midwest
architecture community
collaboration

MIDWEST ARCHITECTURE COMMUNITY COLLABORATION 2020

NOVEMBER 5, 2020

Going Password-Less

Sorell Slaymaker
Principal Consulting Analyst @ TechVision Research

AGENDA

- **Intro** – Who is TechVision Research & Sorell Slaymaker
- **Passwords** – We all have stories on why they are bad
- **Stealing Passwords** – Top ways passwords are stolen
- **"Zero" Security Architecture** – Zero Trust & Zero Passwords
- **Options** – Can we really go Password-less?
- **Examples** – Solutions available on the market today
- **Zero Knowledge** – Adding ZKP to a password-less strategy
- **Next Steps** – Moving your enterprise towards Password-less
- **Q&A** – Let's play "stump the analyst" ☺

midwest architecture community collaboration

INTRODUCTION

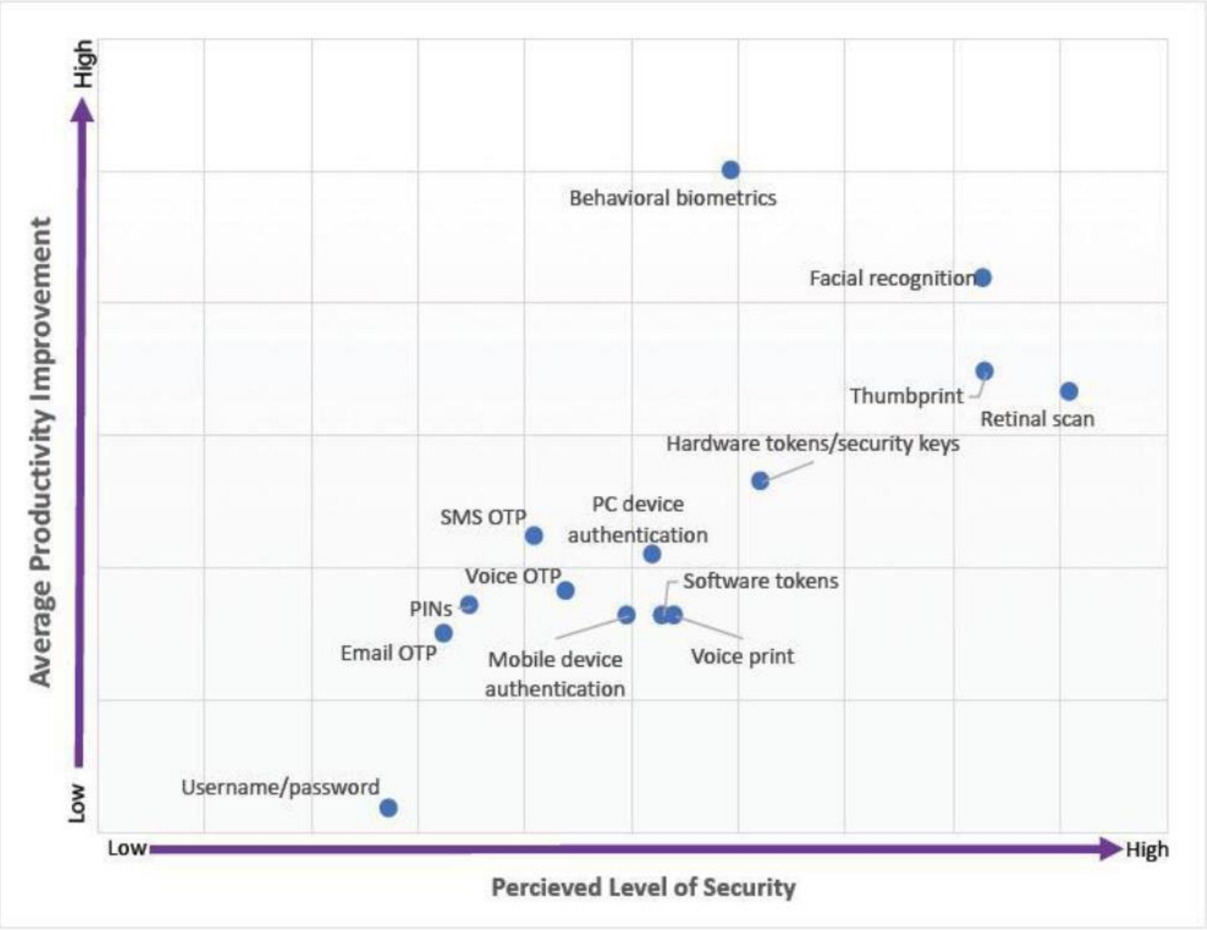
- **TechVision Research**
  - 30+ ex-Gartner Analysts – Burton Group -> GTP -> TVR
  - Focus on Digital Enterprise Strategies & Security
  - Research & Consulting – Primarily Global 1,000 clients
- **Sorell Slaymaker**
  - Principal Consulting Analyst @ TechVision Research
  - Focus on Network, Communications, Security Architecture
  - Worked for Target, United Health Group, Travelers, Gartner, AT&T
  - Based in the Twin Cities over by Stillwater
  - sorell@techvisionresearch.com

TechVision RESEARCH

midwest architecture community collaboration

THE CHALLENGE WITH PASSWORDS

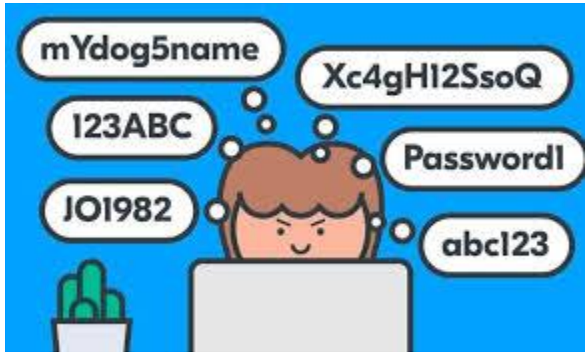
- Passwords are one of the least secure methods of authentication and very inconvenient
- 40-50% of Help Desk Tickets are password resets
- Password overload with average system admins having to manage over 50 passwords
- We all forget passwords and get frustrated getting our password reset
- There are better ways



midwest
architecture community
collaboration

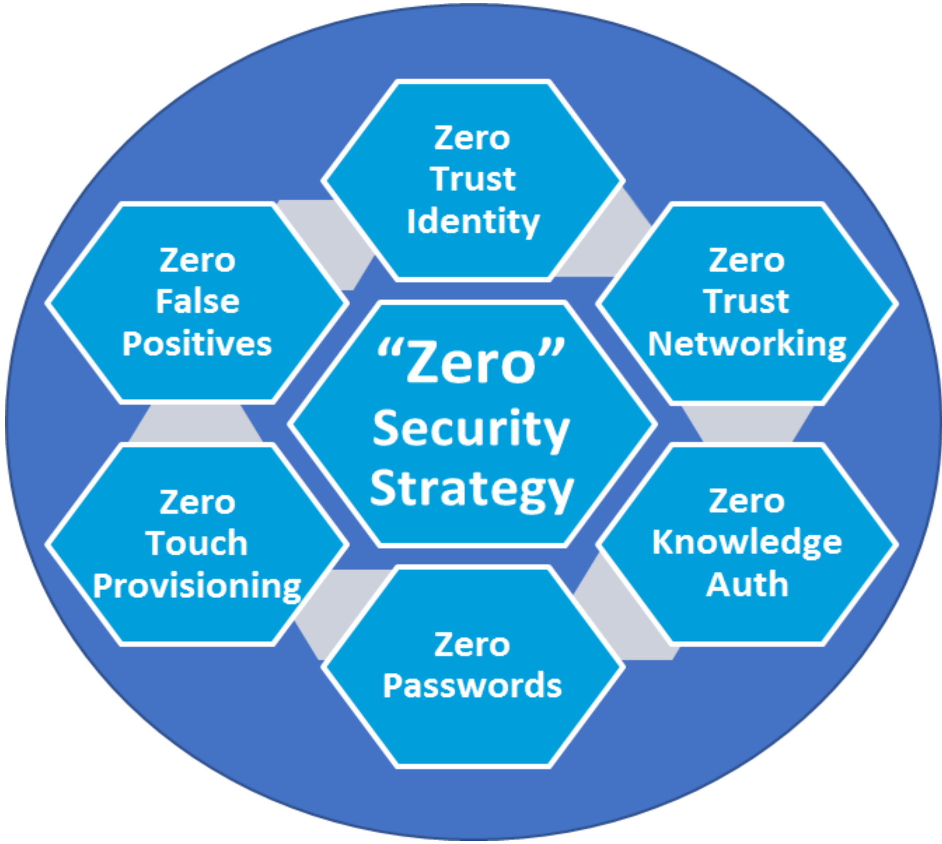
TOP WAYS OF STEALING PASSWORDS

- **Spear-phishing** – Targets a user or group of users and trick them into giving out private information including passwords
- **Surveillance** – Humans and video cameras are everywhere and watching what we do
- **Malware** – Loading key stroke logging software on a device and forwarding all key stroke activity to a remote server or to a rogue file that can be uploaded later. There are over 100,000 different key stroke logger malware variants, many of which are used and supported by government agencies, both domestic and foreign.
- **Password Resets –** In these scenarios, hackers can ascertain enough personal information from social media and then performs an SMS hijack
- **Guessing** – The oldest trick in the book, brute force attacks involve some level of guessing using simple passwords. Maga2020!
- **Force** – Bribing or threatening someone to give up their password. Hackers are becoming like spies and recruiting people to help them get information.



“ZERO” SECURITY ARCHITECTURE & ZERO PASSWORDS

- **Zero Trust Identity** – Ensures access is only granted to fully verified individuals.
- **Zero Trust Networking** – Standardizes on 1:1 micro-segmentation where users, devices, services, applications, and data must be authenticated and authorized to communicate with one another.
- **Zero Knowledge Authentication** – An interactive method for one party (the prover) to prove to another party (the verifier) that it knows the user and can authenticate and authorize them, without revealing anything about the user.
- **Zero Passwords** – Eliminating passwords, increasing security and giving employees and customers secure fast-track access to enterprise services, applications and data with zero sign-on technology. Coupling user and device identification with location, context, biometrics and device certificates delivers a more effective and efficient model.
- **Zero Touch Provisioning** – Automating provisioning and de-provisioning of users and devices for access to services, applications and data, with least privileged access and an automated way of handling exceptions.
- **Zero False Positives** – The Zero Trust model utilizes AI/ML in security information event management (SIEM) systems to understand the context and risks associated with security events.



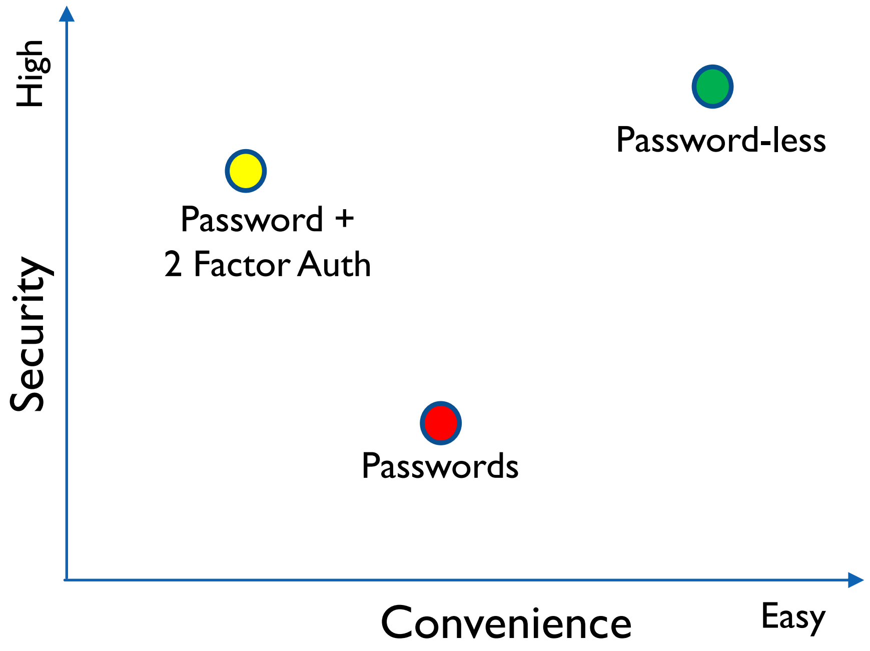
BALANCING HIGH SECURITY & USER CONVENIENCE

- If you do not make it easy and convenient, users will circumvent security controls
- Passwords are not going away, they just should not be the primary mode for authentication
- Authentication should have 6 dimensions

1. Something you know
2. Something you have
3. Something you are
4. Somewhere you are
5. Time
6. Context & Conditional

Traditional (1–3)

New (4–6)



midwest architecture community collaboration

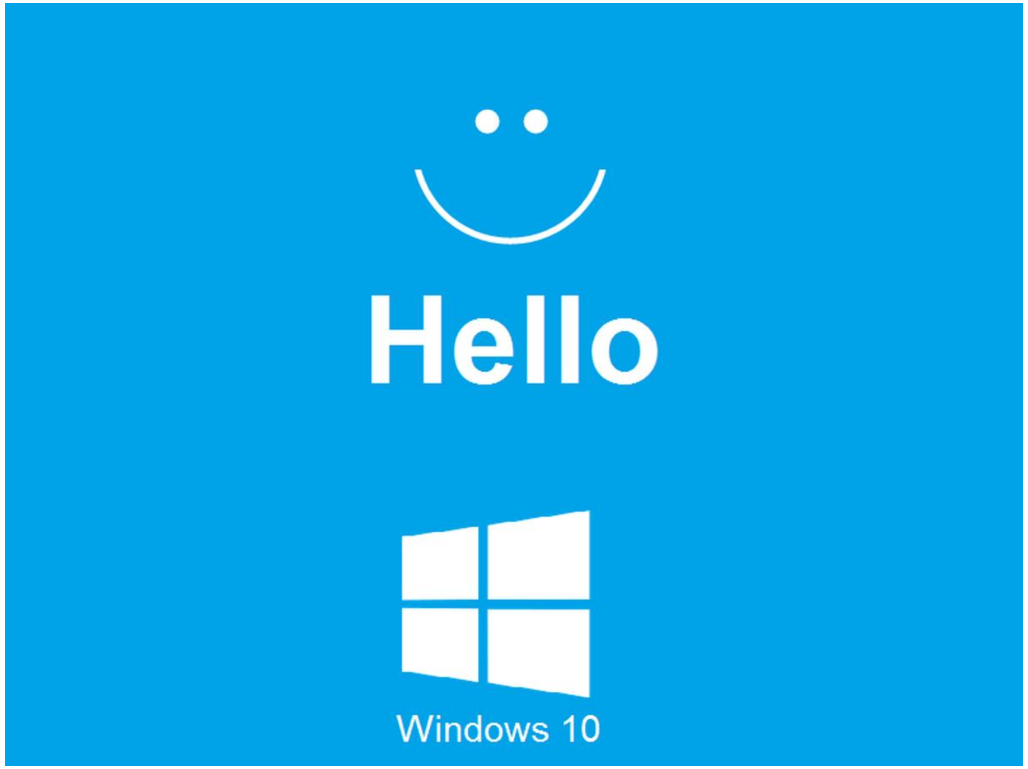
OPTIONS FOR GETTING RID OF PASSWORDS

- **MFA** – A great Multi-Factor Authentication strategy consists of utilizing multiple sources of identity along with a set of business rules and information that can dynamically identify the degree of certainty of a user's and devices identity. Certificates/tokens and biometrics work very well
- **JiT-PAM** – Just in Time Privileged Access Management means that system administrators – whether human or application functions, can be assigned privileges in near real time using their existing, or creating temporary, end-user accounts. JiT PAM limits the duration for which an account possesses elevated privileges and access rights in that the creation and deletion of an appropriate privileged account is assigned only to meet that specific period's mission objectives.
- **Contextual Awareness and Runtime Access Control -** contextual awareness pertains to the ability of the identity management system to determine certain characteristics about a user during runtime authentication and authorization and then using this information to both:
  - Measure the risk associated with the device, location, information sensitivity and the like during the authentication and authorization request and
  - Enforce specific policies regarding the type of authentication and identity information required to access the desired resource to better combat fraud.
- **Identity Governance and Administration (IGA) -** To be able to perform the requisite level of contextual awareness during runtime authorization, security systems must be able to access the data that supports the actual context. This means that the runtime authentication/authorization components must be able to reference "what good looks like" from a contextual standpoint.

A great MFA strategy consists of utilizing multiple sources of identity along with a set of business rules and information that can dynamically identify the degree of certainty of a user's identity, while also being convenient to the user.

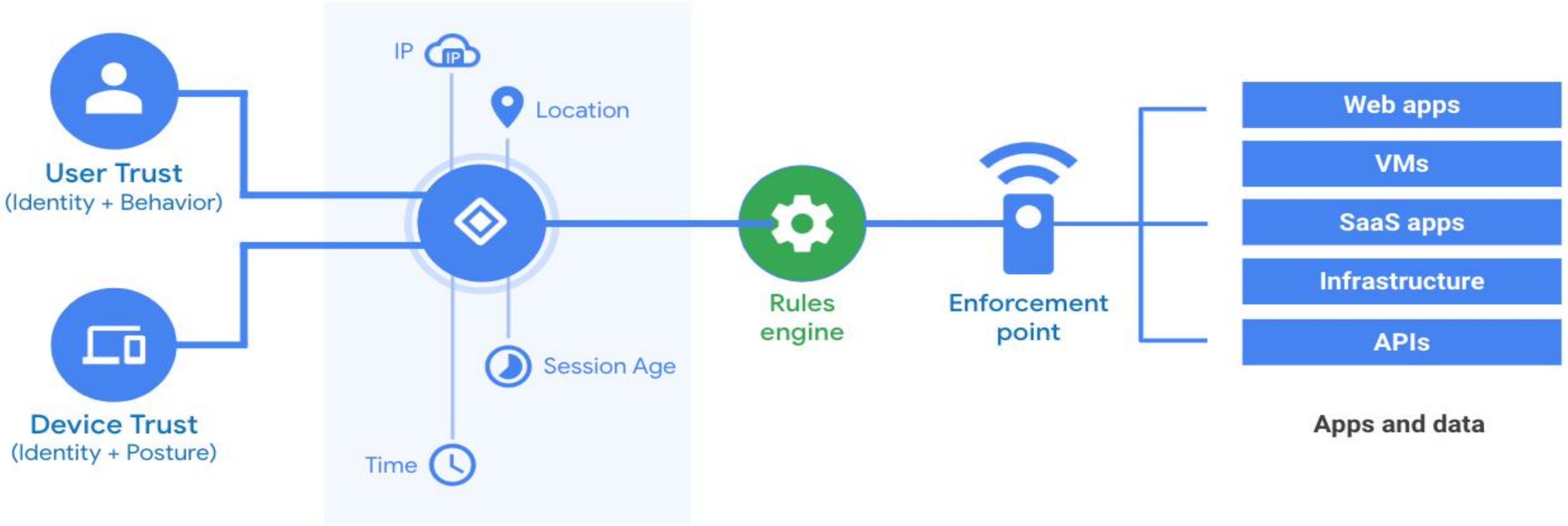
VENDOR EXAMPLE – MICROSOFT'S WINDOWS HELLO

- Biometrics based – Facial, fingerprint
- PIN vs Password
- Why a PIN is better than a password
  - Tied to specific device with a Trusted Platform Module chip which is a secure crypto processor
  - PIN is just to local device, not sent to a server and someone must get the physical device to get into it
  - PIN can be simple or complex depending on security requirements
  - PIN does not need to be changed on a regular basis



VENDOR EXAMPLE – GOOGLE’S BEYOND TRUST

BeyondCorp is a Zero Trust Policy Based Management System framework originally created by Google that shifts access controls from the perimeter to individual devices and users, thereby aligning with ZT and password-less models. The BeyondCorp Framework enables real-time authentication and authorization of users, devices, and resources to allow employees to work securely from any location without the need for a traditional VPN.

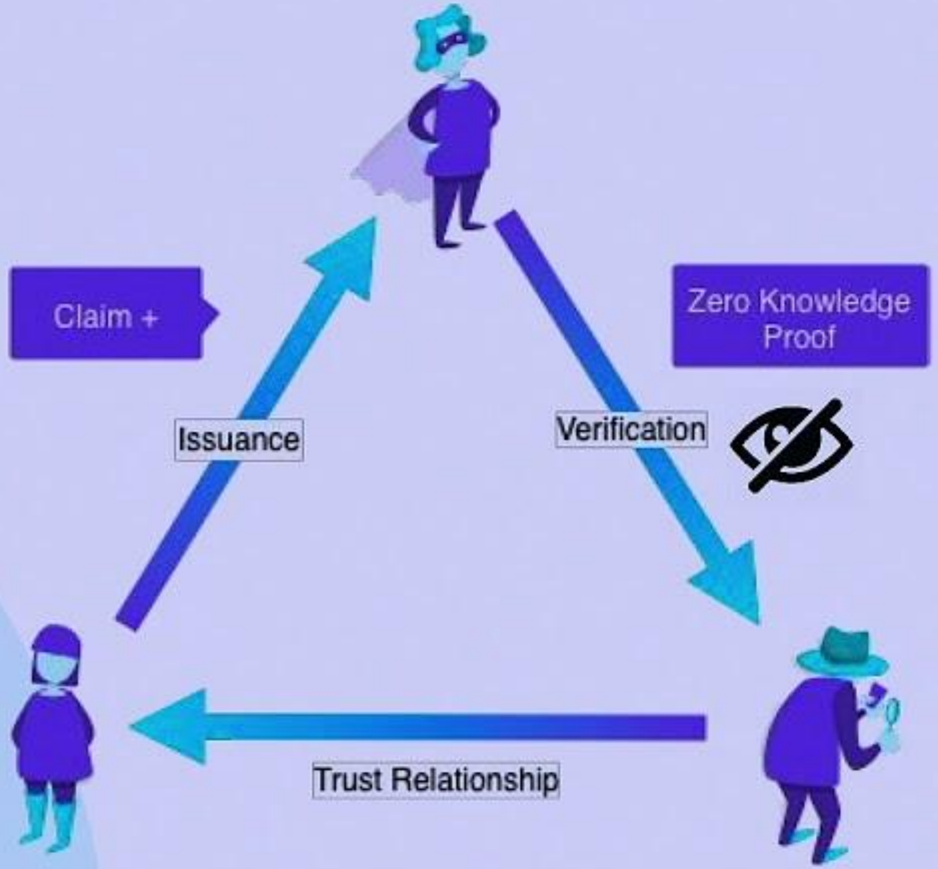


midwest architecture community collaboration

Privacy:
Zero-knowledge proofs

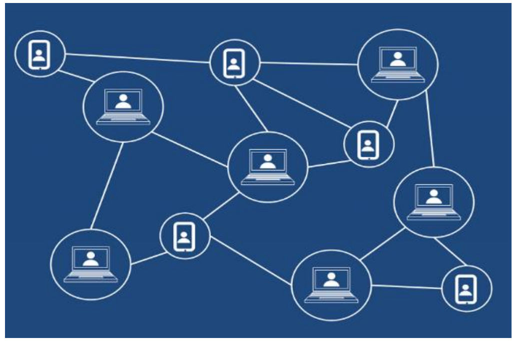
You can prove something **without revealing** unnecessary information:

- Prove you paid your taxes.
- Entrance to a nightclub proving that you are 18+ .
- Anonymous voting.
- Participate in an ICO anonymously but with the warranty that a 3rd party KYC'd you.



ADDING ZERO KNOWLEDGE PROOFS TO PASSWORD-LESS

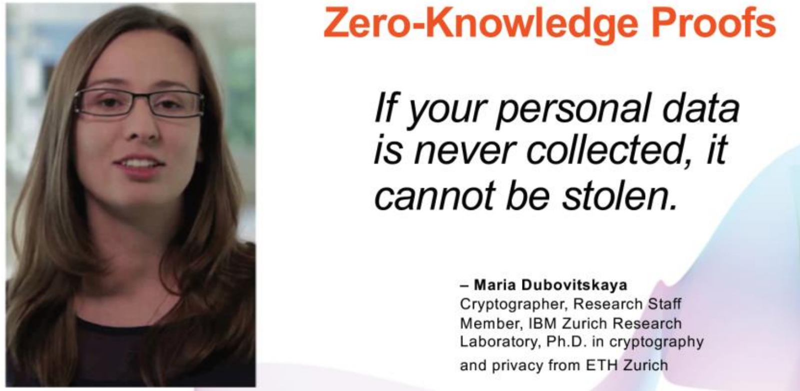
Smart Phone Biometrics (Facial, Finger, Behavioral) Plus Location and SMS



Stop Creating Central Databases With Private Information That Can and Will Get Hacked

Zero Knowledge Trusted Identity Verification

Faster, More Convenient, Ultra-Secure Identity Authentication



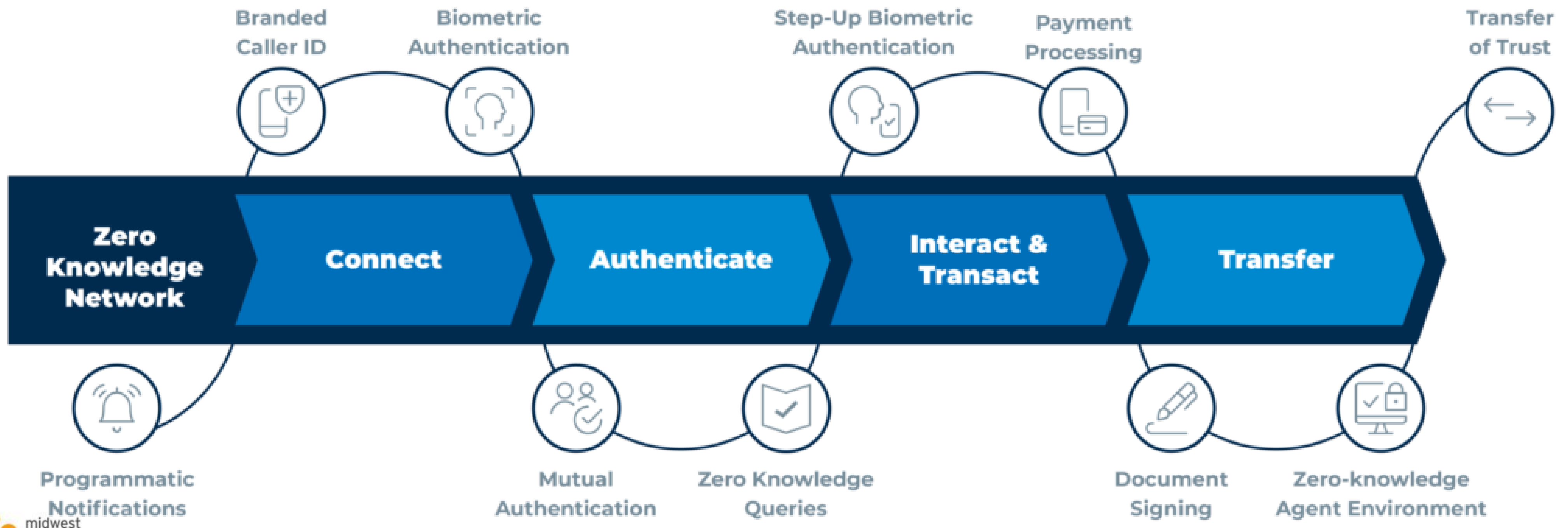
Zero-Knowledge Proofs

If your personal data is never collected, it cannot be stolen.

– **Maria Dubovitskaya**
Cryptographer, Research Staff Member, IBM Zurich Research Laboratory, Ph.D. in cryptography and privacy from ETH Zurich

VENDOR EXAMPLE – JOURNEY.AI

Zero Passwords and Zero Knowledge authentication for a private, secure, convenient interaction with a bank for example across any form of communication from a smart device



midwest architecture community collaboration

COMPANIES GOING PASSWORD-LESS

Share Your Story of Going Password-less

NEXT STEPS

- Identify Use Cases
- Determine Where Your Enterprise Sits
  - Adoption – Early, Mid, Late Adopter
  - Competitive Advantage – H, M, L
- Craft a Pilot & Test Solutions
  - Internal
  - External/Consumer

Someday our future self will be watching an old movie and realize that back in the old days, people had to remember passwords ….

Q&A