

HOW TO SOLVE THE STRONG CUSTOMER AUTHENTICATION REQUIREMENT WITHIN PSD2?

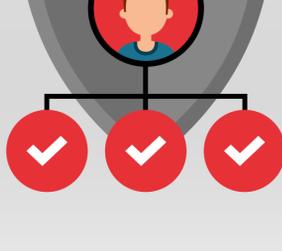


VEINID



The **Second Payment Services Directive (PSD)**, or PSD2 as it is commonly known, was implemented in January 2018. It aims to bring the original Payment Services Directive from 2007 **up to date** with the digitalisation and innovation agenda that is now widespread throughout the payment services industry.

PSD2 is a force for **good for consumers** by improving security and hoping to **address the fast growing problem** of banking and payment fraud.



PSD2 defines customer authentication as “the **validation of the identification** of a person based on two or more elements categorized as **knowledge, possession and inheritance** that are independent.”

What does that mean practically?

- **Knowledge** = something you know. A passcode or PIN, for example.
- **Possession** = something you have. A SIM card or a cashpoint card.
- **Inherence** = something you are. Biometric information, such as a finger scan



Just one of these elements **on its own isn't very secure**. For instance, something you know such as a **login passcode could be stolen** and **used by someone else**.



“For ultimate protection, you really need all three layers. That means biometric technology is going to **become increasingly important.**”

Ravi Ahluwalia,
Deputy General Manager,
Information Systems Group.

The role of **biometrics in banking is expected to grow** dramatically with Goode Intelligence predicting that by the end of 2020, **1.9bn bank customers around the world** will be using biometrics.



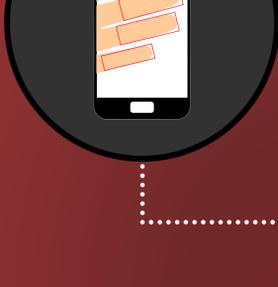
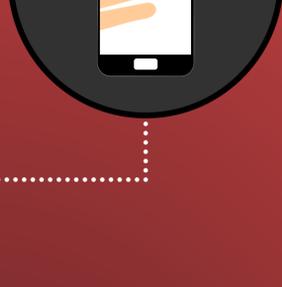
The **next generation of VeinID** takes things to a whole new level. Allowing finger vein data to be captured using a digital camera, **the ability for consumers to use privacy compliant biometrics in everyday transactions** without any special devices or tokens being issued by a bank, will become a reality.

See how it works below.



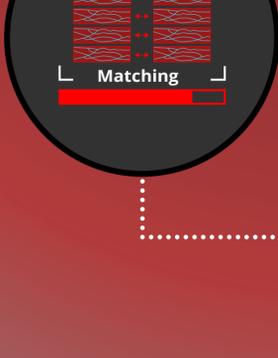
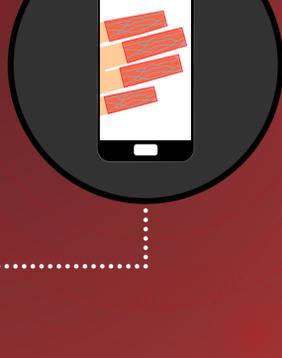
Step 1
User presents their fingers.

Step 2
Device captures the image.



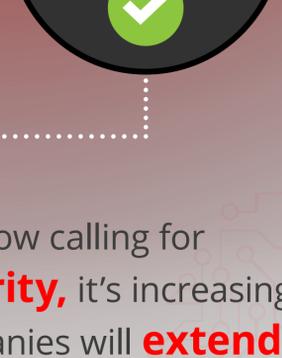
Step 3
Finger regions segmented.

Step 4
Finger Vein patterns extracted.



Step 5
Multiple finger matching.

Step 6
Customer authenticated.



With legislation now calling for **more rigorous security**, it's increasingly likely that more companies will **extend their offering to include biometrics like Hitachi's VeinID**.

To make the most of the opportunities in this digital business era, contact us at **Banking.Solutions@hitachi-eu.com**