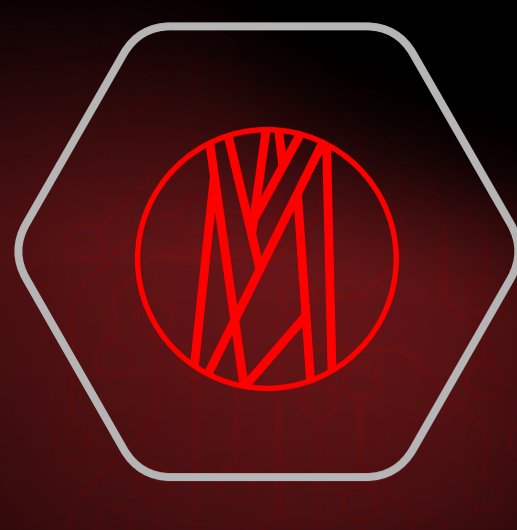
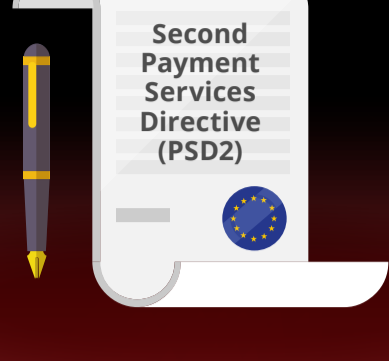


MULTI-FACTOR AUTHENTICATION

WHAT DOES IT REALLY MEAN?



VEINID



The law now calls for **multi-factor authentication** to keep payments safe — but what does this really **mean**?

PSD2 defines authentication as “A procedure for the **validation of identification** based on the use of **two or more** elements categorised as **Knowledge, Possession** and **Inherence** that are independent”



KNOWLEDGE

Knowledge is **something you know** – a username, password or PIN number

Possession is **something you have** – a mobile phone for a One Time Password text message (OTP SMS) or a hardware security token



POSSESSION



INHERENCE

Inherence is **something you are** – biometric information such as a finger print or iris scan

Just one of these elements on its own **isn't very secure** – for **ultimate protection**, you really need **all three**

ONE-FACTOR AUTHENTICATION



A **username** and **password** can be **phished, stolen** or even **guessed**, so it's really not secure

TWO-FACTOR AUTHENTICATION

Combining a password with an **OTP SMS** or **RSA token** makes it **stronger** – but SIM cards can be **cloned** and keyfobs can be **stolen**



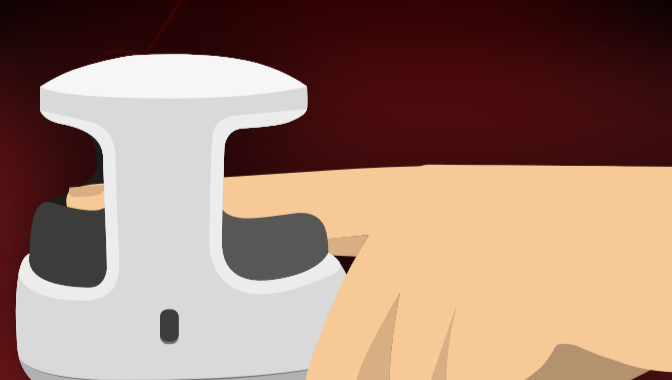
THREE-FACTOR AUTHENTICATION



Finger print recognition such as **TouchID** adds an additional level of security – but the **same device** is used for **Possession** and **Inherence**, if a phone or tablet is stolen, the finger print could be lifted from the screen

VEINID IS DIFFERENT

Combined with a username (**Knowledge**), VeinID uses a separate scanner (**Possession**) and a **biometric map** of the **vein structure** within the finger that **can't** be copied (**Inherence**)



This makes **VeinID** the **ultimate in customer protection**

See how VeinID can increase payment security at digitalsecurity.hitachi.eu