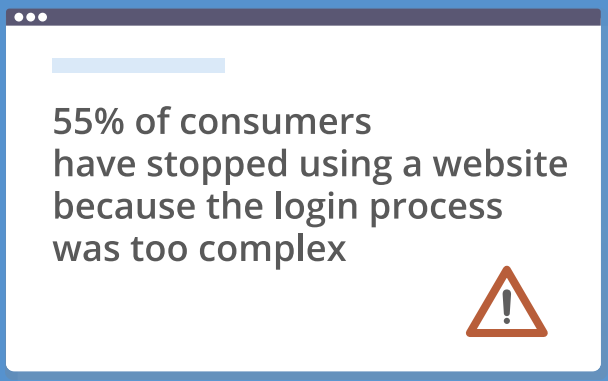


“it would be a miracle to find password-less authentication that just worked”

MIRACL®

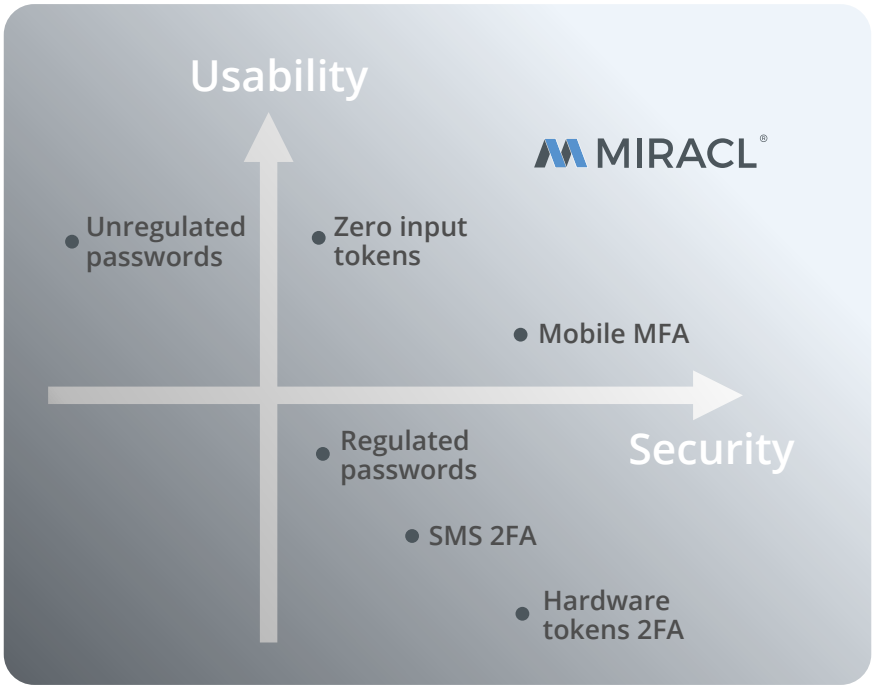
Whichever way you look at it, **passwords are a terrible idea**: hackable or unmemorable, interceptable and data-vulnerable. Big ideas to replace them come and go, and they fall on problems of friction, failure or cost. **And we're stuck with passwords.**

But not any more. MIRACL is one big idea that's here to stay.

MIRACL combines:

- **usability**: intuitive and uncomplicated
- **multi-factor**: without a second step
- **deployability**: no hardware required, device and OS independent
- **cost-effectiveness**: total cost of ownership lower than passwords
- **bomb-proof protocols**: military-grade security for mission-critical service
- **rapidity**: start-to-finish authentication in 2 seconds

No other authentication system ticks all these boxes.



There's no compromise or payoff between security and usability. MIRACL delivers both. And within a highly cost-effective package.

MIRACL in detail

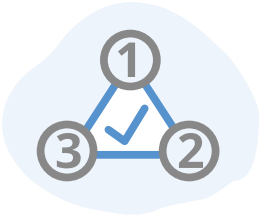
Usability:

MIRACL authentication is a unique one-step process available through any device and in any operating system. It takes place on the device in a web browser or mobile app. No supporting browser plug-ins are required or the incorporation of extra standards.

A simple 4-digit access PIN is all the end user has to remember. Furthermore, as MIRACL authentication becomes more common in people's lives as businesses upgrade their password-based systems, this single PIN can, if desired by the user, be used for all their MIRACL sign-ins.

The MIRACL process is incredibly robust and achieves an exceptional success rate. Where password failure rate is 5-10% and two-device MFA is from 10% upwards, MIRACL's success rate approaches a near-perfect 99%.

Users enjoy a simple, consistent, reliable operation on the device of their preference without ever requiring a second step.



Multi-factor security:

MIRACL achieves a gold standard MFA through a process in which the end user proves possession of the factors, without ever revealing those factors to the verifying party.

Unlike passwords and standard two-factor authentication, MIRACL authenticates without exchanging any personal information at all so it requires no database. This means that since there is no security-related information stored on our servers or yours; there is nothing of value for a hacker to intercept or steal and no GDPR risk. And there are no known practical or theoretical attacks against our cryptography and protocols.

Cost effective:

Eliminating the service response requirement for password-resets, typically up to 50 to 60% of total service costs, MIRACL delivers an impressive saving against password-based authentication.

MIRACL compares well too against hardware tokens and authentication-as-a-service offerings. With a pay-as-you-go model, where billing is for usage not for a maximum-case scenario license, and no system management or infrastructure maintenance costs, MIRACL delivers significantly lower total cost of ownership.

MIRACL delivers high RoI. With its lightning fast authentication and minimal failure rate, MIRACL shrinks customer fall-outs and propels a significantly higher percentage of would-be purchasers to sale/ conversion.

Deployability:

MIRACL is simple to activate, deploy and on-board users at scale. Clients can be live within minutes.

MIRACL easily integrates into any point of your web and mobile application security process, and can support the authentication mechanisms you have planned or have in place.

MIRACL is designed to work at internet scale, through browser or mobile app. It delivers multi-factor authentication with no compromise to users' experience. MIRACL Trust® for mobile login can secure your end users into mobile applications with the same multi-factor authentication solution through our software development kits (SDKs) for Android or iOS.

Rapid authentication:

Because password authentication is so ubiquitous, it is easy to forget that the process takes on average 10 seconds to authenticate. Two-device MFA is a noticeably longer process with multiple steps taking 30 seconds or more.

MIRACL authenticates in 2 seconds, 5 times faster than passwords. With no second device and no second or multi step. Lightning fast.

How does MIRACL dominate the threat landscape?

Systemic threats

Password hacking

MIRACL is passwordless. There are no passwords or password databases to hack at the user end or at the server end.

Phishing

The MIRACL platform does not send any user verification data of value across a mobile or web network. Malicious actors will be phishing in an empty lake.

Man in the Middle

Without the possibility of intercepting authentication information, data sent between points cannot be decrypted.

Replay

Without authentication information to intercept, there is no possibility of a replay attacker being able to read and spoof any communications.

Credential Stuffing

The MIRACL platform generates its own keys. There is no sense that authentication information from elsewhere can be used to guess entry.

Password Spraying

Malicious actors can guess passwords until they are blue in the face, MIRACL is passwordless - there are no passwords to guess.

FAQs

“So how secure is MIRACL?”

We assert that there are no known practical or theoretical attacks against our cryptography and protocols. This is not hype, it is mathematically provable and born of 20 years of publicly disclosed tech. It has been licensed to many of the world’s largest and most security conscious organisations like the US Military, Intel and Google.

“Does MIRACL work alongside client or third party IAM services?”

MIRACL is an authorisation enhancement service that is completely independent of how you manage your identities. MIRACL only handles the user enrolment or authorisation request then passes it back to your service. All identity, access and enrolment management takes place on your system. There’s no replication of databases and no increase in GDPR footprint.

“How's a 4 to 6 digit PIN more secure?”

A MIRACL pin is of zero value without another possession factor (the security shard held on the local device). Furthermore, it can only be used on enrolled devices. It is not transmitted or stored locally or remotely and there is no central database of PINs or users locally or remotely.

“Can it really contribute to revenue?”

Yes, absolutely. Customer fall-out is a significant dent in revenue through cart abandonment and user attrition. Reduce the fall-outs and revenue will increase.

MIRACL®

MIRACL®

No complicated passwords to remember
No password database breach possible
No credentials sent across web
No credentials stored in cloud
No hardware tokens
No SMS messages

Single-step, 2 second MFA on any device

MIRACL®

71-75 Shelton Street, London, WC2H 9JQ, United Kingdom

Tel: +44 20 8191 9264

Email: sales@miracl.com

Web: miracl.com