Passkeys! What are they? Navigating passkeys to passwordless security at scale

Joe Scalone
Senior Solutions Architect, Yubico
Co-Chair, *Government Deployment Working Group*, FIDO Alliance

yubico

Agenda

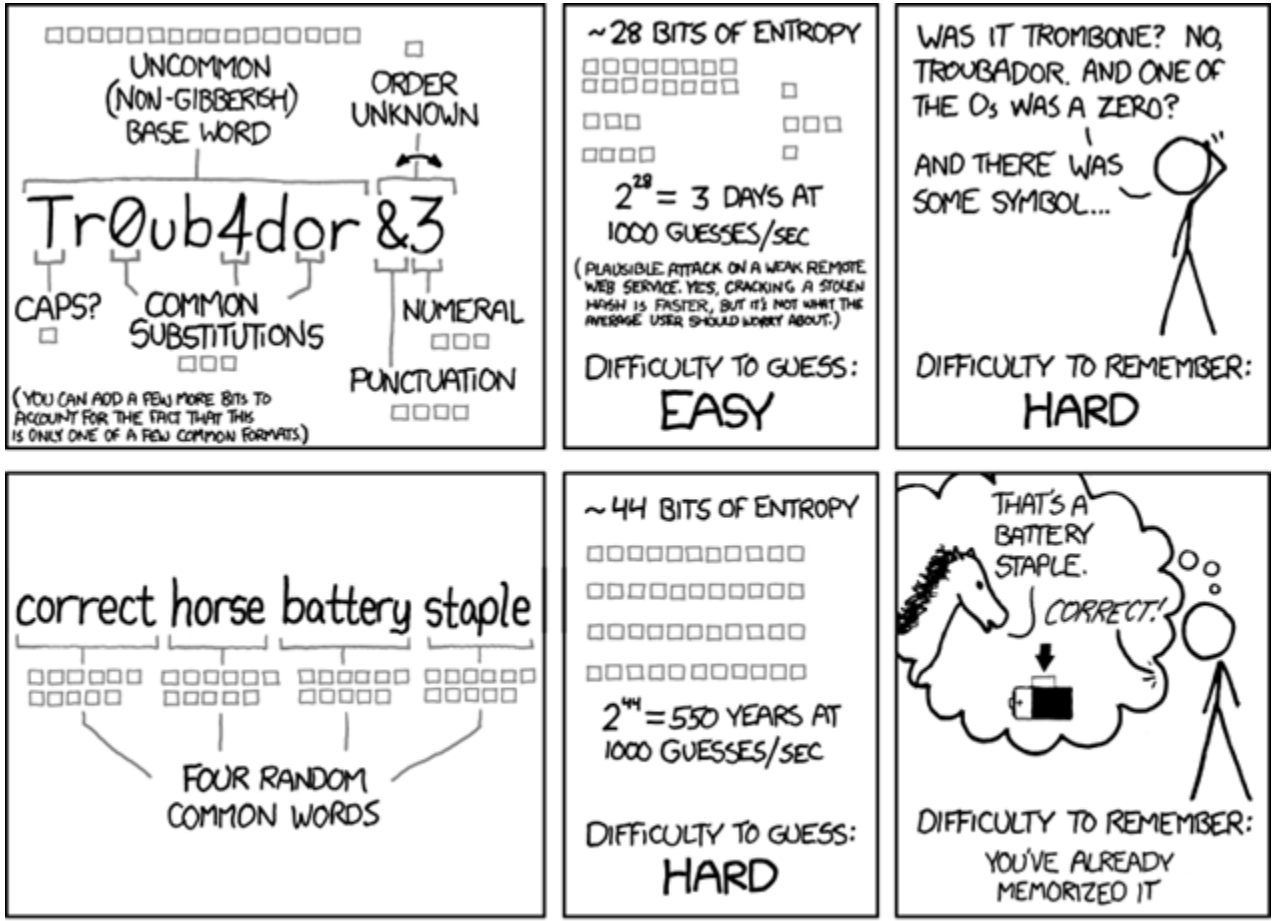
- Formalities
- What is a Passkey?
- Authenticator vs Credential
- Why Use Passkeys?
- A Change in Mindset
- Where are Passkeys used today?
- How to Passkey
- Passkey criticism and misnomers

Disclaimer

The views and opinions expressed in this talk are those of the speaker and do not necessarily reflect the views or positions of any entities they represent.

Who Am I

Joe Scalone is a Senior Solutions Architect at Yubico, committed to enhancing internet security. He focuses on providing secure login solutions for everyone and supports customers with Identity and Access Management (IAM) architectures to modernize authentication processes. Joe collaborates with technical partners and researches government regulations to develop specialized product architectures for the public sector. He co-chairs the Government Deployment Working Group and the US Government Deployment subgroup for the FIDO (Fast Identity Online) Alliance, where he contributes to standardizing FIDO implementations for governments in the US and globally.



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

What is a Passkey?

Passkeys

Accelerating passwordless across individuals and organizations

FIDO
An open security standard backed by the FIDO Alliance, a group focused on moving away from a password-based system.

Credential
The unique ID a user has that “gets you through the gate” when you log on to any system.

Passkeys

Enabling a move away from passwords

Passkey =

Discoverable FIDO credentials for passwordless

The relying party can identify a discoverable credential without knowing the user's ID in advance, as the user ID is embedded within the credential itself.

How passkeys are managed and used differentiate the "types" of passkeys.

FIDO Alliance

The FIDO Alliance is an open industry association dedicated to reducing the world's reliance on passwords. To achieve this goal, the FIDO Alliance advocates for the development of and adherence to authentication and device attestation standards.

FIDO2 is a secure, phishing-resistant, passwordless authentication protocol built on WebAuthn and CTAP2.

FIDO terms

- ***Device / hardware bound passkey*** - A credential tied to a single authenticator, such as a security key.

- ***Synced / multi-device passkey***- A credential that can be synced to more than one device. iCloud or 1Password are example transport mechanisms

- ***Hybrid Mode*** - The ability to use passkeys from one platform to another (Apple to Google for example)

- ***Authenticator*** - A device that holds credentials, PINs, attestation certificates and facilitates authentication
  - *Roaming* - stores device bound passkeys
  - *Platform* - stores multi device passkeys interacting with sync fabric

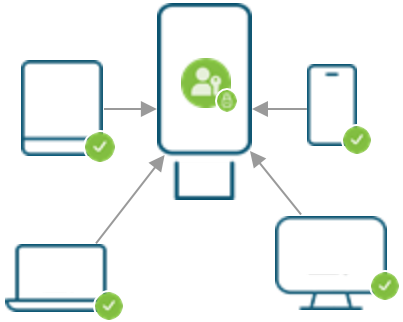
- ***Attestation -*** A certificate specific to a device model that can cryptographically prove that a user's authenticator is a particular device

Passkey Credentials Classes

Synced passkeys

Device-bound passkeys

(also referred to as hardware bound)



Syncable Passkeys

Synced passkey credentials are stored within a specific ecosystem and can be copied to approved devices like Apple's iCloud, Google, or 1Password.

Pros:

- Phishing-resistant authentication
- Limited attack surface: need to compromise service, user’s account, or sync fabric
- Credential automatically on device
- Credential recovery is managed by cloud service

Cons:

- Credential can only be used on owned devices
- Credential currently cannot be synced across multiple ecosystems
- Credentials are synced to devices on same account (i.e. family devices)
- Cloud accounts are typically managed by the individual and not the company

Synced Passkeys can be copied

Passkey credential can be copied to other devices by design

Pros:

- Easy to share credentials
- Can copy between ecosystems

Cons:

- A company has no control or visibility over a copied credential, leaving the user to decide with whom to share it. Those shared users, in turn, can copy the credential at will
- No restrictions on copying a credential, leading to potential loss of control over credential management

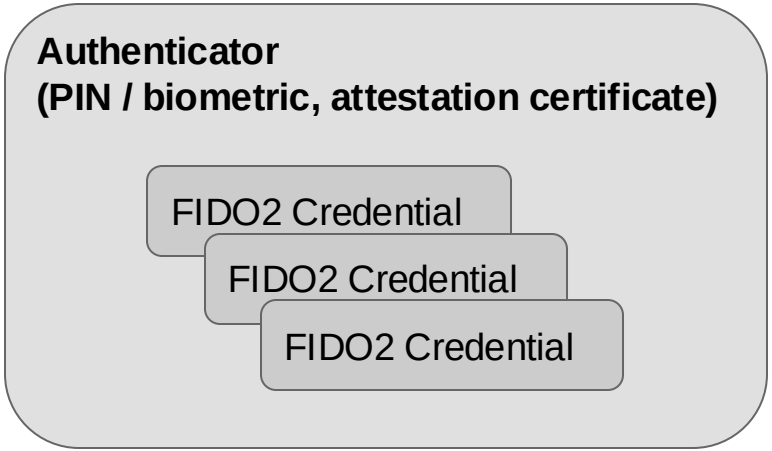
Authenticator vs Credential

Authenticator vs Credential

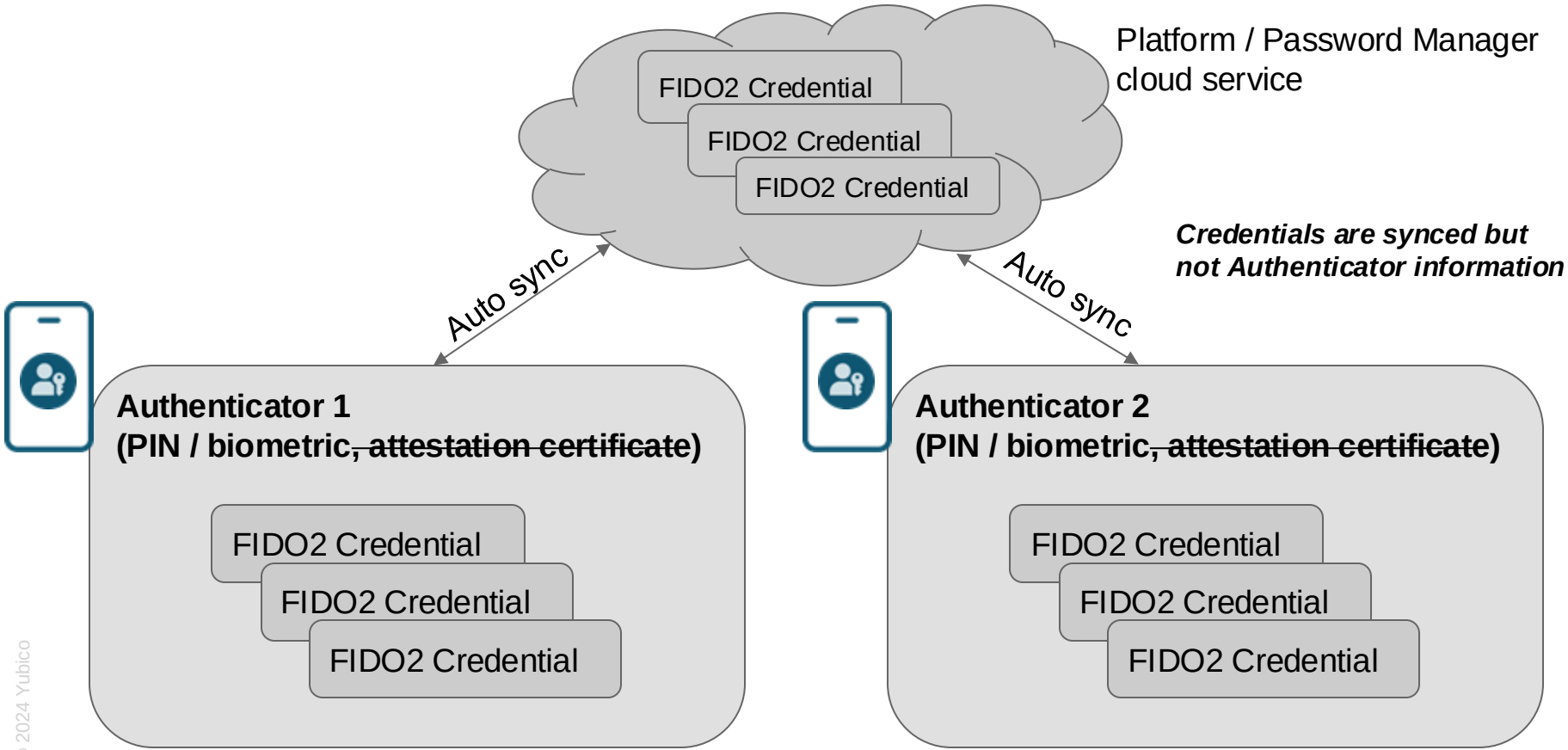
Authenticators are not credentials but create and control access to FIDO credentials

Attestation provides cryptographic proof that the authenticator created and controls the credentials.

Device attestation is only available for device bound authenticators.



What gets synced?



Back to Passkeys

Types of Passkeys

Device bound

- Not copyable; stays on single trusted device (authenticator)
- No device, no access
- Device attestation; highly provable security
- Can meet AAL3
- Can meet FIPS Level 2

Syncable / Backup enabled / Copyable

- Copyable; can be copied to other devices (ex. Air drop)
- Syncable; can be synced to a cloud account
- No device attestation
- Can meet AAL2 if designed properly on AAL2 sync fabric
- FedRAMP implications

Hybrid Transport

- Facilitates authentication and registration of passkeys from one device to another
- Leverages QR codes and Bluetooth capability to securely facilitate transfer
- Devices must be within BLE (Bluetooth Low Energy) range

Other terms and concepts

Device Public Keys (DPKs)

- A proposed extension to the WebAuthn specification that provides information about the device storing the synced passkey
  - DPKs do not control the syncing process but offer signals regarding the device that holds the synced passkeys

Sync fabric

- The hardware and software behind the synchronization of passkeys
  - Encompasses cross device and cross platform models
  - Describes how synched credentials move from one authenticator to another
  - Different nodes do not need to be aware of each other

Support for Passkeys

- Expect all platforms, IDPs, and password managers to provide passkey support and solutions
  - Vendors will differentiate based on credential management

- Passkey Information
  - https://passkeys.directory/
  - https://fidoalliance.org/passkeys/
  - Google's passkey talk at RSA
  - Devising Your Enterprise Authentication Strategy: Passkey Implementations and Tradeoffs
  - Our Take on Passkeys - Vittorio Bertocci (Okta)
  - Yubico Passkey workshop

Why use Passkeys?

Today attackers don't hack in, they login

Yahoo Announces 500 Million Users Impacted by Data Breach

BBC NEWS

Home | Queen Elizabeth II | War in Ukraine | Coronavirus | Climate | Video | World | US & Canada | UK

Tech

Holiday Inn hotels hit by cyber-attack

The New York Times

Uber Investigating Breach of Its Computer Systems

The company said on Thursday that it was looking into the scope of the apparent hack.

HELSINKI TIMES

Hacked Finnish psychotherapy service provider declared bankrupt

THE DISTRICT COURT of Helsinki has confirmed it has received a declaration of bankruptcy concerning Psychotherapy Centre Vastaamo, the Finnish provider of psychotherapy services whose client database was compromised in a hacking in November 2018.

ars TECHNICA

SolarWinds hackers have a clever way to bypass multi-factor authentication

Hackers who hit SolarWinds compromised a think tank three separate times.

TC

Twilio hackers breached over 130 organizations during months-long hacking spree

Carly Page

@carlypage_ / 1:00 am PDT • August 25, 2022

The Register

{* CYBER-CRIME *}

Now Oktapus gets access to some DoorDash customer info via phishing attack

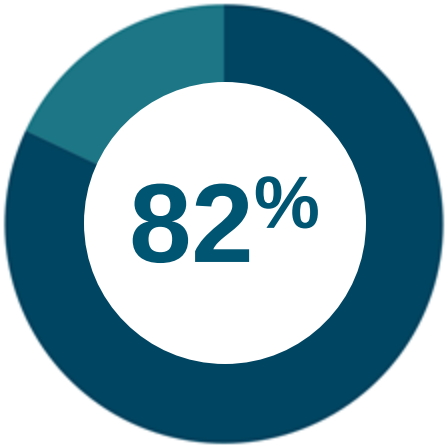
FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Enforcement

Home / Enforcement / Recent FTC Cases Resulting in Refunds

Equifax Data Breach Settlement

Verizon 2022 report



82% of breaches caused by stolen credentials

Source: 2022 Verizon Data Breach Investigations Report

Phishing, the biggest threat vector today

Source: Statista 2021

Worldwide Cost of Cybercrime in 2021

$6 Trillion USD

Phishing attacks are evolving

AI

Breaches

More laws/ regulations

Cybersecurity is expensive

Passwordless

Phishing-resistant MFA as a bridge to passwordless

A Change in Mindset…

User-centric authentication

The next frontier of authentication

From

Phishing-resistant authentication

To

Phishing-resistant users

Phishing-resistant user

Strong authentication that moves with the user

Across platforms

Across devices

Across business scenarios

Phishing-resistant users

Always secure as they live and work

- For every authentication task, the user uses phishing-resistant MFA
- Easily register new devices without calls to the help desk
- Work remotely without adding operational and security risk to the enterprise

Phishing-resistant users create phishing-resistant enterprises

Where are Passkeys used today?

Who has a passkey already?


Adobe
facebook
coinbase
DocuSign
GOV.UK
THE HOME DEPOT
DASHLANE
CVS
CAREMARK
GitHub
CLOUDFLARE
WORLD OF HYATT
INTUIT
instacart
IBM Security
TOYOTA
ROBLOX
ebay
PayPal
Vanguard
verizon
PNC
INTUIT turbotax
yahoo!
Proton
YouTube
NVIDIA
okta
Uber
salesforce
SAMSUNG
USAA
Synology
MERCARI
Robinhood
MERCK
Microsoft
NHS
intuit quickbooks
SK telecom
NETFLIX
KAYAK
mint
Google
NTT docomo
NESCAFÉ
GoDaddy
Discord
LOGIN.GOV
Bridgecrest
dinero.
Locker
LINE
BEST BUY
T-Mobile
Aflac
CVS Health
amazon
GitLab
Carnival

How to Passkey ?!?

Securing the enterprise user

Enterprise users have different authentication needs

Security Keys

Device Bound Credentials with Attestation

Platform Authenticators

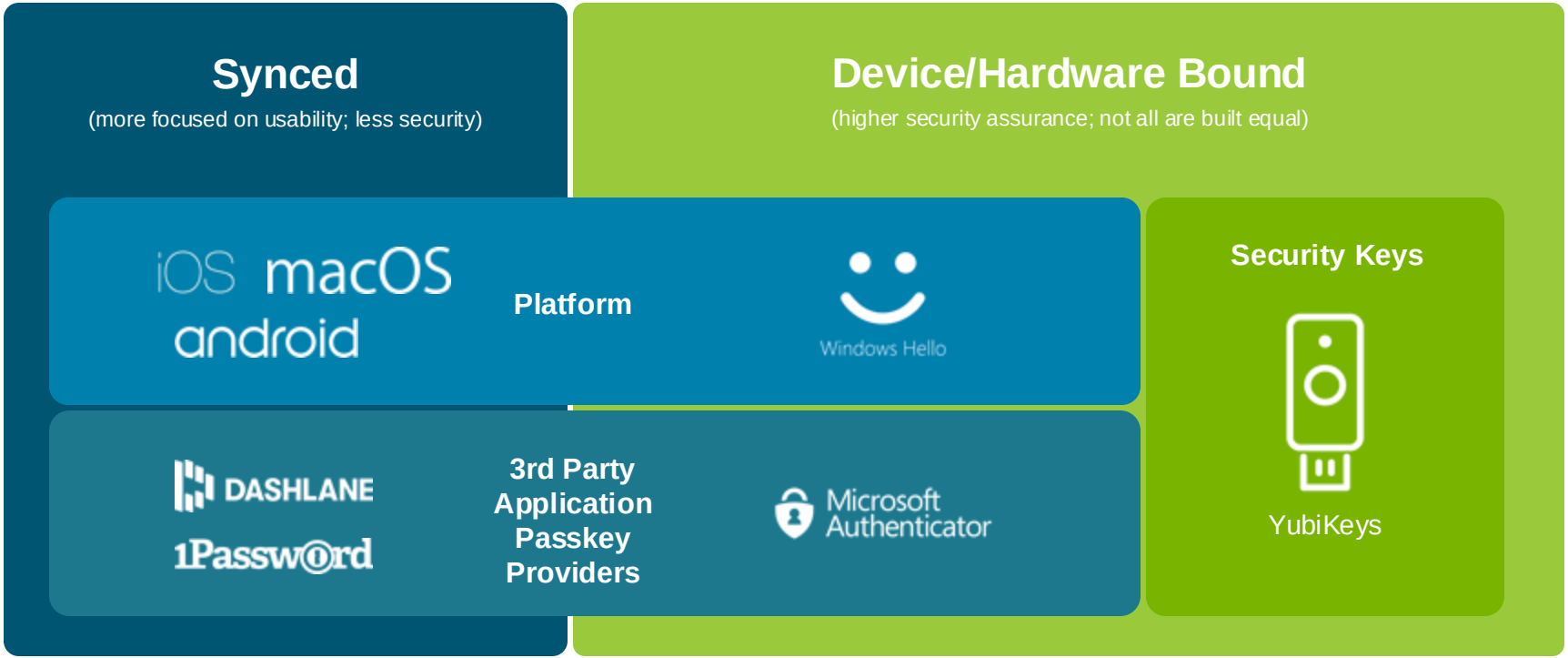
Authenticators built into your devices

3rd Party Authenticator Apps

Applications that provide user authentication solutions

The passkey toolbox

Not everything is a hammer



While going passwordless, enterprises need to consider

Credential lifecycle management

Onboarding/ registration

Credential recovery

Compliance, audit, risk

Criticism and Misnomers of Passkeys

- Too new
- Vendor Lock-in
- Does not stop every attack
- Too complicated
- Costly
- Password manager is good enough
- Single device reliance (device bound passkeys)
- Not supported
- MFA?

If not to Passkey, then what?

- Do nothing - keep using passwords
- Stronger passwords
- OTP
- Phone App
- Smart Cards
- Smoke signals
- Secret Handshake

Critical Takeaways

1

Passkeys represent a “new” technology aimed at replacing traditional passwords

2

There are numerous passkey solutions available, so it's essential to find the one that best suits your needs and enterprise requirements

3

Ensure you understand the security properties for all stages of the user lifecycle and clearly grasp risk acceptance within your enterprise

Q&A

Thank you!

joe.scalone@yubico.com

Learn more

Passkeys.org
Passkeys.io
Passkeys.dev

Ebook
Synced passkeys and pitfalls for the enterprise
yubi.co/syncedpasskeys

Ebook
Device-bound passkeys for the enterprise
yubi.co/deviceboundpasskeys

PASSWORD SECURITY, A SHORT STORY...