Innovation in action: continuous biometric authentication

Insight into the future of access security

Authentication is your first line of defence

Protecting secure content on a device or within a service usually relies on authentication via something we know (such as a password), something we have (such as a token) or something we are (such as a biometric).

Although effective, these forms of authentication aren't perfect. Passwords and PINs have security and convenience issues, and tokens are easily lost or damaged. Biometrics do balance usability and security well, authenticating individuals transparently and accurately in real-time. However, single biometric measures such as your face, fingerprint or voice, have all been successfully 'spoofed', where the system was fooled by a replica of the real thing. And, currently, they're often only deployed at the point of entry.

Robust security needs to authenticate users throughout a session and continuous biometric authentication schemes can deliver this capability. Drawing on recent advances in devices, machine learning and processing power, these schemes train models on frequently sampled biometrics, so that future samples can be collected and authenticated in real-time. These solutions are secure and highly usable and there's a strong appetite in the financial services market for them.

Introducing a continuous element to biometric authentication has the potential to take security to a new level.

The European Data Protection Supervisor considers continuous biometric authentication to be one of their six trends for 2021 / 2022[1].

What are the business implications of continuous biometric authentication?

Continuous biometric authentication systems have a critical role to play in the security of businesses, consumers and governments.

In 2020, the BBC reported that 2,004 government devices had been lost in just 12 months[2]. It's possible that such devices could be unlocked by impostors with 'smudge attacks' where the unlock pattern is worked out based on smudges left on the screen. If continuous biometric authentication was in place, even if an attacker could get hold of the device, they wouldn't be able to gain access because their biometrics wouldn't match.

Market analysts expect the continuous biometric authentication sector to grow significantly. The global behavioural biometrics market size was valued at USD 0.87 billion in 2019 and is expected to expand at a compound annual growth rate (CAGR) of 24.5% from 2020 to 2027[3].

Where is continuous authentication heading?

Currently, facial biometrics and keyboard dynamics are leading the way in continuous authentication.

Facial biometrics are prominent, possibly because most devices have a front-facing camera function.

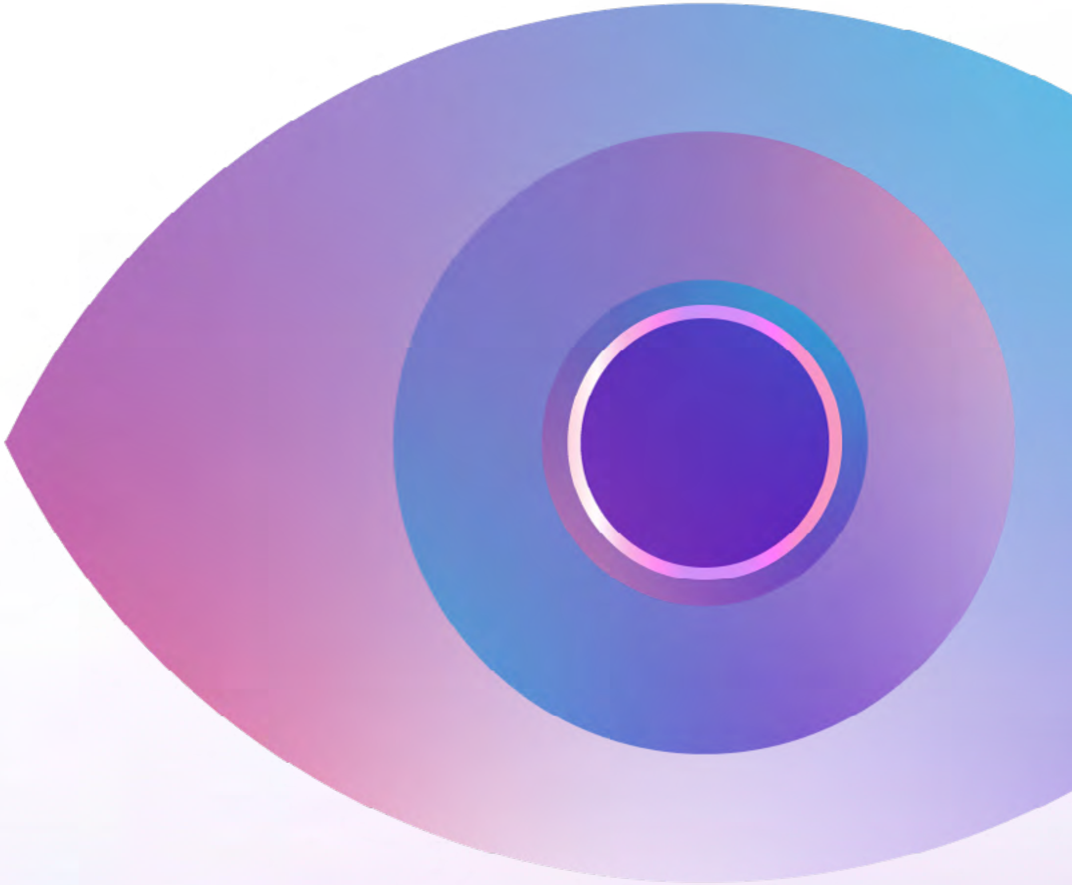
Keyboard dynamics also see significant use, allowing users to be authenticated as they type based on the rhythm of their typing. On mobile devices, touchscreen dynamics have been used to authenticate users based on the speed, location and pressure of their finger as they swipe.

User location (such as via GPS) is used by some solutions because users will often attempt access when at certain places.

Context is a critical factor

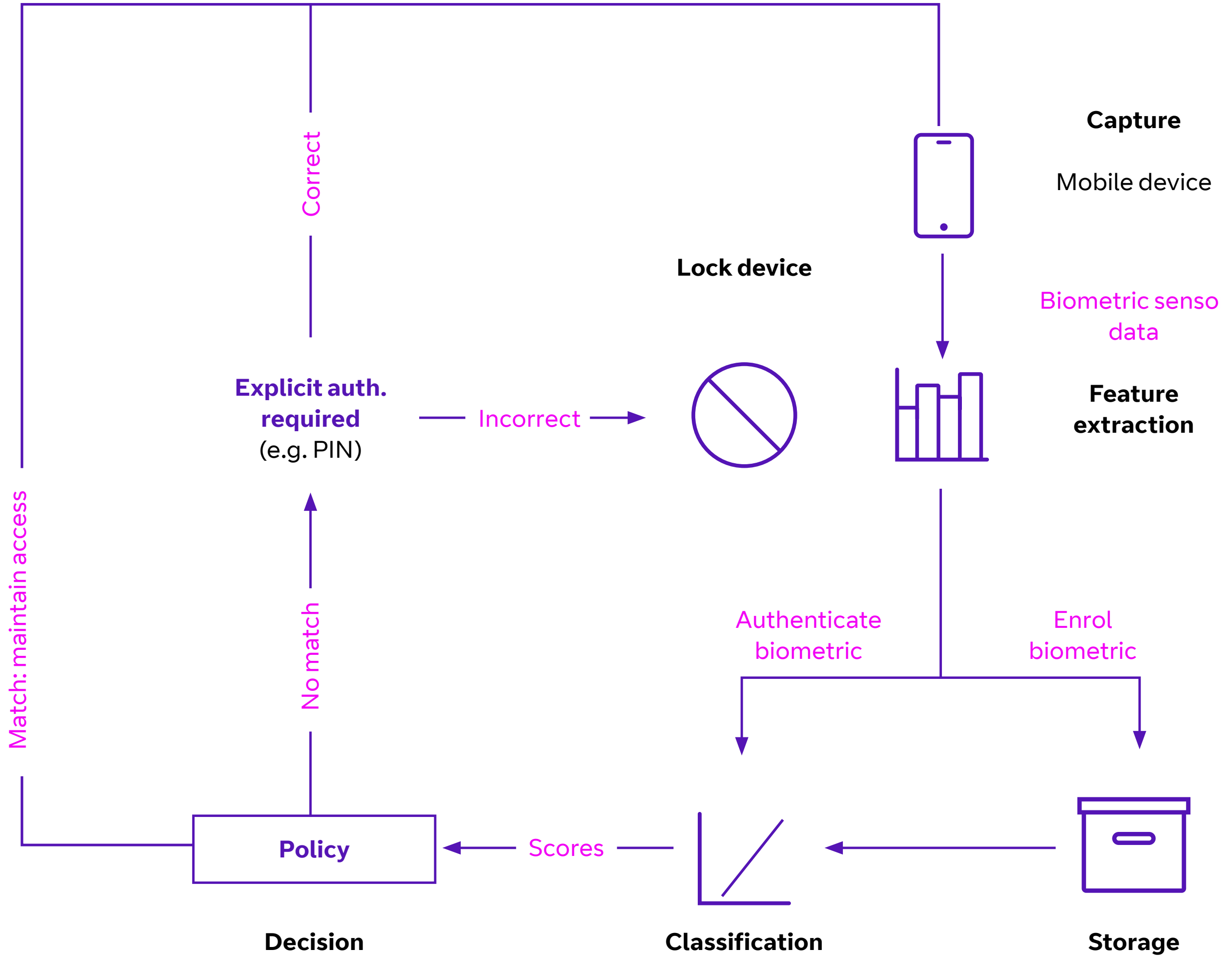
Context-aware continuous authentication systems are also incredibly important today, making use of contextual information such as the time of day or the user's location. These systems make custom models of how a user's biometrics might look in certain scenarios. For example, morning behaviour compared to evening behaviour when the user is more relaxed.

Context can also indicate potential threats (like contexts where the threat of impostors is higher, such as a café as opposed to a workplace). The continuous biometric authentication system can then respond to the context, potentially increasing the threshold required from the biometrics, or even increasing the number of biometrics authenticated.



Continuous biometric authentication process flow

A standard continuous biometric system repeats a series of steps that protect data and services in real time, ready to revoke access at any time.



The authentication solution collects user biometrics. These can be physiological (for example, the face) and / or behavioural (for example, typing behaviour) and must always be collected with the user's consent. On enrolment, these biometrics are stored and used to train a machine learning algorithm. In regular use, these biometrics are compared with the stored data.

The system starts authenticating the user by continuously collecting biometrics and classifying them in real-time against the user profile to produce an authentication score.

The authentication score is compared to a policy threshold that determines whether access to a device or service is maintained. Falling below the threshold can completely revoke access to the system / device or might only restrict access to certain highly secure resources.

Inventing the future

We're committed to developing and delivering best-in-class security solutions that give the banking and financial services sector resilience and confidence.

Our Applied Research team has been investigating continuous biometric authentication concepts for some time, but our work to produce proof-of-concept solutions has accelerated considerably during the last couple of years. In collaboration with leading universities, we've published market-shaping papers in this field and have filed patents to protect our intellectual property in this space.

Today, we have proof of concepts for a variety of devices including Android smartphones and laptop devices. Our solutions collect biometrics including face, keyboard dynamics, Bluetooth devices, wi-fi hotspots and location. We've built our own machine learning models as well as harnessed open-source models to accurately authenticate all these biometrics in real-time.

We've investigated full-system continuous authentication as well as web-service / app-specific continuous authentication.

Internal trials have been successful and indicate that biometric continuous authentication could prevent a variety of attacks, from impostors using devices left unlocked through to impostors cracking a user's password.

Privacy will always be a critical factor, so we can build our solutions to only use a mathematical feature vector of biometrics that's only stored locally on the user's device. It's really difficult to recreate the original biometrics from the mathematical version and local storage keeps the user in control of their information.

Our current use cases specifically target situations where privileged access to a system / service is required and where continuous security above and beyond a password at the point of entry would be beneficial.

Visit our webpage to find out more about how global, end-to-end fraud protection can meet your security needs.

We continue to explore this space, pioneering new ways to improve authentication built on the innovation that comes from our ground-breaking Adastral Park facility.

Discover how we innovate for a connected world by visiting: atadastral.co.uk.

References

[1] European Data Protection Supervisor, Biometric continuous authentication, nd
[2] BBC News, Thousands of mobiles and laptops lost by UK government in a year, 2020
[3] Grand View Research, Behavioral Biometrics Market Size, Share & Trends Analysis Report By Component, By Type, By Application, By Deployment, By Enterprise Size, By End-use, By Region, And Segment Forecasts, 2020 – 2027, nd

Offices Worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

October 2022