DIGITAL FINGERPRINTS

Real-time behaviour analysis as an invisible MFA

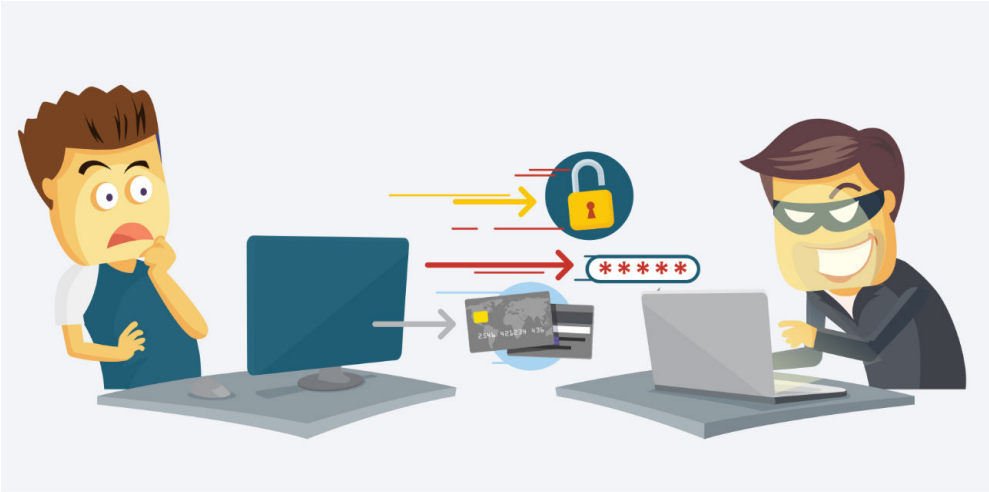
Problem

Account Take Over (ATO) If any of users struggle with identity theft – account take over is the next step to care about.

Session Take Over (STO) Cybercriminals perform man-in-the-middle attacks and steal the information that is used to authenticate user.

Stolen credentials Using sticky notes, using same passwords or simple passwords for multiple services sooner or later ends in compromise of credentials.

Friendly Frauds is an uphill battle even for best equipped organisations as these are very difficult to detect especially with PSD2 regulations.



Account Sharing Credential sharing is major impediment for services that are based on subscription model. If end users share the account – you lose money.

Automated attacks Automated programs are used to perform fraudulent actions.

UX with current MFA With behavioural biometrics no additional hardware is required.

Other frauds Purpose of fraud is very often a monetary gain by deceiving users.

How it works

Anonymised data is collected

Machine Learning models are iteratively created for each user

User is continuously scored against models when using app

Security Operation Centre is notified in real time when user's behaviour does not match

Demo Time

Stolen Credentials
With data leak or too simple login or password

Session Takeover
After login keyboard is taken by another user

Reaction time
Configurable from hundreds of milliseconds

Features

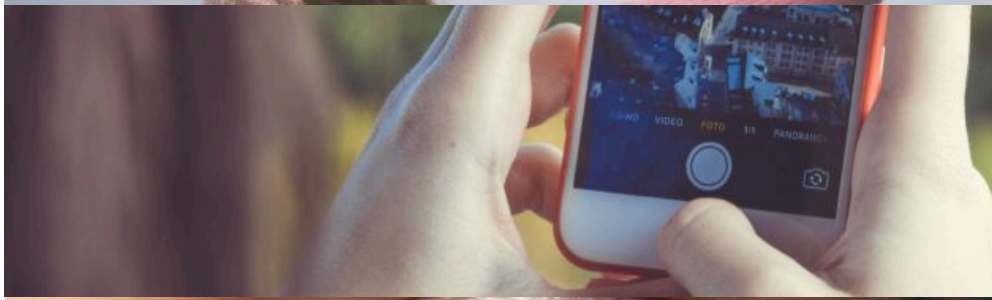
	Privacy & GDPR	Online Model adaptation	Continuous Authentication	Model per user	Contextless Operation	Low latency
DIGITAL FINGERPRINTS	✓	✓	✓	✓	✓	✓

Classical biometrics

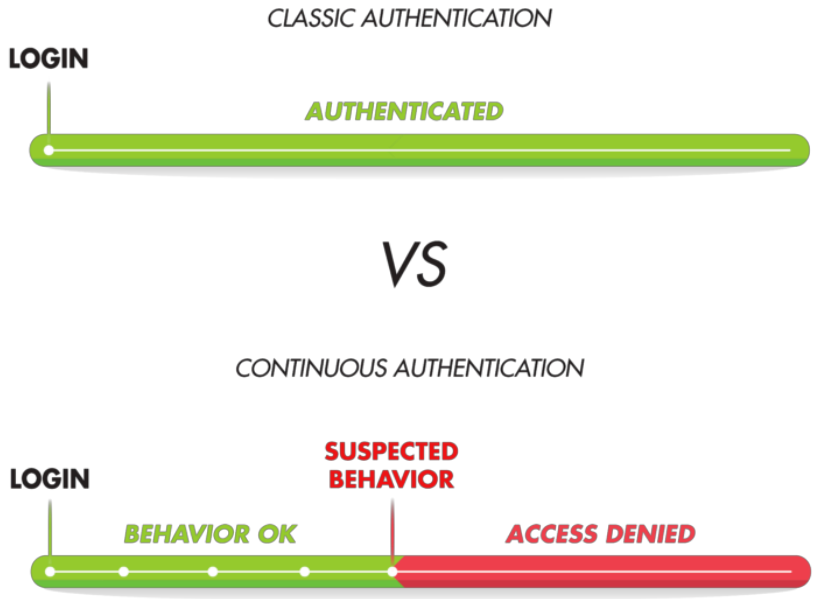
PIN, Face Recognition, Fingerprints, Iris Recognition

Disadvantages:

- Difficult to change the traits,
- Sometimes easy to crack
- Does not always work
- Only work at the moment of authentication



Continuous authentication



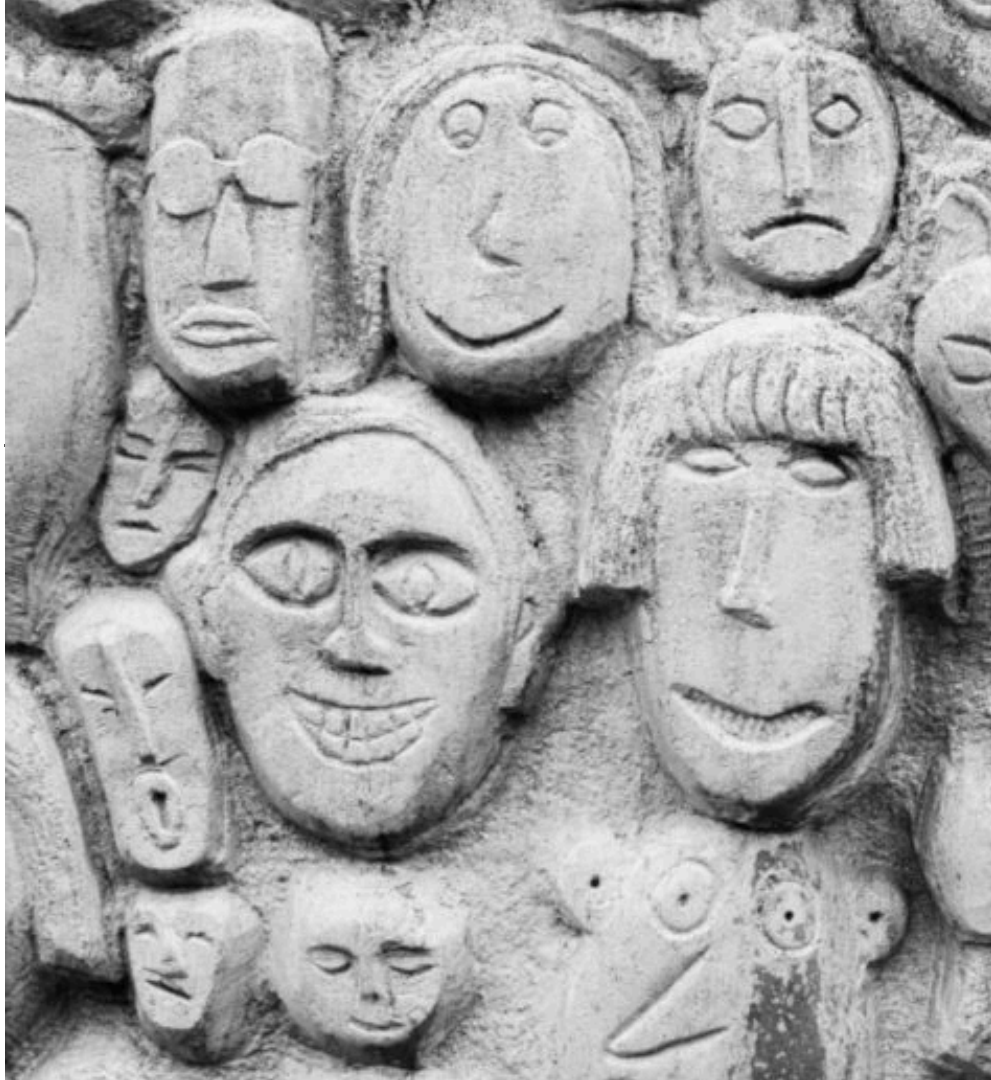
Classic authentication uses information to verify user **only** during single operation such as **logging** in or **sending money**. This is known widely as “Doorkeeper Problem”.

Continuous authentication starts protecting you **before the moment of login and finishes upon the end of the session**. With that approach, it is possible to react to Session Takeover Attacks and Account Takeover Attacks.

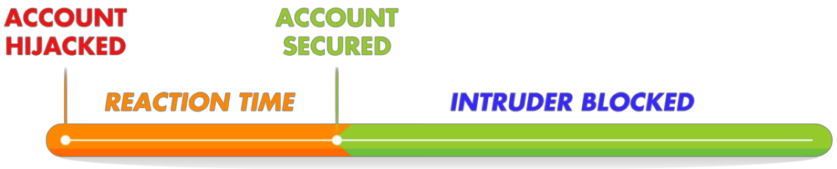
Model per customer

We create a Machine Learning model per user to maximise the **quality of service**. We use custom created components to provide scalability for millions of users.

Our business model is **as a service subscription** based on the amount of users protected with digital fingerprints.



Quick response time



We use stream processing to provide the measurements related to behavioural biometrics verification **very quickly**.

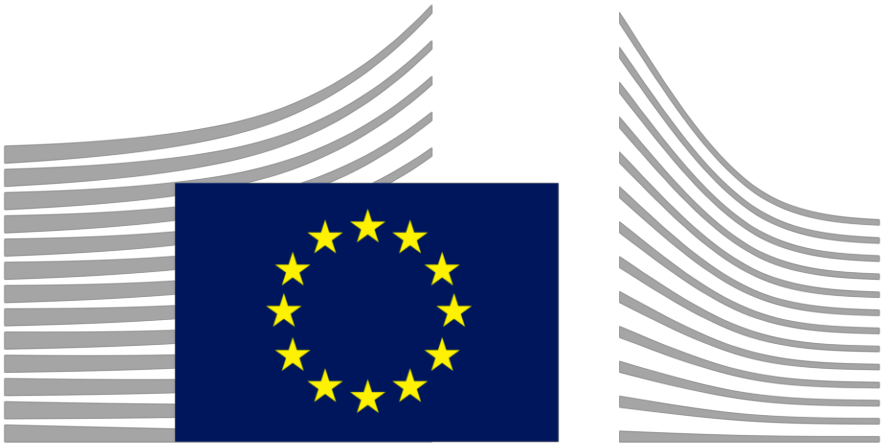
We can scale to **millions** of **concurrents** sessions with delay as low as hundreds of milliseconds for most of the requests.

Online model adaptation

User behaviour changes. Sometimes very abruptly due to unexpected events. It is important to follow the changes in order to provide a high quality of Machine Learning models.

Our solution **adapts to the changes** in behaviour of end users.

Compliance with Payment Services Directive 2



Payment Services Directive
(PSD2)

- All Payment Service Providers (PSP) need to be compliant with the requirement of **Strong Customer Authentication (SCA)**. From September 2019 PSD2 will affect all financial institutions in Europe. Behavioural Biometrics is considered compliant with the requirement of SCA.

Contextless operation

Digital Fingerprints does not acquire any information about you that is considered **uniquely identifiable** such as an identifier of your browser or your **IP address** .

We do not want to know what you do. **Just how you do it**. Our measurements are based purely on behaviour.

Data anonymisation

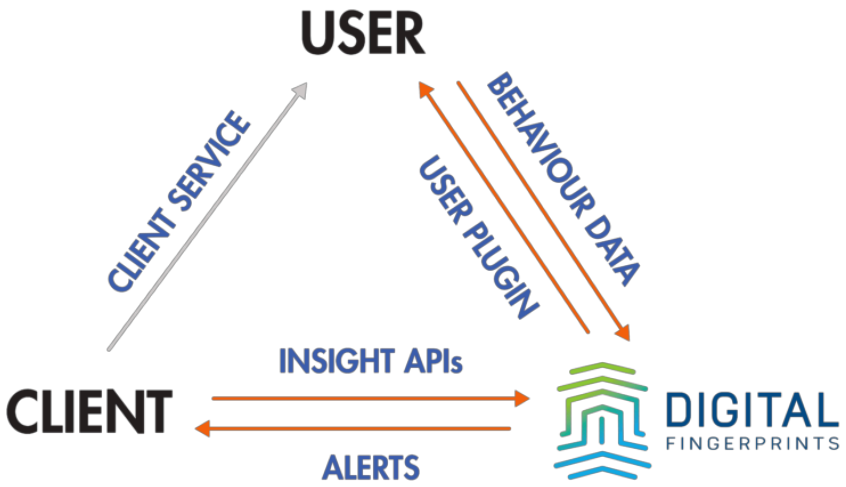
Digital Fingerprints **anonymises** data from your interaction with a computer. We only acquire information on **how you do things** not what you do.

For example, keyboard – we look at the way you write and how often you use manipulation keys such as backspace, return or delete.

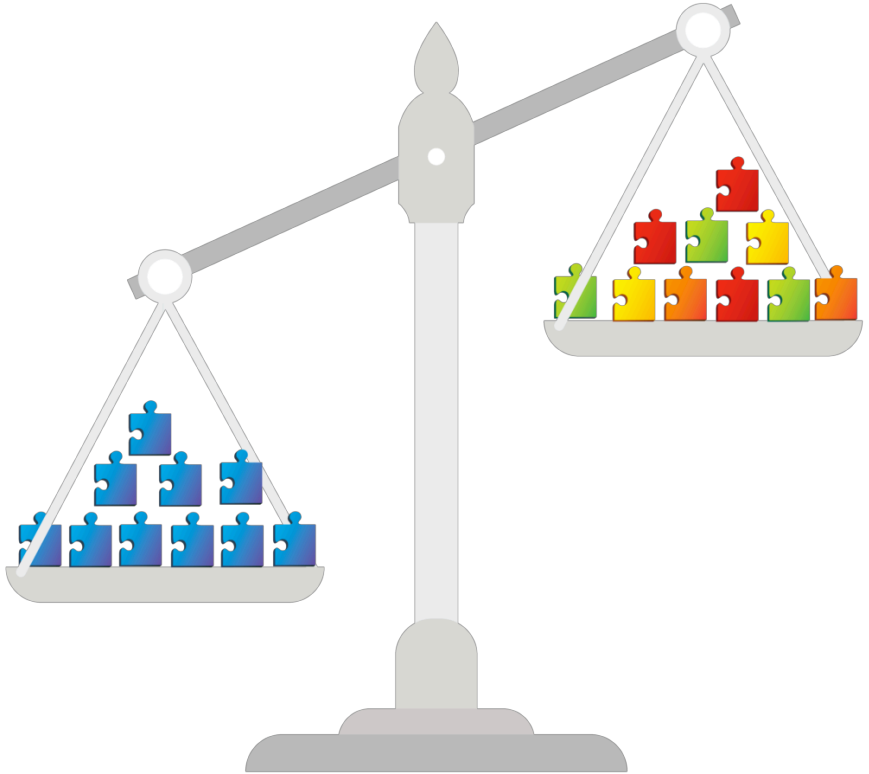
We are compliant with **GDPR** requirements to allow for opt-in and opt out. We fully respect the law to be forgotten and delete data of users if they wish so.

Easy integration

We provide a set of simple RESTful API's that might be used to integrate our service. **There are several options of integration** depending on the chosen **functional** and **non-functional** capabilities of the service required.



Model quality adapted to your needs



- Do you prefer to keep your **False Positives** low?
- Or maybe it is more important for you to have **models** ready **quicker** at the cost of quality?

Our approach is to set the quality of models to your needs.

Customer Case Study

mBank rozpoczyna pilotaż biometrii behawioralnej fintek.pl

Linie papilarne na celowniku hakerów. Klawiatura sposobem na sprawdzenie tożsamości użytkownika? CyberDefence24.pl

Rewolucja w bezpieczeństwie bankowania – mBank wprowadza biometrię behawioralną Antyweb.pl

mBank testuje biometrię behawioralną Digital Fingerprints money.pl

Biometria behawioralna w mBanku rp.pl

mBank will recognize you after you move the mouse. Behavioral biometry is how it works xiaomist.com

We are already protecting customers of mBank S.A.

Join the pilot and become part of the security revolution!

Thanks for your time!

Let’s protect your customers the way they are

Mateusz Chrobok

CEO

mateusz@fingerprints.digital

+48 514 579 805

Adam Forma

Business Development Exec

adam@fingerprints.digital

+48 606 659 522