CELENT

Solution Brief

MIRACL TRUST ID

Can an Authentication Solution Live Up to Its Name?

Zil Bareisis

July 12, 2022

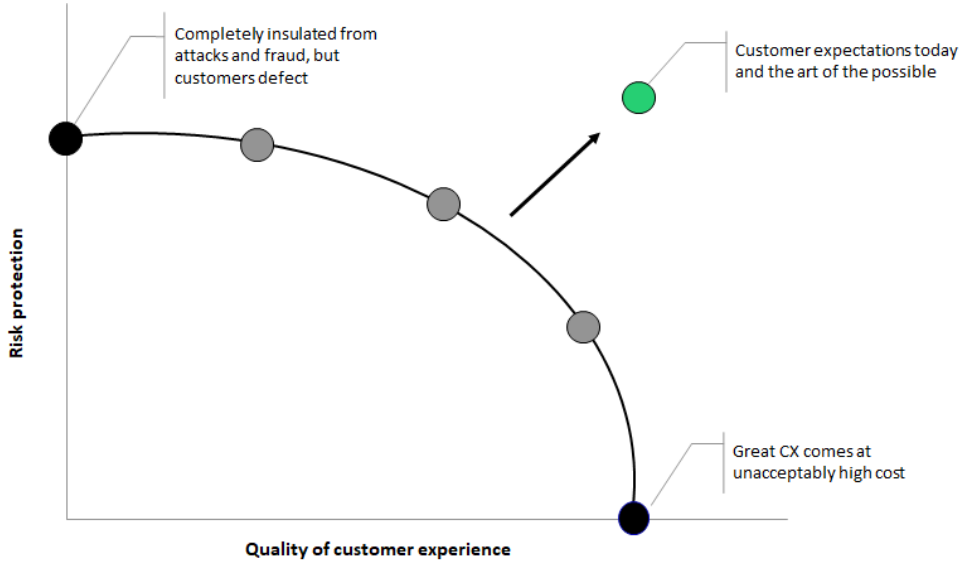
EXECUTIVE SUMMARY

Over the years, industry analysts have learned to take some vendor claims with a grain of salt. So, when coming across a company named MIRACL, our guard was instinctively up: 'They'd better be able to back it up.' We were positively surprised to find that MIRACL Trust® ID is an authentication solution that does live up to its name.

Context

Banks have always sought to balance security and user experience when authenticating customers. In the past, it was a very explicit trade-off—what was easy for customers (e.g., a simple password) often came at an unacceptably high cost for the bank, while tightening security meant risking losing customers. The progress of various technologies (smartphones, biometrics, behavioural analytics, etc.) has been moving the dial to where that trade-off is no longer necessary — customers today expect both strong security AND good experience.

Figure 1: Traditional Trade-offs Are Getting Addressed



Source: Celent

Because of strong customer authentication (SCA) requirements under PSD2, European banks have been deploying multifactor authentication (MFA) solutions, such as a regular password ('what you know') supplemented with a one-time passcode (OTP) delivered via SMS to prove the customer is in possession of their phone ('what you have'). However, such solutions again come at the expense of user experience and with their own vulnerabilities.

Company and Solution Overview

MIRACL Trust platform is a cloud-based service that provides secure, multi-factor authentication to employees, partners, and external users without sending authentication credentials across the web for storage in the cloud.

Originally founded as Certivox in 2011, the company changed its name to MIRACL in 2016. Actually, the name MIRACL has little to do with magic; it stands for **M**ultiprecision **I**nteger and **R**ational **A**rithmetic **C**ryptographic **L**ibrary. The firm's chief cryptographer, Dr Michael Scott, is known in the industry for his cutting-edge research into pairing-based and elliptic curve cryptography. According to the company, their open-source cryptographic library is widely used by hardware manufacturers and has many closed source licensee customers. The M-Pin Protocol eliminates password risk in a variety of computing systems with a user-friendly, zero-knowledge proof authentication protocol built on strong cryptography and open standards.

We came across MIRACL at a recent industry event and arranged a briefing with **Michael Tanaka, Chief Commercial Officer**, to learn more about MIRACL Trust ID, the company's SaaS authentication solution.

KEY BRIEFING TAKEAWAYS

The simplicity and elegance of the solution masks the complexity of behind-the-scenes cryptography responsible for ensuring the highest levels of security.

Introducing MIRACL Trust ID

From the user point of view, MIRACL Trust ID is very simple—you first register your ID and choose a four-digit PIN. The ID can be your email, an employee number, or any other username. To log in, you just enter the PIN again and you are in.

Now, compare that with a typical SCA process, such as when paying online with a digital wallet. You first need to enter a password, which is likely to be complex and more than eight characters. Then you are probably given a choice for additional authentication—either via the app, which you need to open and then log in, or via the SMS OTP, which you need to wait to receive before typing the passcode into the main login screen. According to MIRACL, and as can be easily seen when using the solution, their process takes 2.5 seconds, while alternatives can take as long as 38 seconds.

The obvious question is: How is this different or better than a traditional username and PIN/password combo? In the traditional setup, username and password or PIN are stored in the provider's database, which becomes a honeypot-like focus of hackers' attention, requires hardware and maintenance by costly IT personnel, and can be vulnerable to data breaches. Also, a password is only a single factor—'what you know'—and for SCA needs to be supplemented with 'what you have' or 'who you are', introducing friction to the user experience. Even when typical hardware or software tokens are used for the second factor, they usually store the entire private key and can be vulnerable to key compromise or theft.

In contrast, MIRACL authenticates without exchanging any personal information at all, so it requires no database. MIRACL's cryptography destroys the key and only the key shard (the 'broken' key) remains on the enrolled device and is used as the possession factor. This means the key shard is of no cryptographic value and cannot be misused. Only the end user who enrolled the device (and broke the key) can rebuild the key using the PIN (knowledge factor). The PIN or the key shard are never copied, transmitted, or in any other way accessed except on the local device. The PIN is not stored on the device and can't be discovered in any way; it only ever resides in the user's head. That means there is nothing of value for a hacker to intercept or steal and therefore, no GDPR risk.

MIRACL's solution relies on Pairing-Based Cryptography (PBC)[1] for its innovative multi-factor authentication protocol called M-Pin. The protocol is what cryptographers call 'zero knowledge'—the client can prove possession of the issued secret key whilst revealing no details about this key.

In addition to Enrolment and Authentication, every MIRACL Trust ID service integrates two other basic functions, Revocation (blacklist) and Signing (the ability to digitally sign data assets). This means the solution can not only authenticate but also create a digital proof that associates the identity to the action (or asset). By associating the transaction to a specific user/device/enrolment, it meets and exceeds the requirements of PSD2's Dynamic Linking to create an immutable ID for a transaction. This can be done from within a secure session on the same browser tab.

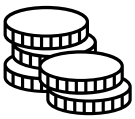
Solution Benefits and Opportunities for Banks

According to MIRACL, their authentication solution offers a better combination of security and usability than many other solutions available in the market (Figure 2). MIRACL's ID solution combines:

- **Usability:** It is intuitive, simple, and easy to use. Login is very fast and can be done in a few seconds.
  - This leads to a **high success rate**—99.8-99.9% at live clients[2]. In contrast, password failure rate can be 5–10%, and two-device MFA from 10% upwards, when measured across the entire process.

- **Security:** It is **multifactor** without any additional steps. It is also effective against many known threats, such as password hacking, phishing, 'man in the middle', credential stuffing, and others. The company asserts that there are no known practical or theoretical attacks against their cryptography and protocols, which have been licensed to many of the world's largest and most security-conscious organisations like the US military, Intel, and Google.

- **Deployability:** It can be deployed across different types of devices and operating systems with no additional hardware. It is designed to work at internet scale through browser or mobile apps. Native iOS and Android apps can integrate MIRACL's SDK. Not only does this provide a primary authentication for the app, but it also turns the customer's service app into an authenticator app capable of logging into a second (unenrolled) device.

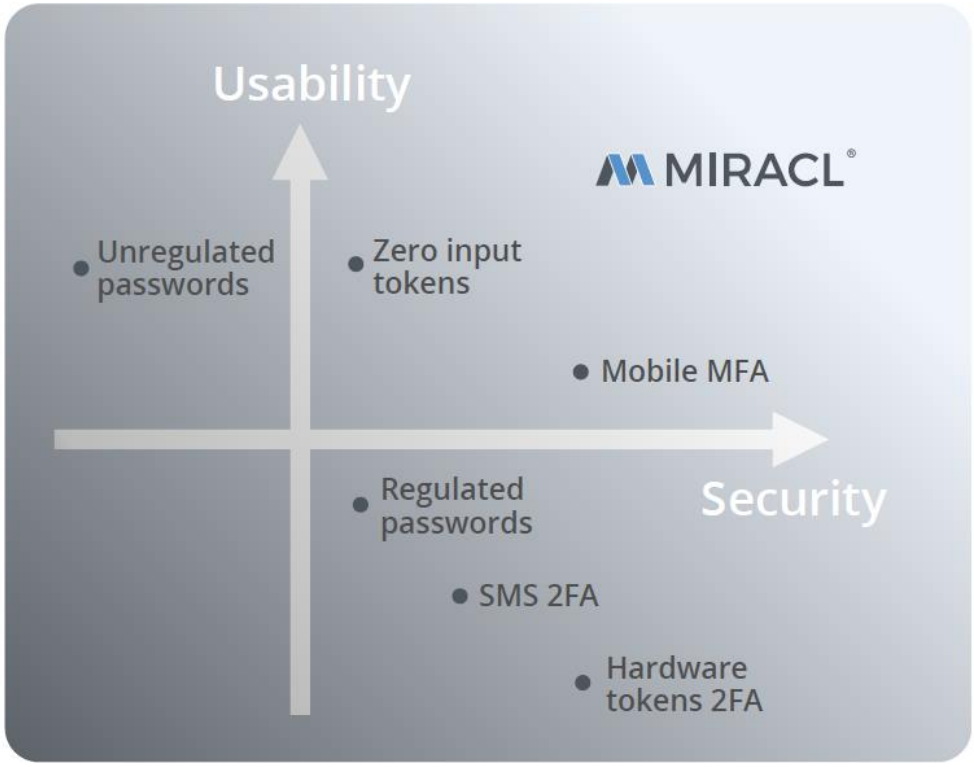


- **Cost effectiveness:** Password resets can be responsible for 50–60% of total service costs. MIRACL claim to deliver lower total cost of ownership against other alternatives, including passwords, given its pay-as-you-go pricing model and zero system management or infrastructure maintenance costs. As there are no IDs to maintain or databases to synchronise, some MIRACL clients deployed the solution across thousands of locations but haven't had to visit their SaaS portal at all in over two years.

[1] According to MIRACL, PBC is emerging as a solution to complex problems that have proven intractable to the standard mathematics of Public-Key Cryptography.

[2] Average for all authentications over all clients is 99.65%, but that includes Pilots/PoVs, which purposefully try things like PIN resets and typos to test the system.

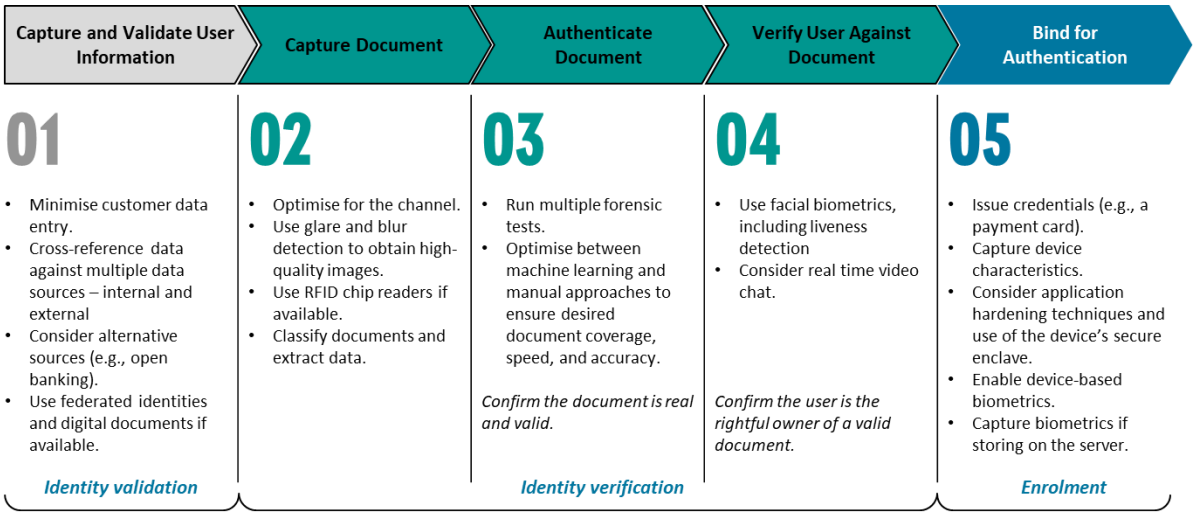
Figure 2: MIRACL Offers Both Security and Usability



Source: MIRACL

MIRACL Trust ID is purely an authentication solution and must be implemented alongside identity verification, authorization, and fraud and risk management solutions. As we describe in our five-step best practice process for identity proofing (Figure 3), once a financial institution is comfortable with the identity checks, it needs to bind the customer and their device for subsequent authentication (Step 5).

Figure 3: Best Practices of Identity Proofing Process



Source: Celent

It is at this point that the customer would be asked to select a PIN for their device; from then on, they can use the same PIN to authenticate themselves on that device and get into their account. This is where MIRACL fits in. The company has partnered with leading providers of adjacent solutions (one of whom has also become a strategic investor) to demonstrate tight integrations.

Financial Services Clients

MIRACL shared with us that their technology is trusted by the military, financial services, and technology companies (Figure 4).

Figure 4: Selected MIRACL Clients

Source: MIRACL

Example clients in financial services include:

- **Cashfac:** a global provider of cash management software, including Cashfac Virtual Bank Technology (VBT). 'The world's most deployed virtual accounts platform' needed an MFA solution for PSD2 SCA compliance. The company integrated MIRACL and went live with 12 companies and 1,600 users using Cashfac-as-a-service in six months.
- **Crédit Agricole Romania:** in the past, the bank relied on hardware tokens for second-factor authentication and faced challenges with maintenance and usability (e.g., sending out the replacement). MIRACL Trust offered a secure alternative, as well as a practical solution for PSD2 SCA compliance, including support for Dynamic Linking without hardware. Furthermore, the separation of authentication and authorisation offered the bank more flexibility in how they manage customers and what they can access. The ability to digitally sign data assets was an important feature for both Cashfac and Crédit Agricole.
- **Experian UK:** Experian was selected as one of the seven third party identity providers that UK citizens could choose from when accessing government services under the GOV.UK Verify programme. Experian partnered with MIRACL to create the secure and yet user-friendly means of logging in. Approval required a review of MIRACL's system and architecture by GCHQ[3] in order to satisfy HMRC[4] that login for tax filings and highly sensitive information would be securely protected.

[3] Government Communications Headquarters, commonly known as GCHQ, is the UK's intelligence, security, and cyber agency.

[4] Her Majesty's Revenue and Customs is the UK's tax, payments, and customs authority.

TO CONSIDER

Many of us teach our kids to believe that if something sounds too good to be true, it often is. Such natural scepticism is one of the barriers this innovative solution needs to overcome to achieve a more widespread adoption.

According to the company, the 'too good to be true' scepticism has been a genuine challenge for them. First, people don't know or expect that it is possible to have such a solution, so they don't look for it.

> Nobody searches for 'browser-based multifactor authentication that doesn't require download' because nobody thinks that's possible.
>
> Michael Tanaka, MIRACL, 2022

Second, even when people are shown the solution, they can easily mistake the simplicity of the user experience for lack of sophistication—after all, they've been told that passwords and PINs on their own no longer provide enough security. And while the bank's security professionals can appreciate and understand the cryptography behind the scenes, it is harder to reassure casual users that this username-and-PIN authentication is genuinely different from other username- and PIN/password authentications they've experienced in the past.

There is another subtle nuance that has to be explained to users. Typically, a username and password are at the **account level**. Once set up, customers can use the same details to log in to their account from any device, whether it's a laptop, a desktop, or a mobile phone. Because of the way MIRACL Trust ID manages the cryptographic keys, the customer's PIN is enrolled for a **specific device**, not the account. That means that if they want to access their account from a different device, they have to enrol again—something that might come as an unexpected surprise to them. And while the MIRACL enrolment process is straightforward, and customers can even choose the same PIN if they want, the bank (or indeed, any app or website operator) will want to ensure that they have a way to verify customer's identity again. Even the best authentication solutions are meaningless without robust enrolment. Just remember the levels of fraud that banks experienced in the early days of Apple Pay: The transactions were perfectly secure, but some banks didn't have sufficient controls against fraudsters registering fake cards.

On the other hand, this device-level enrolment offers an opportunity to control access on a device-by-device basis, i.e., enable or block specific devices but keep

accounts open. Back in 2017, we published a report called **Building a Consent and Control Centre: Towards Monetising Customer Data**, where we highlighted this exact capability as an important feature the leading banks should aspire to offer for their customers:

> Today customers access their bank accounts via various bank channels, such as branch, contact centre, ATM, and online and mobile banking. Tomorrow they will be accessing their banks not just via laptops, phones, and tablets, but also via voice platforms, smart TVs, car dashboards, and other digital connected devices. To minimise fraud, customers will expect to be able to control—grant, change or revoke—the access level for each of those devices.
>
> Customers should be able to set the access parameters at a reasonably granular level. For example, users may want to grant full access to their latest laptop but turn off any access from the laptop they are retiring, and only limit voice commands to balance enquiries.
>
> Celent report, November 2017

Since the solution is browser-based, it is device independent and can be deployed on any device capable of launching a browser—a PC, a smartphone, a smart TV, and so on. However, it doesn't work with browsers in private mode, which destroy all the session information after closing. In other words, a bank looking to implement MIRACL Trust ID needs also to plan for investing in **customer education** to explain how and where the solution should be used.

We already mentioned that this is a solution for authentication, not identity verification, and during authentication itself there is no positive identity confirmation. That means if somebody knew my PIN and had my device, they could log in to my account. This is not a criticism or a limitation of the solution—if somebody takes my card and I tell them my PIN code, they can make a chip-and-PIN card payment, generally considered among the most secure payment types. Similarly, if I allow somebody to register their fingerprint on my phone and then enable TouchID, they can also access the account. That is why leading banks are deploying **layers of security**, such as adding 'live' biometrics-based authentication for higher risk transactions, and risk-based authorization, which may include behavioural analytics and other techniques.

Finally, even though MIRACL has been around for some time, the company changed its focus several times before settling down on SaaS products and remains relatively small, with fewer than 50 people. To better promote and accelerate adoption of its Trust ID, MIRACL is transitioning from direct sales to alliances and partnerships with larger players that offer a broader set of

solutions. Also, each new client requires a consultative approach at the start, as they need to figure out how the various functions of MIRACL Trust ID would be integrated into a broader identity and authentication management architecture. To address those needs, the company is looking to work with channel partners, such as system integrators.

*****

As an authentication tool, MIRACL Trust ID does live up to its name—once enrolled, the subsequent login is secure yet seems magically simple. Whether and how soon it becomes an established way banks and other web and app operators manage customer authentication depends on the company's ability to scale up and roll it out beyond the early adopters.

About Solution Briefs

A Solution Brief (formerly Briefing Note) is a type of Celent Insight launched in 2019 to provide research clients with timely updates on vendor/fintech solutions and strategies. Celent does not charge any fees to write a briefing note, and vendors do not have to be Celent research clients to be eligible for one. However, Celent analysts are selective and publish a limited number of notes throughout a year about briefings they found particularly interesting; the decision whether to write a note is at the Celent analyst's discretion. Vendors have the opportunity to check the draft before it's published to ensure we accurately represent the facts and don't disclose anything confidential, but otherwise do not have editorial control.

For more information, please contact info@celent.com or:

Zil Bareisis zbareisis@celent.com

Americas

USA
99 High Street, 32nd Floor
Boston, MA 02110-2320

+1.617.262.3120

USA
1166 Avenue of the Americas
New York, NY 10036

+1.212.345.3960

USA
Four Embarcadero Center
Suite 1100
San Francisco, CA 94111

+1.415.743.7960

Brazil
Av. Dr. Chucri Zaidan, 920
Market Place Tower I - 4° Andar
Sao Paulo SP 04583-905

+55 11 5501 1100

EMEA

Switzerland
Tessinerplatz 5
Zurich 8027

+41.44.5533.333

France
1 Rue Euler
Paris 75008

+33 1 45 02 30 00

Italy
Galleria San Babila 4B
Milan 20122

+39.02.305.771

United Kingdom
55 Baker Street
London W1U 8EW

+44.20.7333.8333

Asia-Pacific

Japan
The Imperial Hotel Tower, 13th Floor
1-1-1 Uchisaiwai-cho
Chiyoda-ku, Tokyo 100-0011

+81.3.3500.3023

Hong Kong
Unit 04, 9th Floor
Central Plaza
18 Harbour Road
Wanchai

+852 2301 7500