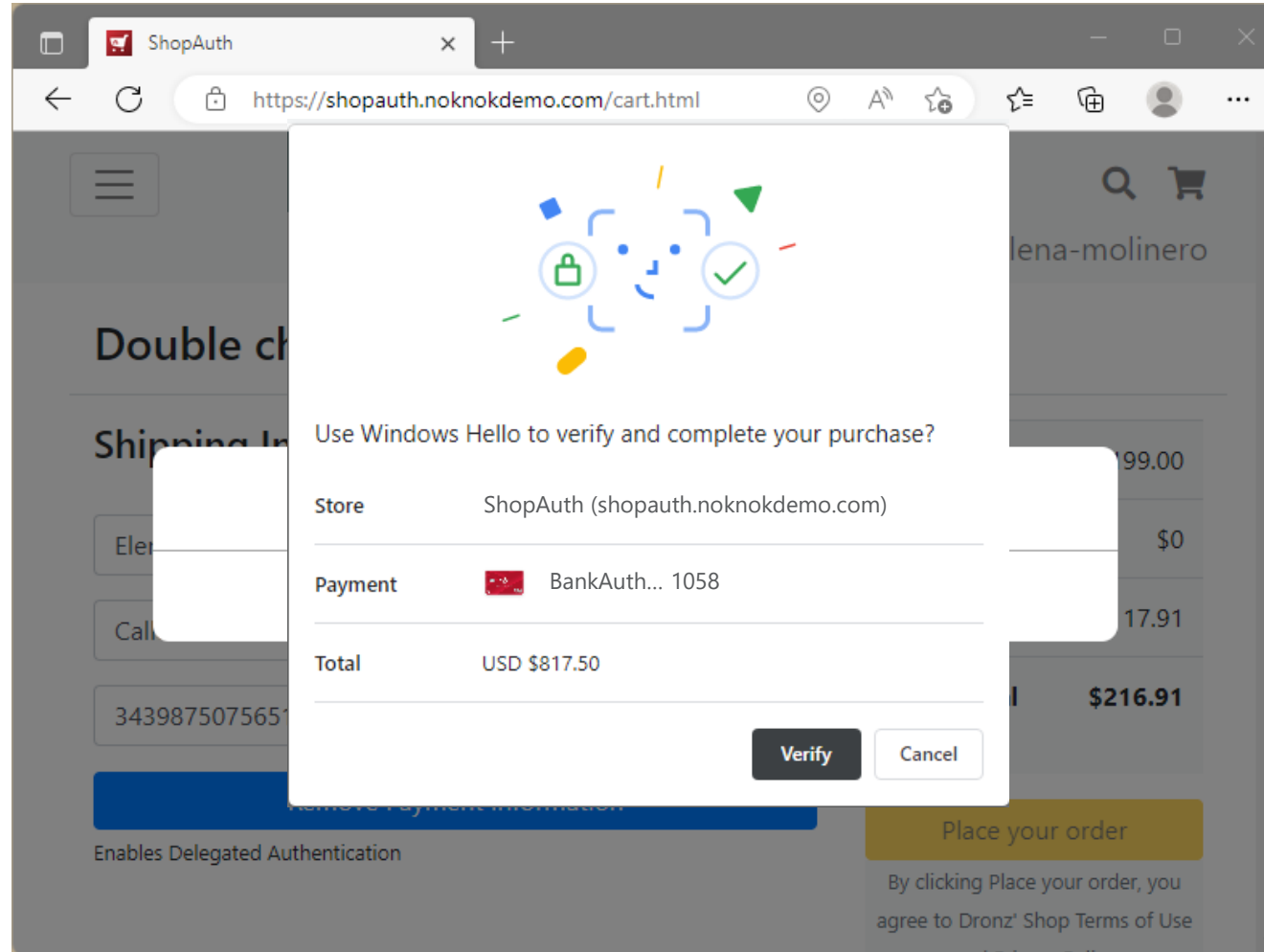
The screenshot shows a web browser window with the following details:

- Browser Tab:** ShopAuth
- Address Bar:** <https://shopauth.noknokdemo.com/cart.html>
- Page Header:** noknok logo, search icon, shopping cart icon, and user profile 'elena-molinero'.
- Main Content:** A shopping cart page with the heading 'Double check your order details'. It includes a 'Shipping Information' section with a text input field containing '3439875075651058'. A blue button labeled 'Remove Payment Information' is visible below the input field, with the text 'Enables Delegated Authentication' underneath it. To the right, there is a summary table for the order total.
- Payment Summary Table:**

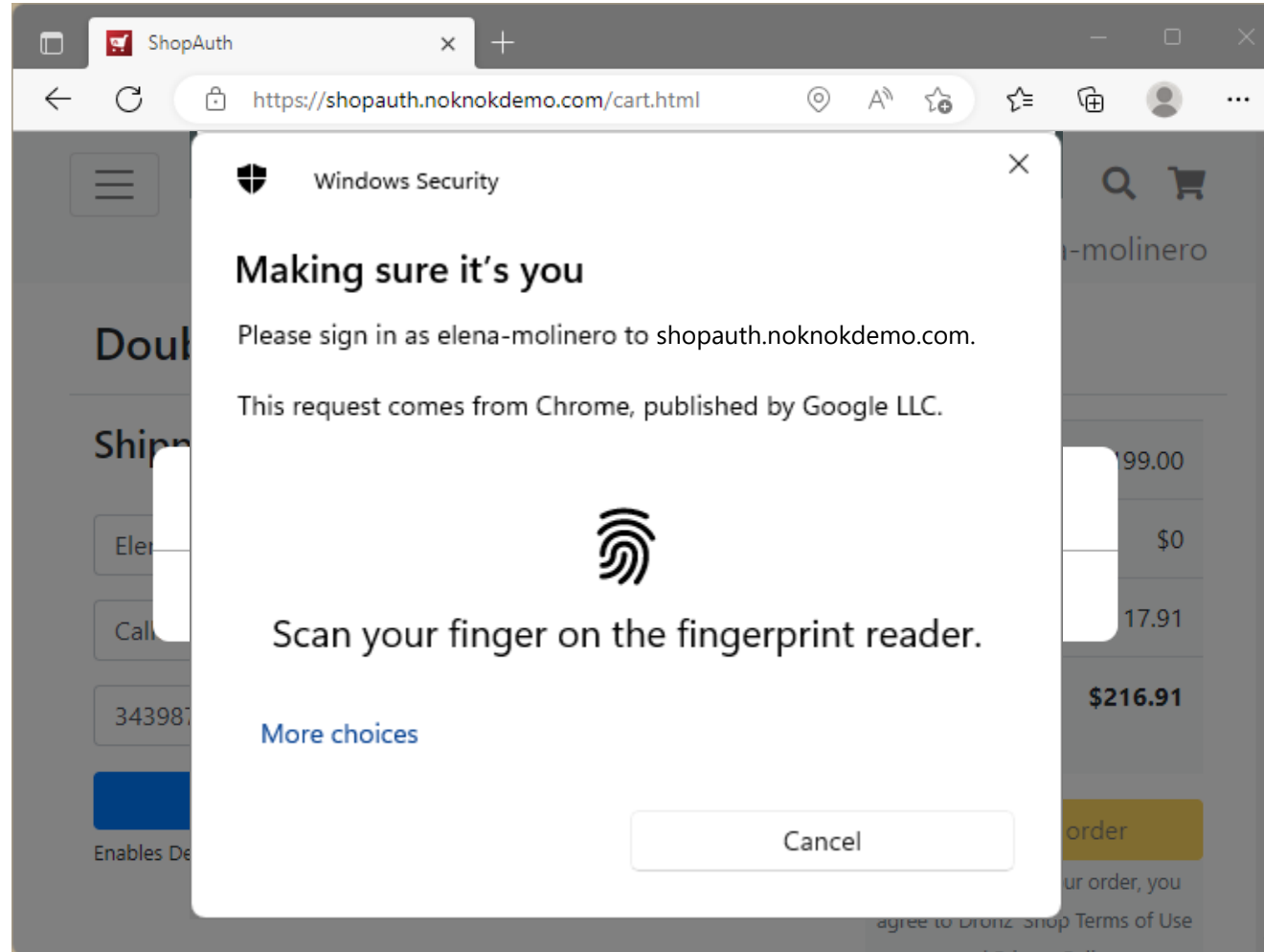
Order total	\$216.91
(1 item)	
- Dialog Box:** A white modal dialog box is centered on the screen with the text 'Authorize \$216.91 payment?'. It contains two red buttons: 'Authorize' and 'Decline'.
- Footer:** A yellow button labeled 'Place your order' is visible at the bottom right of the page, with the text 'By clicking Place your order, you agree to Dronz' Shop Terms of Use' below it.



Alternative: Merchant-SPC



Alternative: Merchant-SPC



ShopAuth x +

← ↻ 🔒 https://shopauth.noknokdemo.com/order-complete.html 🔍 ⭐ 📌 👤 ⋮

☰ **nok nok** 🔍 🛒

👤 elena-molinero

Thank you for shopping with us, Elena Molinero.

We hope to see you again soon!

Order No.	#10724
Total:	\$216.91

Shipping to

Calle Puente Grau 300, Arequipa
04000 Peru

Scenario Summary (Delegated Authentication)

	WebAuthn Variant	Merchant-SPC Variant
Transaction display	Merchant web app (HTML & JS)	FIDO Client (Web Browser)
Transaction detail linked ¹ to authentication code ²	The FIDO assertion includes a server challenge derived from a cryptographic hash of the transaction text	The FIDO assertion includes a cryptographic hash of the structured transaction details.
Credential type	Depends on authenticator/device – single device credential or multi-device credential	
Authentication factors ³	Possession of authenticator + user verification	
Transaction text appearance	HTML – up to full screen	Browser-specific visual representation
Devices required	1	
MITM protection	Yes, if user verifies transaction text	
Additional user interaction	None	
Notes	Supported by all modern Browsers	Supported in Chrome only, no roaming authenticator support (yet)

¹ See PSD2 RTS Article 9 “Independence of Elements”

² PSD2 term for the FIDO assertion is “authentication code”

³ See PSD2 RTS Article 5 “dynamic linking”

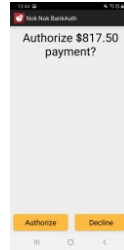
Auditability

Driving factors

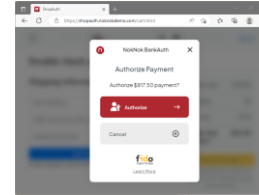
1. Altering transaction details should be detectable (“dynamic linking”)
2. Ensure the user has seen and approved (“non repudiation”)

Auditability – Dynamic Linking

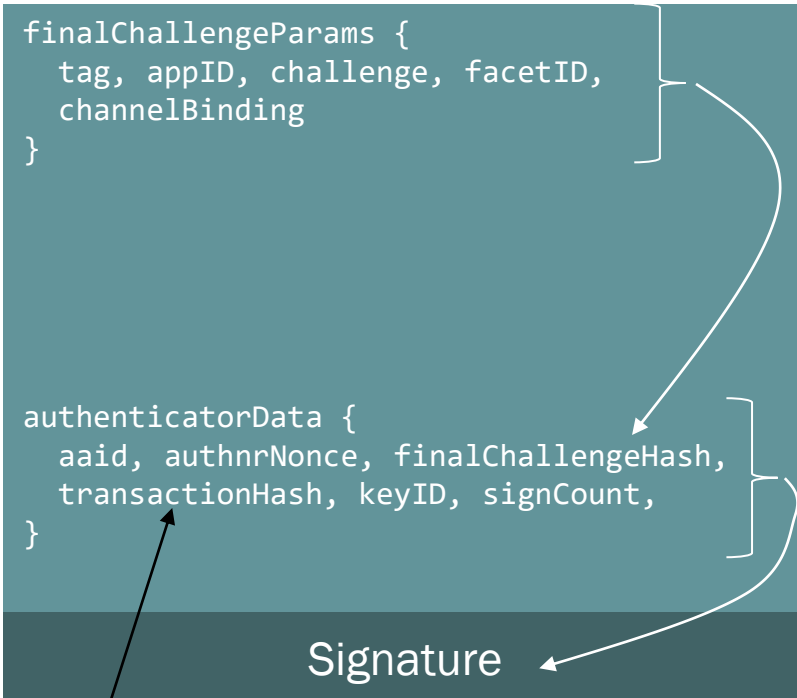
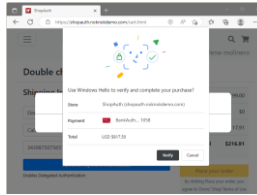
UAF txConf



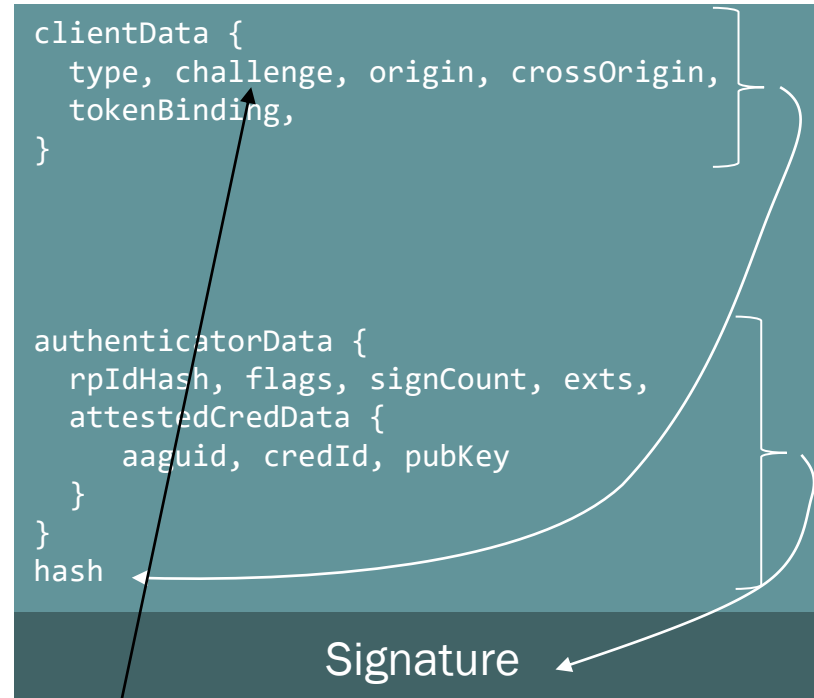
WebAuthn



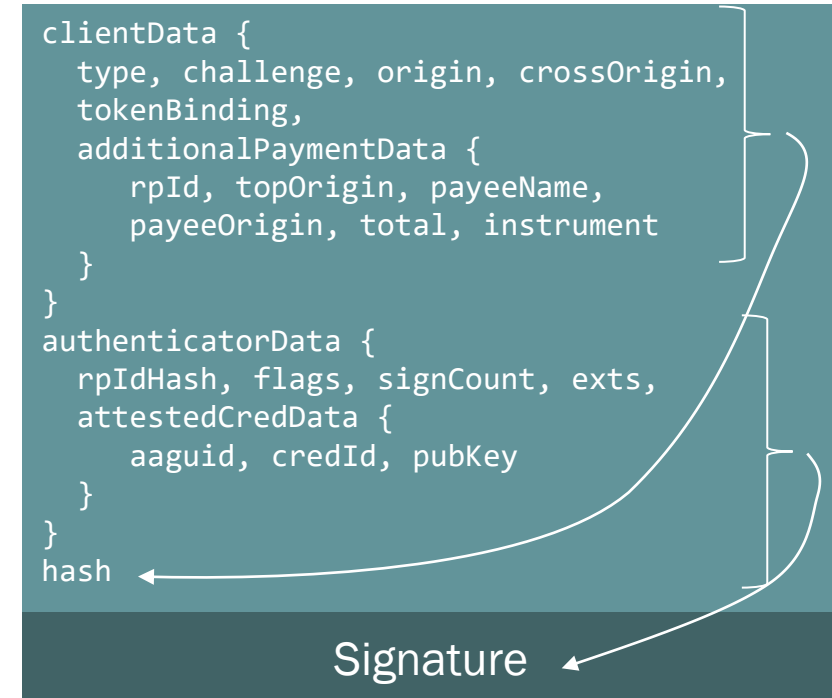
SPC



SHA256("Authorize \$817.50 payment")



Challenge = SHA256(random, transaction)

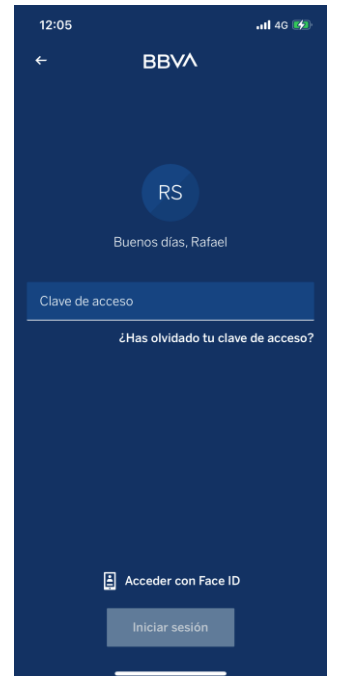
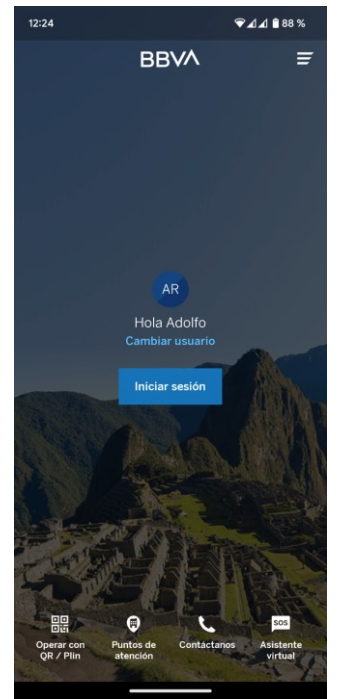


Auditability – Non-Repudiation

- Verify the entity that displayed the transaction details
- Use user's credential public key to verify signature
- FIDO2/WebAuthn+SPC: Check flags to know whether user was verified (“UV”)
- Look back when credential was created:
 - The user was known (ID proofing or legacy authentication method)
 - Verify aaid/aaguid to get more information about authenticator characteristics (if attestation was provided)

Takeaways

- FIDO can address the most common sources of Fraud in Payments
- FIDO can vastly improve the user experience resulting in less cart abandonment
- Some companies have already deployed FIDO in Perú (BBVA)
- Considerations:
 - Payment use cases differ from standard “login” use cases
 - One-size does not fit all – seek solutions that can address multiple use cases
 - Ability to assess and handle Authenticator characteristics (e.g., TEE use, single-device-credential vs. multi-device credential etc.)
 - Support for FIDO UAF Transaction Confirmation and Secure Payment Confirmation



THANK YOU

rolf@noknok.com

