Five

# All Biometrics are not the same

# Who is the changeme of Biometrics

Andy Milton

Hitachi Security
Business Group

HITACHI
Inspire the Next

# Why passwords need to go?

PayPal

“Passwords, when used ubiquitously everywhere at Internet scale are starting to fail us. Users will pick poor passwords and then they'll reuse them everywhere. That has the effect of reducing the security of their most secure account to the security of the least secure place they visit on the internet.”

**Michael Barrett,**
Chief Information Security Office (CISO) of Paypal

Google

“Companies looking for ways to keep their users secure should know one thing Passwords are dead. In the future, the game is over for anyone that relies on passwords as its chief method to secure users and their data.”

**Heather Adkins,**
Google’s Manager of Information Security

Microsoft

“There is no doubt that over time, people are going to rely less and less on passwords. People use the same password on different systems, they write them down and they just don’t meet the challenge for anything you really want to secure.”

**Bill Gates**
Microsoft Founder

mastercard.

As we shift towards using digital services, and the need to protect our data becomes ever more critical, the use of passwords is woefully outdated.

Many people simply have more passwords than they can remember and forget them, or worse use the same one for all their accounts. In payments technology, we are moving from cash to card, and password to biometrics. It’s far easier to authenticate yourself with a thumbprint or a selfie, and it’s safer.

New payments regulation will speed the adoption of biometrics. We will all need to authenticate ourselves more frequently when buying online, and passwords just won’t be good enough.

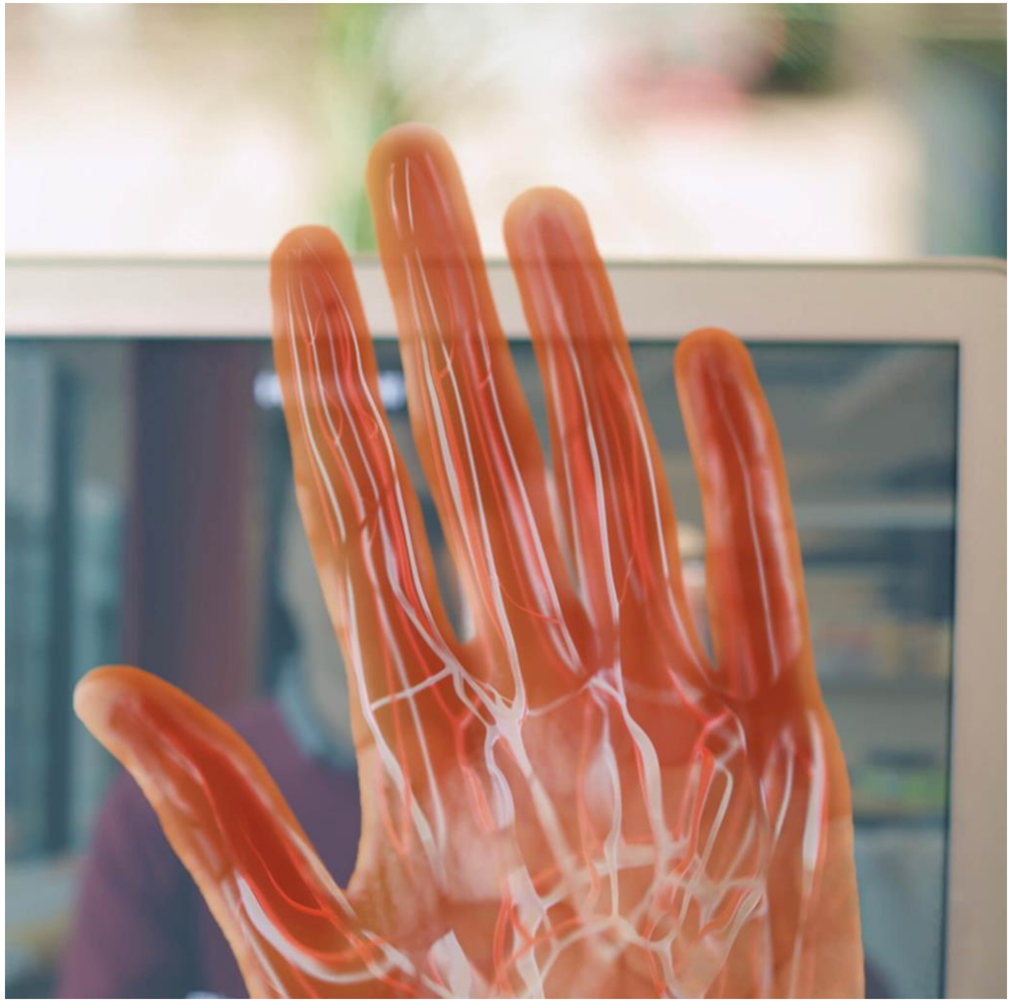
We estimate that one in four online purchases will need a one-time password or code, or some form of biometric authentication. This is a huge jump from the one in 100 of online payments that need further checks today. Given the choice, for many consumers the simplicity, speed, and convenience of biometrics means that it will not be a hard decision to make.

**Ann Cairns**,
Vice Chairman of Mastercard

# Why Biometrics?

- Proof of real identity
- Passwords are not working……. Complexity, reuse, breached, shared, stolen
- 2Factor – is good but complex- Part of Blended Solution
- Neither prove Identity they just prove knowledge or possession.
- User experience is key – Where, when, how, speed
- Managing Personal Data is challenging
- Biometrics have become accepted – Phones
- Face, Finger print, Iris, Finger Vein, Hand, Palm, Voice and others

# Are all Biometrics Equal



- FAR, FRR, their relationship
- PAD and Liveness detection
- Speed vs quality
- Right Biometric for the use case
- Complicity in reading and capture

- Manging the risk across different Biometrics
- Suitability for Different Environments
- Adaptability physical attributes
- Accessibility to services
- Blending of Biometrics and other techniques
- Security posture of blended.
- Never Storing images or templates or PPI

Operating system login

Banking and Payments

PKI backed transaction and document signing

Access control / time and attendance

ATM transactions

Retail payment solutions

Five

# Thank you

**Hitachi Europe Limited**
**T:** +44 (0) 1268 585000
**E:** veinid@hitachi-eu.com
**W:** hitachidigitalsecurity.com

# Why password replacement?

**83% of IT decision makers predict their organisations will be password-less in the next five years.**

**Gartner 2019**

# Why have passwords lasted for 60 years

**User experience is key**

- Employees need to carry secure tokens and remember PINs.
- Complexity leads to problems
- Management and recycling

**Additional hardware**

- Apps on Phones
- Additional devices to be carried or forgotten
- Tokens
- Smartcards

**Weakest Link**

- Phishing
  - Password Stuffing
  - Running Cost: Operational cost of password resets
  - Constant changes
  - Lost productivity

Password stuffing

VeinID Hand gesture Fast

2 factor Complicated

Complacency Lost hardware Costs

Slower Annoying

User experience is the king ROI

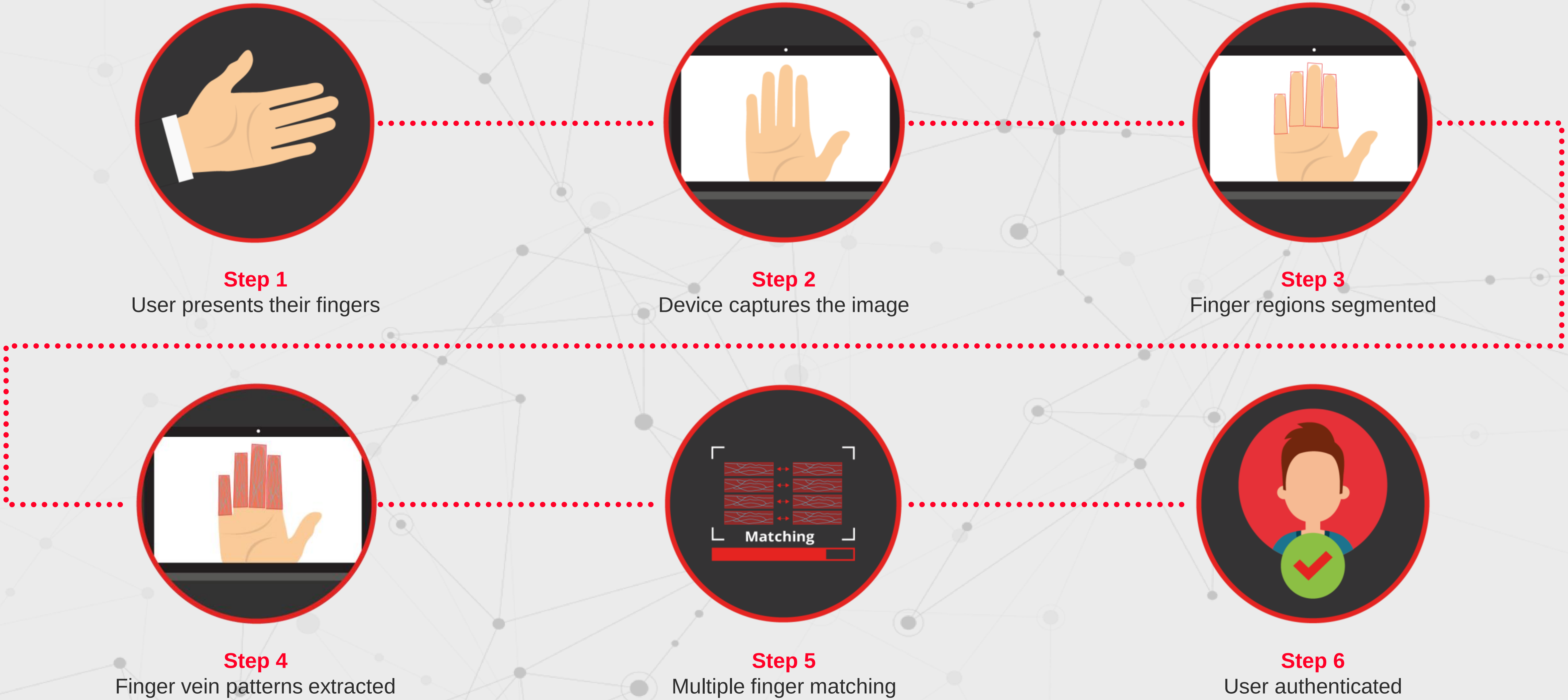
Focusing on the business problem

Nothing Additional Hardware

Frustrating Mobile Security

Budget Phishing

# How it works



**Step 1**
User presents their fingers

**Step 2**
Device captures the image

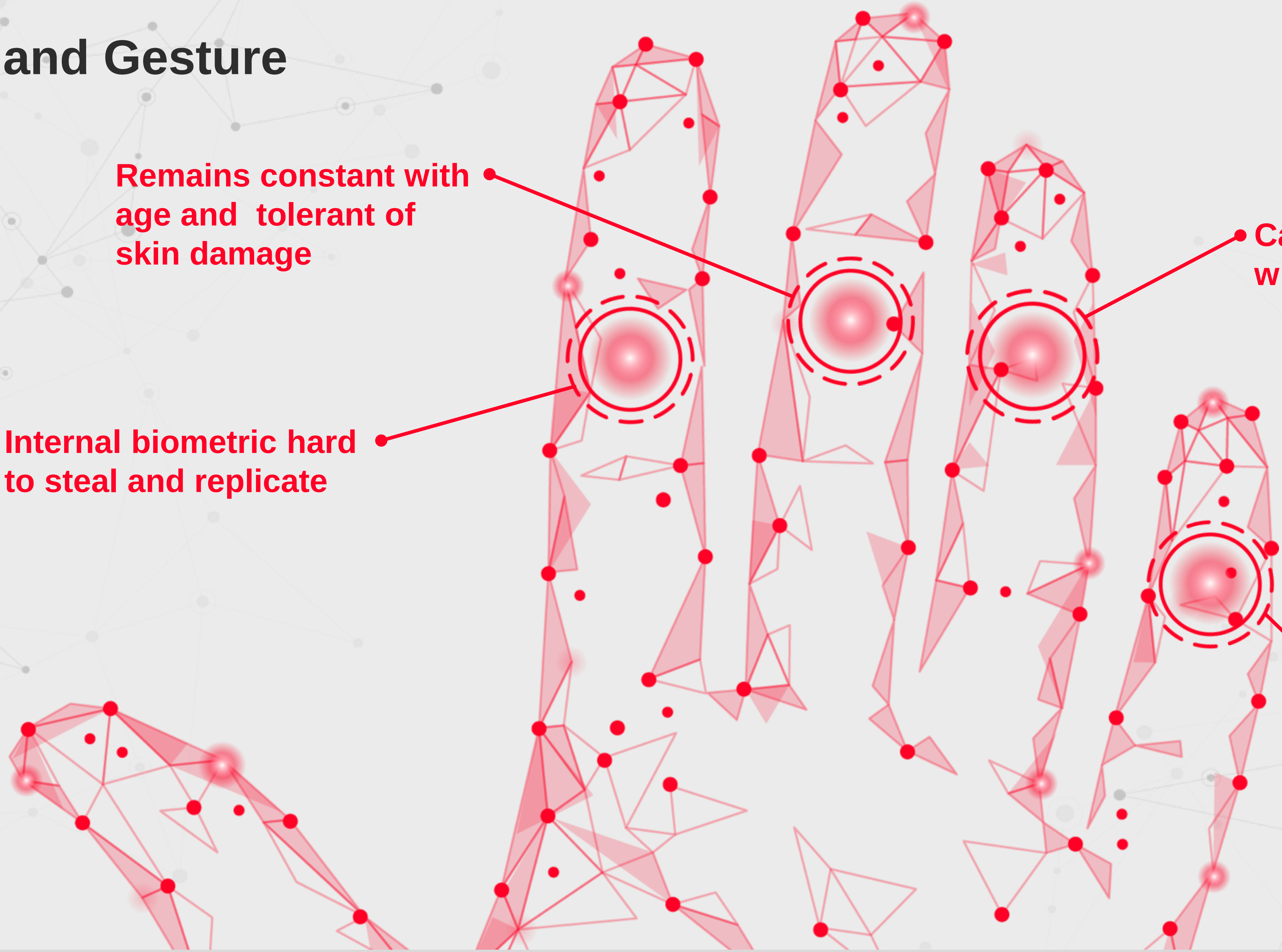
**Step 3**
Finger regions segmented

**Step 4**
Finger vein patterns extracted

**Step 5**
Multiple finger matching

**Step 6**
User authenticated

# About Hand Gesture



Remains constant with age and tolerant of skin damage

Captured and read without contact

Internal biometric hard to steal and replicate

Needs bloodflow to function