Data Perceptions®

Digital Strategy and Transformation

Modern Workplace Authentication

Introduction to passkeys

Cybersecurity – Protect

passkey - what it is?

What is a passkey?

A passkey is used for Password-less sign-in.
It is a system generated digital credential based on modern cryptography tied to a user account and a specific website or application.

What is in a passkey?

A passkey is a collection of several pieces of information

Information received from the Website or Application

Website or Application Information	User Account Name	***sam@dataperceptions.com***	... Website/App Package
	Website/App ID	***example.com***	
	Website/App Name	***demo-site***	
	Other Information	**************	

Information generated by the system

Cryptographic Private/Public Key Pair	Private Key		Private key Public key
	Public Key		

Passkey Identifier	Credential ID	***Djfj679snbfyjfh5***	Credential ID

Counter	Start at 0	***00000***	COUNTER 000000

Cybersecurity – Protect

passkeys – Where are they stored?

Where are the passkeys stored?

passkeys are stored in an Authenticator(s)

AUTHENTICATORS

Android Phones and Tablets: Google Password Manager

iPhones iPads and Macs: iCloud Keychain

Password Managers:
1password, Bitwarden, LastPass, etc.
Password Manager Secure Vaults

Windows / Linux:
Intel and AMD platforms
Windows Hello TPM Module

Secure Keys:
YubiKey, Titan, Feitian, etc
Secure Modules

Sync (Software) passkeys

- Software passkeys can be available for use by a user on any device registered to the software Authenticator.
- Software passkeys can be synchronized to multiple devices.

Platform (Hardware) passkeys

- Hardware passkeys are restricted to the hardware device which created the passkey
- Each hardware module must get their own key

Passkeys can be added to multiple Authenticators for the same website or application

Data Perceptions®
Digital Strategy and Transformation

Cybersecurity – Protect

passkey – Sync (software) VS Platform (hardware)

Sync (software) passkeys

Google Password Manager

iCloud Keychain

Password Manager Secure Vaults

- □ Design for easy adoption of passkey technology
- □ Simpler for users to understand
- □ Can be applied to existing technology resources *(iPhones/iPads, Android, Password Managers)*
- □ Relatively low cost of deployment

Platform (hardware) passkeys

Secure Keys

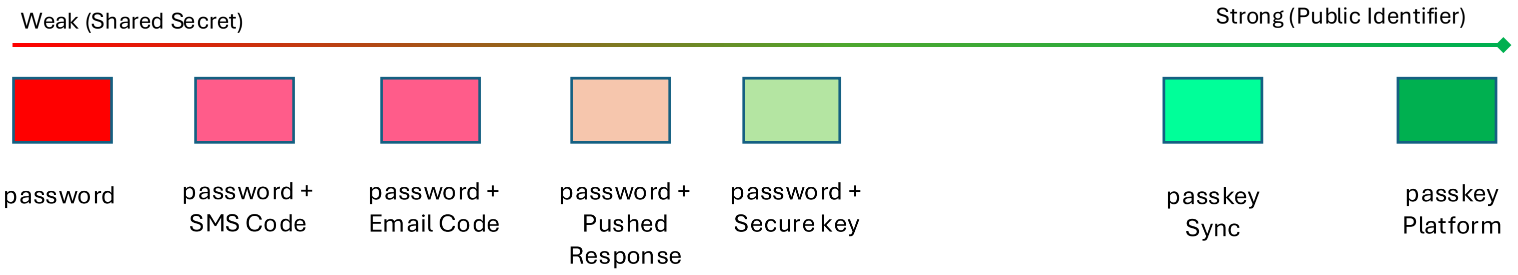
Windows Hello

- □ Recommend for roles where with higher security requirements *(Administrators, Executives, Developers, etc.)*
- □ Recommend minimum of two or more platform keys per user
- □ Cost of deployment is higher as there is a cost for each Authenticator

Cybersecurity – Protect

passkey – How secure are passkeys

Are passkeys more secure than passwords?



Weak (Shared Secret)

Strong (Public Identifier)

password

password + SMS Code

password + Email Code

password + Pushed Response

password + Secure key

passkey Sync

passkey Platform

- ❑ Passkeys are system generated, the user has no knowledge of the content
- ❑ Passkeys never leaves the hardware or software **Authenticator** that created it
- ❑ Passkeys are phishing resistant by design; the user account and destination information is included within the passkey any deviation will generate an alarm
- ❑ The **Secure Modules/Service** cannot be accessed by design. Request can be made for public information about the passkey
- ❑ The passkey must either be in the device or within Bluetooth range (30ft) of the devices that you are using to login
- ❑ There are no user passwords to be stored on the website or application servers
- ❑ Device PIN/Fingerprint/Face is required to use a passkey (Proof of user presence)

Cybersecurity – Protect

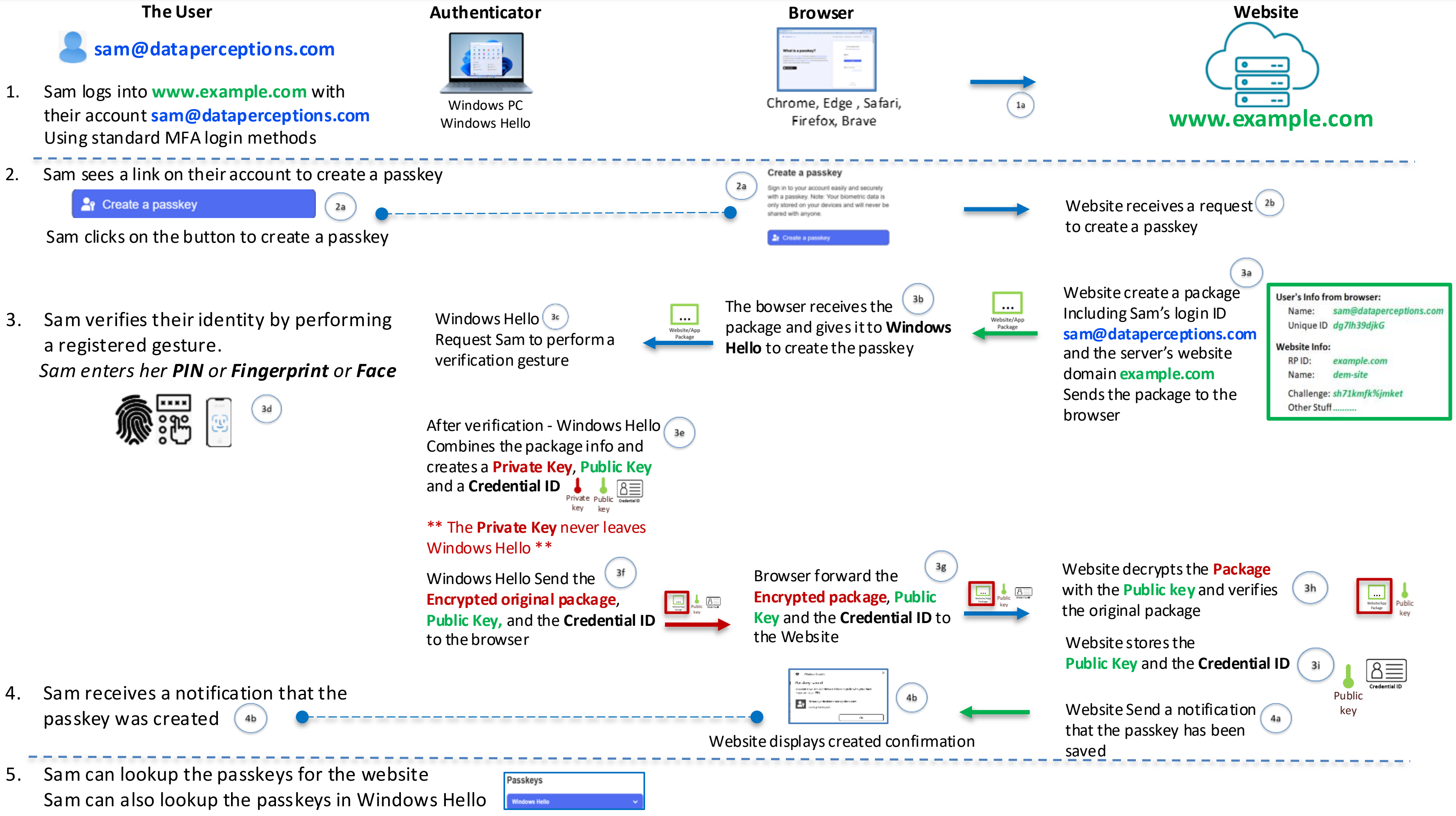
passkey – Challenges

The challenges of migrating to passkeys?

- □ Today, the user account must be authenticated before the user is able to setup a passkey
- □ Most websites or applications maintain both the password authentication and passkey authentication (confusing)
- □ Some websites replaces passwords with passkeys, still requiring MFA verification (*e.g.: amazon.com*)
- □ The passkey must either be **in** the device or **within Bluetooth range** (30ft) of the devices that you are using to login
- □ There can be confusion on where passkeys are stored and used
- □ There can be confusion on the use and limitations of hardware vs sync passkeys
- □ Passkeys are in a transition period (2025)

Cybersecurity – Protect

passkey – How are passkeys are CREATED



The User | **Authenticator** | **Browser** | **Website**

sam@dataperceptions.com

Windows PC
Windows Hello

Chrome, Edge , Safari,
Firefox, Brave

www.example.com

1. Sam logs into www.example.com with their account sam@dataperceptions.com
Using standard MFA login methods

2. Sam sees a link on their account to create a passkey

Sam clicks on the button to create a passkey

Create a passkey

Sign in to your account easily and securely with a passkey. Note: Your biometric data is only stored on your devices and will never be shared with anyone.

Website receives a request to create a passkey

Website create a package Including Sam's login ID sam@dataperceptions.com and the server's website domain example.com
Sends the package to the browser

User's Info from browser:
Name: *sam@dataperceptions.com*
Unique ID *dg7lh39djkG*

Website Info:
RP ID: *example.com*
Name: *dem-site*

Challenge: *sh71kmfk%jmket*
Other Stuff..........

The bowser receives the package and gives it to **Windows Hello** to create the passkey

Windows Hello
Request Sam to perform a verification gesture

3. Sam verifies their identity by performing a registered gesture.
*Sam enters her **PIN** or **Fingerprint** or **Face***

After verification - Windows Hello Combines the package info and creates a **Private Key**, **Public Key** and a **Credential ID**

** The **Private Key** never leaves Windows Hello **

Windows Hello Send the **Encrypted original package**, **Public Key,** and the **Credential ID** to the browser

Browser forward the **Encrypted package**, **Public Key** and the **Credential ID** to the Website

Website decrypts the **Package** with the **Public key** and verifies the original package

Website stores the **Public Key** and the **Credential ID**

Website Send a notification that the passkey has been saved

Website displays created confirmation

4. Sam receives a notification that the passkey was created

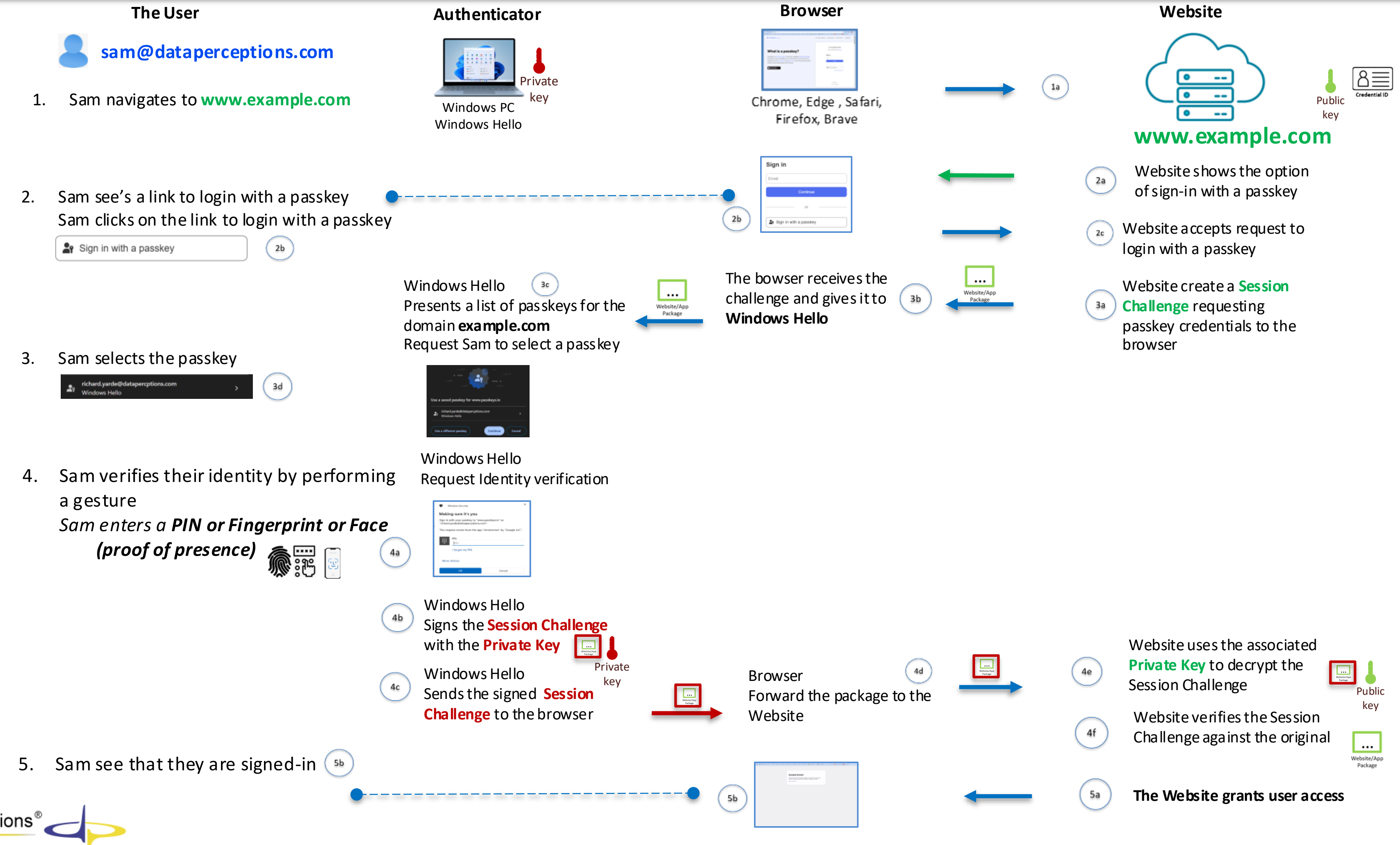
5. Sam can lookup the passkeys for the website
Sam can also lookup the passkeys in Windows Hello

Passkeys

Data Perceptions®
Digital Strategy and Transformation

Cybersecurity – Protect

passkey – SIGN-IN with a passkey



The User

sam@dataperceptions.com

1. Sam navigates to www.example.com

2. Sam see's a link to login with a passkey
   Sam clicks on the link to login with a passkey

3. Sam selects the passkey

4. Sam verifies their identity by performing a gesture
   *Sam enters a **PIN or Fingerprint or Face (proof of presence)***

5. Sam see that they are signed-in

Authenticator

Private key

Windows PC
Windows Hello

3c Windows Hello
Presents a list of passkeys for the domain **example.com**
Request Sam to select a passkey

Windows Hello
Request Identity verification

4b Windows Hello
Signs the Session Challenge with the Private Key

4c Windows Hello
Sends the signed Session Challenge to the browser

Browser

Chrome, Edge , Safari, Firefox, Brave

The bowser receives the challenge and gives it to **Windows Hello** 3b

Browser
Forward the package to the Website 4d

Website

www.example.com

2a Website shows the option of sign-in with a passkey

2c Website accepts request to login with a passkey

3a Website create a Session Challenge requesting passkey credentials to the browser

4e Website uses the associated Private Key to decrypt the Session Challenge

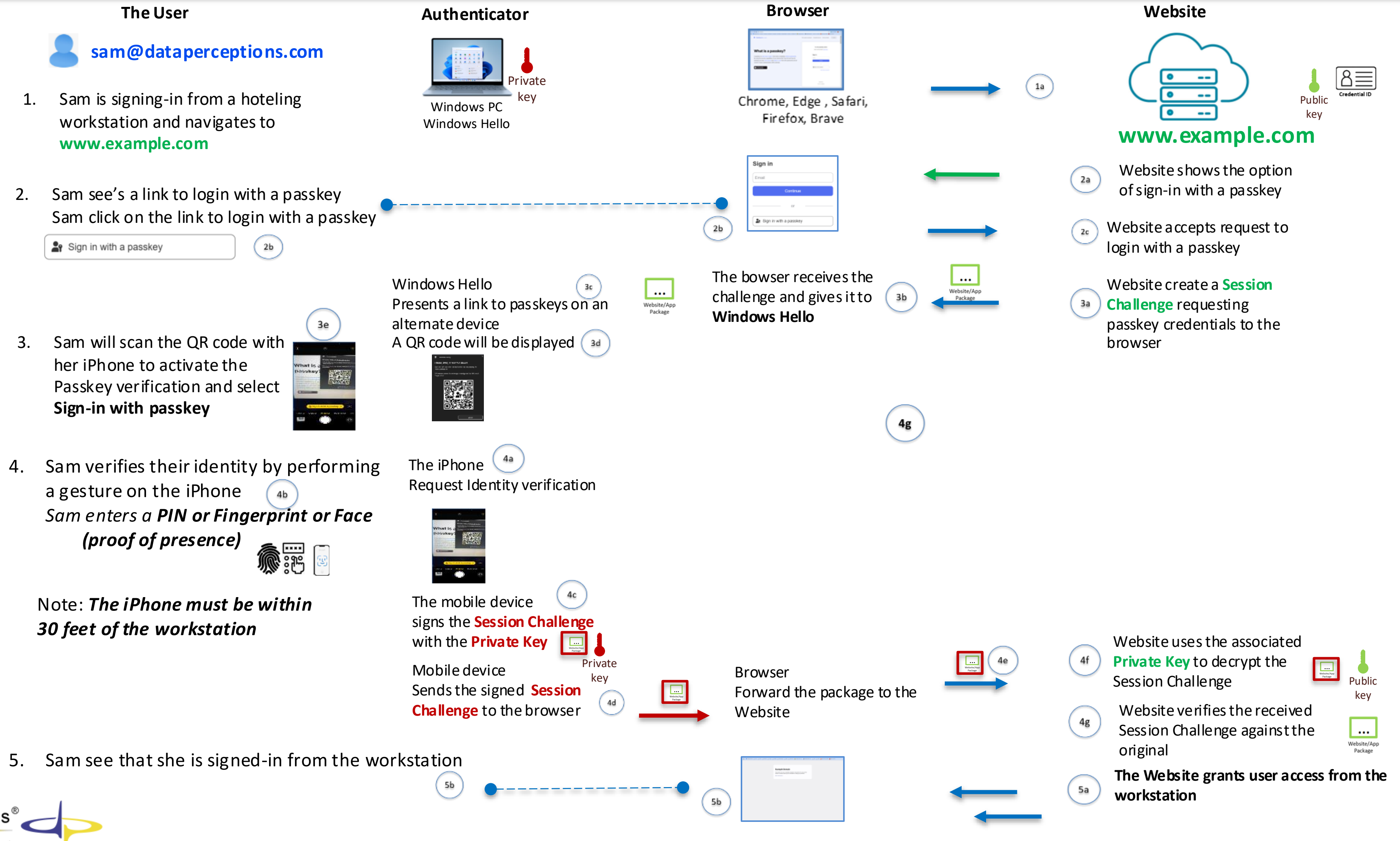
4f Website verifies the Session Challenge against the original

5a **The Website grants user access**

Data Perceptions®
Digital Strategy and Transformation

Cybersecurity – Protect

passkey – Cross-Device Sign-in with a passkey on devices which do not have a passkey



The User

sam@dataperceptions.com

1. Sam is signing-in from a hoteling workstation and navigates to www.example.com

2. Sam see's a link to login with a passkey
   Sam click on the link to login with a passkey

3. Sam will scan the QR code with her iPhone to activate the Passkey verification and select **Sign-in with passkey**

4. Sam verifies their identity by performing a gesture on the iPhone
   *Sam enters a **PIN or Fingerprint or Face (proof of presence)***

Note: ***The iPhone must be within 30 feet of the workstation***

5. Sam see that she is signed-in from the workstation

Authenticator

Windows PC
Windows Hello

Private key

Windows Hello
Presents a link to passkeys on an alternate device
A QR code will be displayed

The iPhone
Request Identity verification

The mobile device signs the Session Challenge with the Private Key

Private key

Mobile device
Sends the signed Session Challenge to the browser

Browser

Chrome, Edge , Safari, Firefox, Brave

The bowser receives the challenge and gives it to **Windows Hello**

Browser
Forward the package to the Website

Website

Public key

www.example.com

Website shows the option of sign-in with a passkey

Website accepts request to login with a passkey

Website create a Session Challenge requesting passkey credentials to the browser

Website uses the associated Private Key to decrypt the Session Challenge

Public key

Website verifies the received Session Challenge against the original

The Website grants user access from the workstation

Data Perceptions®
Digital Strategy and Transformation

Data Perceptions®

Digital Strategy and Transformation

Modern Workplace Authentication

How can Data Perceptions assist…

1. Fitting passkeys into your security strategies
2. Planning for passkey implementation