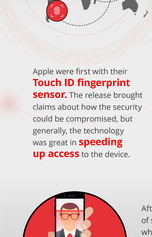
Hitachi Digital Security

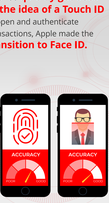
MOBILE AUTHENTICATION WITH CAMERA PHONE FV

VEINID



The growth in the use of **biometrics in the mobile channel** and the innovation towards using **different biometric modalities** shows no signs of slowing down.

Apple were first with their **Touch ID fingerprint sensor.** The release brought claims about how the security could be compromised, but generally, the technology was great in **speeding up access** to the device.

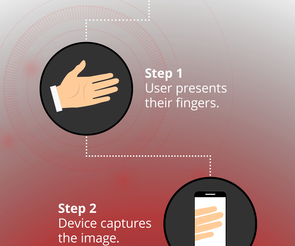


After **capturing an audience** of several hundred million users who had **quickly got used to the idea of a Touch ID** to open and authenticate transactions, Apple made the **transition to Face ID.**

With Face ID boasting a **far higher accuracy rate** than Touch ID, it was a no brainer for **Apple to move** to face recognition.

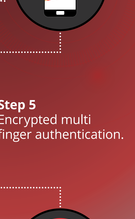
As Apple Pay was **established as a payment tool**, the optional use of Touch ID and Face ID instead of passcodes meant millions were seamlessly **transitioned over to biometric authentication.**

The problem now for service providers is **how to deploy standardised authentication tools** in their Apps across the two main mobile platforms that **doesn't compromise privacy regulations and protects against identity theft.**



Hitachi's **next generation solution** based on the award-winning finger vein authentication technology, aims to contribute to a **safer and more secure society.**

It can be used by **any device equipped with a digital camera** (smart phone, tablet, laptop etc.) to easily **authenticate users by their finger vein patterns** in a fast, simple transaction.



The goal of the service provider is to "know your customer". Hitachi's solution addresses this by performing the **authentication in conjunction with the service provider.** It means that the authentication step stays clearly in the **control of the service provider.**

See how it works below.

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
Encrypted multi finger authentication.

Step 6
Customer authenticated.

With deep knowledge of **cybersecurity, biometrics and banking security,** and having the related tools that **secure many enterprises,** Hitachi is able to ensure that fast and flexible user authentication can be **served up in the safest and most practical way.**

To speak to us about how our solutions can be part of a multi-factor program for securing the mobile channel, contact us at **Banking.Solutions@hitachi-eu.com**

HITACHI
Inspire the Next