MIRACL®

G-Cloud 15

Service Definition

Lot 2 Cloud Software

Digital Signatures
MIRACL Trust® Proof
MIRACL International Limited

Version: 2.0
25/01/2026

MIRACL International Limited (Registration No 14713119) | 71-75 Shelton Street, London, WC2H 9JQ, United Kingdom
T: +44 (0) 20 8191 9262 | E: info@miracl.com | www.miracl.com

MIRACL International Limited (Registration No 14713119) | 71-75 Shelton Street, London, WC2H 9JQ, United Kingdom
T: +44 (0) 20 8191 9262 | E: info@miracl.com | www.miracl.com

MIRACL International Limited (Registration No 14713119) | 71-75 Shelton Street, London, WC2H 9JQ, United Kingdom
T: +44 (0) 20 8191 9262 | E: info@miracl.com | www.miracl.com

1. Introduction

Company Overview

MIRACL helps any organisation replace insecure passwords, complex 2FA and expensive SMS texts - with a simple PIN. Purpose-built for sectors where any additional security drives users away, it uses cryptography licensed to Experian, Google, the US Military and Intel to block 99.9% of all account attacks.

A combination of user friendliness, hardware independence and cost make it possible to deploy strong multi-factor authentication and designated verifier signatures to large enterprises or diverse customer networks where it was previously impossible or impractical.

Value Proposition

As the creation, transmission, processing and storage of sensitive information continues to move from old paper-based methods to the new all-digital world, it becomes increasingly important to replicate ink-based signatures electronically to guarantee authenticity. Many existing digital signature schemes rely on PKI certificates and are therefore limited by the administrative overheads and poor scalability associated with a PKI infrastructure and, in particular, client-side certificates.

MIRACL solves these issues with its own Designated Verifier Signature (DVS) digital signature scheme, which, when used in conjunction with MIRACL's authentication platform, solves the **P.A.I.N.** issues commonly found in cyber security scenarios:

- **P**rivacy – the transmission of sensitive data can be secured by encrypting the communication channel using Transport Layer Security (TLS) with traditional server-side PKI certificates. Or, for a fully certificateless implementation, the TLS channel may be created using a pre-shared key (PSK) generated by the MIRACL Trust platform.
- **A**uthenticity – recipients of data signed with DVS can be certain of the signature creator's identity.
- **I**ntegrity – the DVS signature is uniquely linked to the signed data. If the data is changed, the signature will fail verification
- **N**on-repudiation – the DVS scheme is key-escrowless meaning that only the user can create digital signatures and not a server. Note that the PIN is required to create the signature and this is not stored or transmitted anywhere - it is only remembered by the user.

MIRACL International Limited (Registration No 14713119) | 71-75 Shelton Street, London, WC2H 9JQ, United Kingdom
T: +44 (0) 20 8191 9262 | E: info@miracl.com | www.miracl.com

Note that in classic digital signature schemes, the global community is capable of verifying signatures, however, with DVS, only the "designated" MIRACL platform can verify signatures via a request to its DVS service.

MIRACL delivers: Improved Security AND Improved Experience

> *"Protecting the person online and giving them a good user experience of the services they are using is a key goal for us as a business. MIRACL is a pioneering company that will help us achieve that."*
>
> **Nick Mothershaw**, Former UK & I Director of Identity & Fraud at Experian

Service Uses

Transaction Processing & PSD2 Compliance

DVS signatures are PSD2 compliant and can therefore be used to sign electronic payment transactions. The DVS signature is necessarily unique per transaction and thus meets the "dynamic linking" requirement of PSD2 to replace existing methods such as Transaction Authentication Number (TAN) codes.

Sign Mobile or Desktop Uploads of Documents

It is now commonplace for documents and forms to be submitted electronically. Applying a DVS signature can guarantee the authenticity of such items which may include mortgage applications, clinical data reports, passport applications, any Know Your Customer (KYC) documents etc. The identity is tightly bound to the enrolled entity and the documents are provably sourced and immutable.

User Submitted Content

User submitted (shared) content from unpaid contributors has become an essential source of material for most online and offline businesses. Audio, visual and written content such as mobile video uploads, pictures, commentary, testimonials and blog posts, submitted by the public and loosely affiliated agents, are all indispensable resources.

As the publics' ability and willingness, to capture and submit content becomes ever more prevalent, so to becomes the capability of any party, including the recipient, to undetectably alter that data. MIRACL Trust® Proof allows clients to prove the source and data integrity, forming a crucial audit trail all the way from collection through editing, to display. Similar to document uploads, whatever enrolment process is used, the identity is tightly bound to the enrolled entity and the content is provably sourced and immutable.

Internal & Partner Content Creation

MIRACL Trust Proof can create a valuable audit trail during any multi-staged process of content creation. Signatures can be created at each milestone or at final submission,

MIRACL International Limited (Registration No 14713119) | 71-75 Shelton Street, London, WC2H 9JQ, United Kingdom
T: +44 (0) 20 8191 9262 | E: info@miracl.com | www.miracl.com

forming the backbone of any legal and contractual audit. There is no limit to the size of the data signed, allowing MIRACL Trust Proof to create signatures of the combined content and supporting documentation.

Process Adherence and Audit

Any staged system where compliance and approval are integral to the process. Signatures prove time and participation of process steps. It is possible to create multiple or sequenced signatures to match the process flow.

Hardware Token Generator Replacement

DVS can be seen as a drop-in replacement for costly and theft/loss prone hardware-based token generators.

Machine-to-Machine

DVS may also be used to sign arbitrary data such as API requests being exchanged programmatically between machines such as servers or IoT devices.

What the Service Provides

MIRACL Trust Proof is a service using the Designated Verifier Signature (DVS) digital signature scheme that allows the signing of any transaction (payment), user action, data transfer or Machine-Machine interaction to make it irrefutable. Authenticity of action can be proven due to the immutable, non-repudiable nature of the signatures. The solution meets the requirements of PSD2 for Dynamic Linking and Strong Customer Authentication.

Used to:

- Sign Transactions (payments), User Actions and any Digital Media
- Sign arbitrary programmatic data like API requests machine-machine & IoT
- Inexpensive PAYG SaaS contract with no termination notice
- Standards based API/SDK allows cross platform, OS independent deployment
- Supports P.A.I.N. = Privacy, Authenticity, Integrity and Non-Repudiation
- User-Device has cryptographic secret allowing dynamic linking, signing & authentication
- Signatures are immutable, non-repudiable and verifiable at any time
- Python, Django, NodeJS, Ruby, PHP, Java, .NET and more supported

Service benefits:

- Reduces fraudulent transactions whilst reducing false declines
- Meet the Strong Customer Authentication (SCA) requirements of PSD2
- Unique signature meets the “dynamic linking” requirement of PSD2
- Prevent transaction disputes and charge-backs. Facilitate their handling

MIRACL International Limited (Registration No 14713119) | 71-75 Shelton Street, London, WC2H 9JQ, United Kingdom
T: +44 (0) 20 8191 9262 | E: info@miracl.com | www.miracl.com

- Make Card-Not-Present (CNP) transactions as safe as real-world transactions
- Replace expensive, theft/loss prone hardware-based token generators
- Reduce cart abandonment from complex check-out
- No know practical/theoretical attacks against identity-based elliptic curve cryptography
- Replace transaction methods such as Transaction Authentication Number (TAN) codes.
- No reliance on Public Key Infrastructure (PKI)

Overview of the G-Cloud Service

To understand how MIRACL Trust Proof works, it is useful to understand how the MIRACL Trust ID (authentication) as a Service platform works:

Registration

- Users identities are verified either using email and/or custom methods such as knowledge-based challenges implemented using MIRACL's "Pluggable Verification" API.
- Once verified, users are issued with a "client secret". Importantly, this is generated in two or more halves from two or more physically separated "Distributed Trust Authorities" (DTAs) thus removing the single point of failure inherent in PKI-based solutions namely the Certificate Authority (CA).
- The two halves are combined in memory in the client application to temporarily create the client secret. The user is then asked to create a PIN which is cryptographically subtracted from the client secret and the remainder, the "client token" is stored in the client application. The complete client secret is then discarded.
- This is how MIRACL delivers true, two-factor authentication. The PIN is the first "something you know" factor and is not stored or transmitted anywhere. The token is the second "something you have" factor and is not transmitted anywhere. Note that it is cryptographically impossible to derive the PIN from the token in the event that the token is compromised.

Authentication

- To authenticate, the user enters their PIN which is recombined with the token to temporarily recreate the original client secret.
- The recreated client secret is then used in MIRACL's zero-knowledge M-Pin authentication protocol whereby the user can prove to the authentication server that it is in possession of the original client secret without having to transmit that secret across the network. This is achieved by the server issuing a unique per authentication attempt challenge to the client which performs a calculation on the challenge using the client secret and only returns the result. If the result is

MIRACL International Limited (Registration No 14713119) | 71-75 Shelton Street, London, WC2H 9JQ, United Kingdom
T: +44 (0) 20 8191 9262 | E: info@miracl.com | www.miracl.com

intercepted, it cannot be replayed, and the server can verify the result of the challenge just using its own server secret meaning that the server does not need to maintain a vulnerable password database.

MIRACL Trust Proof works in a similar manner to MIRACL Trust ID:

Registration

- The user is verified – this may simply be done by requiring the user to authenticate using MRACL Trust ID. In this case, no additional verification is required as the user is already verified.
- A public/private key pair is generated on the client and the public key is used as the basis for a new client secret also generated in two halves by the two DTAs.
- The returned halves are then combined on the client with the private key to generate a new client secret to be used for signing data. The private key is then discarded. The signing client secret is also split into a PIN and a token. This gives the user the opportunity to use different PINs to authenticate and to sign data.
- Note that the private key never leaves the device and is what makes MIRACL DVS key escrow-less and truly non-repudiable.

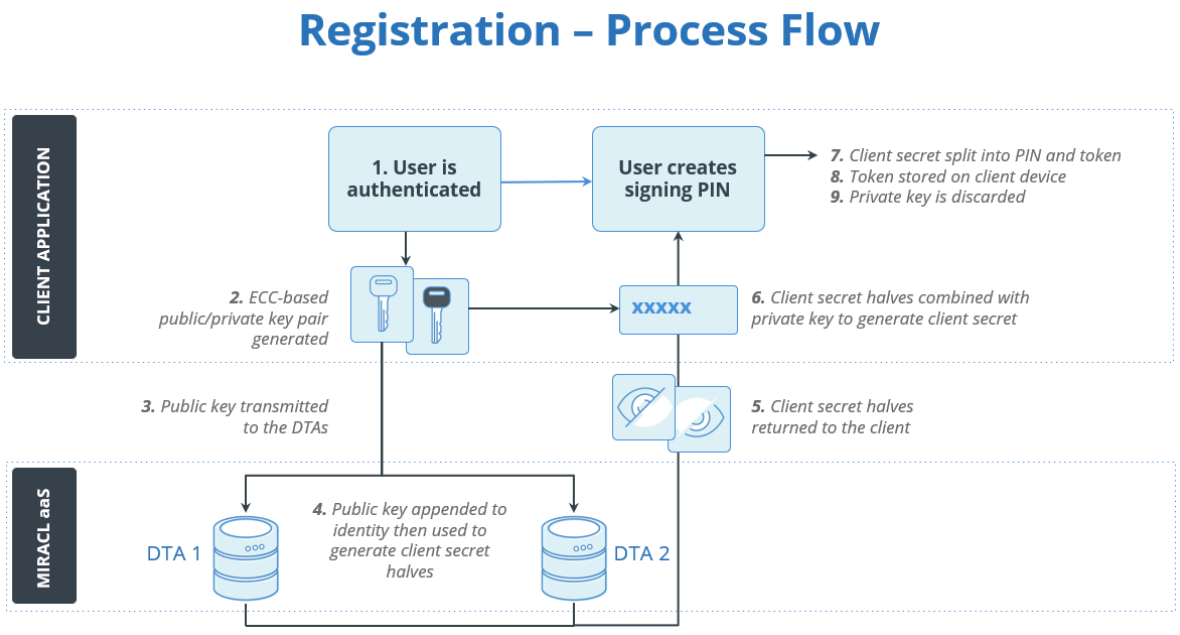

Figure 1 MIRACL User Registration Process Flow

Signing

- To sign data, the user simply enters their signing PIN which is combined with the token to recreate the signing client secret. This secret is then used to sign

arbitrary data. Note that it is not possible to create the signature without the PIN.

- The signature and corresponding payload are then sent to the MIRACL DVS service to be verified. This has the consequence of both verifying that the correct PIN was entered and that the signature matches the payload.
- Any data may be signed, however, it is recommended that the data is hashed first and that the hash instead is signed. This can reduce the size of requests sent to the MIRACL DVS signature verification service (for example if the data being signed is a large document). Hashing also allows MIRACL to verify signatures without having to see the content being signed thus overcoming any concerns around privacy, data retention and jurisdiction whilst still maintaining a cryptographic link between the payload and signature.

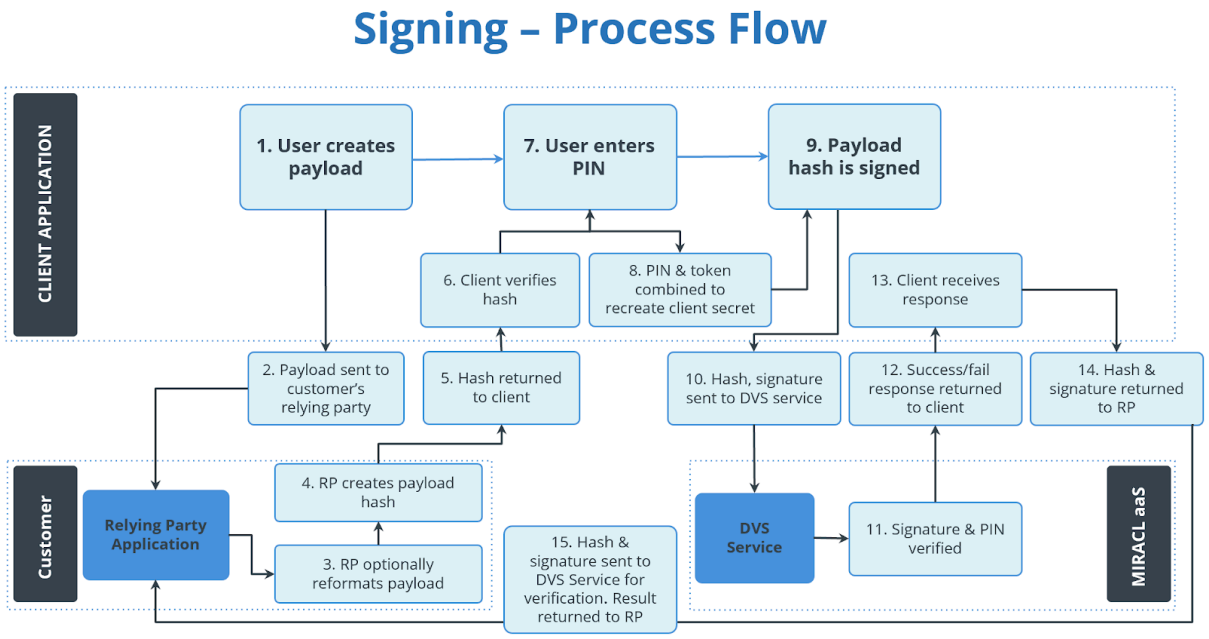

Figure 2 MIRACL Trust Proof Signing Process Flow

Service Management Options

Service configuration and management is normally administered via a dedicated service portal. From here you can set up new authentication endpoints, review logged activities on existing authentication endpoints, manage individual users and administrators of the service.

Our clients have the ability to integrate and extend these functions within their own service platform by utilising the Management APIs

User Enrolment Options

MIRACL Trust Proof can support any enrolment journey as defined by the client. Clients have the option of utilising MIRACL's default, email based, enrolment or validating the users' details (ID Proofing) and subsequently sending that user to MIRACL for enrolment.

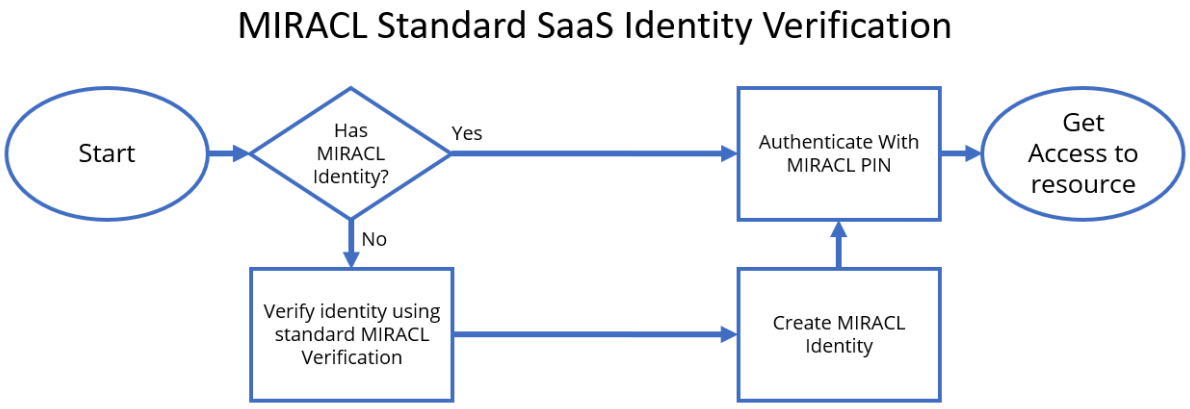

Figure 3 MIRACL Standard SaaS Identity Verification

Customised Enrolment is what enables the provision of custom verification methods instead of the default email confirmation process. Importantly, any user verification takes place outside the control and sight of MIRACL ensuring all data used for verification purposes remains tightly controlled by the client.

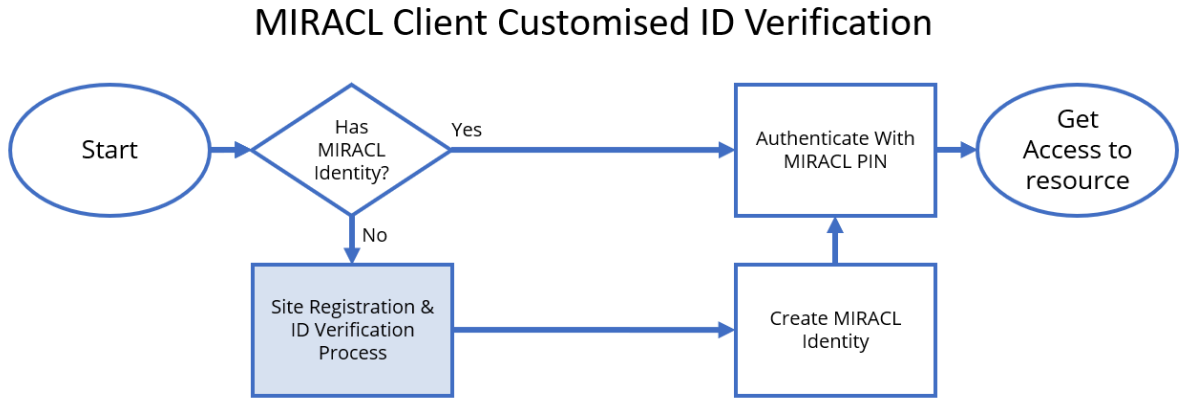

Figure 4 MIRACL Client Customised ID Verification

This flow consists of two parts:

- **External verification** - The Relying Party Application (RPA) creates their own unique verification flow (ID Proofing) based on their needs. Once the verification has passed, the RPA makes a request to the MIRACL platform to register an MPin Identity and receive an activation code for the given user.
- **User Registration -** With the received activation code, the Client activates the user identity and finalizes the registration process on our platform.

MIRACL International Limited (Registration No 14713119) | 71-75 Shelton Street, London, WC2H 9JQ, United Kingdom
T: +44 (0) 20 8191 9262 | E: info@miracl.com | www.miracl.com

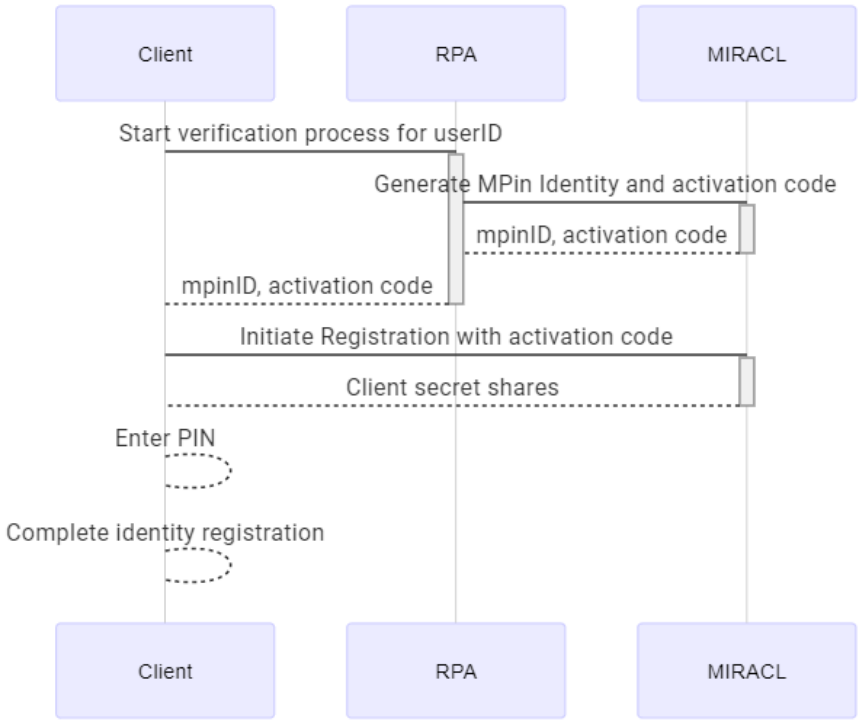

Figure 5 Verification Process

SLA Options

By default MIRACL Trust ID is provided with a 100% service level agreement through the provision of various options including multiple redundancies, geographic and cloud diversity.

Support Options

All contracts are provided with office hour (9am-5pm GMT) phone and email support for client staff. This can be extended to 24 x 7 support for mission critical applications or even direct end user support as agreed between the parties.

Consultancy and Development Resources

Standard support includes assisting our clients to design and integrate the MIRACL Trust Proof within their service platform. We can provide any missing skills and take a more proactive approach. For example designing user flows, creating integration plans, project managing the integration and even providing the hands-on development resources to integrate the service.

Associated Services

MIRACL Trust Proof is provided as a SaaS service and easily integrated into any OIDC compliant platform. For that reason both internal teams and independent 3rd party contractors will be able to integrate the service with minimal or no assistance from MIRACL.

MIRACL International Limited (Registration No 14713119) | 71-75 Shelton Street, London, WC2H 9JQ, United Kingdom
T: +44 (0) 20 8191 9262 | E: info@miracl.com | www.miracl.com

See integration documentation here:

https://miracl.com/resources/docs/get-started/overview/

The documentation for DVS (signing) can be found here:

https://miracl.com/resources/docs/guides/dvs/

Actual integration to a web service takes little more than a day BUT basic design of user flows and security procedures can take longer. By using established user flow templates the entire process can be completed within a week for most web services.

MIRACL's current service stack has capacity to service in the order of 10,000,000 additional users depending on usage frequency and time distribution patterns. Engineered on a highly scalable and flexible Kubernetes stack, additional capacity can be brought online within one or two minutes.

If required, we can also implement entirely independent authentication service stacks on Hybrid or Multi cloud infrastructures.

Creation of different tailored multi cloud or hybrid cloud infrastructures will increase minimum charges. Please refer to our pricing document for final details of costs.

Rapid Integration to Other Platforms Or From Legacy Service

Significant time and effort can be saved by integrating MIRACL Trust Proof to existing identity or access management platforms supplied by companies such as Auth0, ForgeRock, Okta, OneLogin and WSO2 to name but a few. Please speak to us to discuss integration options for the access management platform of your choice.

In almost all cases it should be relatively simple to migrate existing end users from your authentication framework to MIRACL Trust Proof.

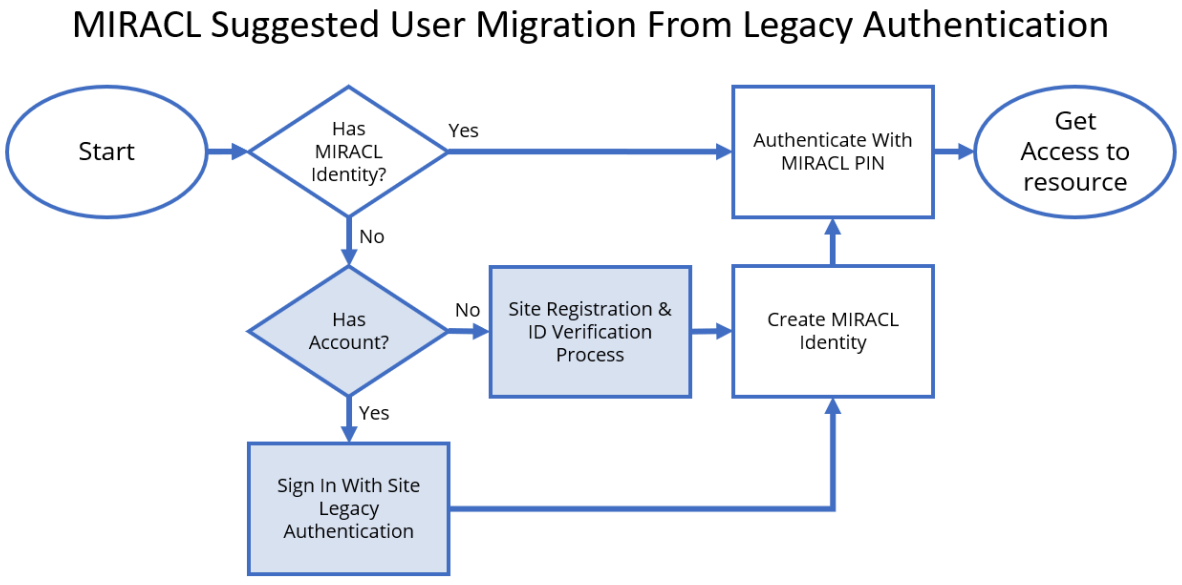

Figure 6 MIRACL Suggested User Migration from Legacy Authentication

2. Data Protection

Information Assurance

We do not store any of the Buyer's users' information with the exception of an identity token, and an authentication history. We are Cyber Essentials certified and comply with IASME governance standards.

Data Back-Up and Restoration

MIRACL runs full backups monthly. Incremental backups are run weekly and then daily. Users cannot control these, but we could agree something different for a user should they need it. Effectively, in the unlikely event of a complete outage, all users who had registered since the last backup would need to re-register. Registration typically takes only a few seconds.

Business continuity statement/plan

The MIRACL business continuity plan covers production systems, staff, support and general operations. The service runs of course from the Google Cloud and has been architected for being resilient. Staff are fully capable of performing all functions from home or any other location. Support staff are backed up by developers where necessary. Effectively, we do not expect any downtime for the service unless due to extreme circumstances.

A more detailed plan can be provided to the buyer on request.

Privacy by Design

MIRACL adopts privacy by design. We do not have access to any of the Buyers' users' data and do not have a database of any identifiable information as we use an industry leading zero knowledge proof to carry authentications and signing.

MIRACL International Limited (Registration No 14713119) | 71-75 Shelton Street, London, WC2H 9JQ, United Kingdom
T: +44 (0) 20 8191 9262 | E: info@miracl.com | www.miracl.com

3. Using the service

Ordering and Invoicing

To order the MIRACL Trust Service, the buyer should email their requirements to be discussed by email first to sales@miracl.com.

Assistance will be provided in completing an Order Form thereafter as needed.

Availability of Trial/Free Tier Service

All users of MIRACL Trust Proof service get the first 10,000 uses/month free of charge. This includes basic email support and basic customisation, which is great for larger organisations to trial the service in their test environment and smaller organisations to use indefinitely.

The Trial Service can be signed up to online in minutes at:

https://miracl.com/get-started/

On-Boarding, Off-Boarding, Service Migration, Scope etc.

It is possible for a Buyer to use the service completely without interaction with MIRACL or our staff, i.e. in a completely self-service model. They would create a login on our developer portal, do a small amount of configuration, and begin testing, or even go-live, completely without assistance. We have had a client integrate with our service in a matter of minutes. However, it is typical to have a technical resource on our side discuss their solution and requirements, and work with them to onboard. Full documentation is provided, and all questions will be answered promptly by the implementation team.

Whilst we have yet to have a customer leave us, off-boarding would be even more trivial. We keep no customer data other than an identity token, secure keys and an authentication history. Migrating from MIRACL would involve the customer changing their configuration to use a different provider, or changing their configuration to perhaps go back to using username / passwords. As they rolled this out over time, the authentications to MIRACL would reduce (as would their bill, as we bill per use of the service) until ultimately they had no further users using MIRACL. They could then ask for a download (should they want it) of authentication history, and we would then simply remove their account.

As noted above, we have not yet had a customer migrate away from our service, but we would be honourable and give every assistance should a customer wish to do so. All and any exit plans would be considered. If we deemed the exit plan a large effort, we may ask for some commercial consideration for such assistance.

MIRACL International Limited (Registration No 14713119) | 71-75 Shelton Street, London, WC2H 9JQ, United Kingdom
T: +44 (0) 20 8191 9262 | E: info@miracl.com | www.miracl.com

Training

Introductory onboarding is provided to the Buyer's service implementor/admin to go through the main features of MIRACL Trust Proof. For end-users steps are described on the services page and user guide.

Implementation Plan

MIRACL Trust Proof can be implemented in as little as one hour, depending on the Buyers existing infrastructure. Service implementation is described in the documentation and if further information is required a detailed implementation plan can be provided to the buyer on request.

- MIRACL Trust Proof is available with a subscription to the MIRACL Trust ID as a Service platform.
- SDKs are available in JavaScript (to implement in-browser signing) and iOS/Android (for in-app signing).
- The server SDK (used to send requests to the MIRACL DVS service) is currently available in .NET and .NET Core with support for other platforms coming soon.
- ForgeRock integration requires: ForgeRock license, MIRACL Trust Proof - ForgeRock Module, MIRACL Trust Proof and ID subscriptions.

Service Management

MIRACL attempts to provide a fully available service. Upgrades are done out-of-hours, and when such upgrades occur, the downtime is only during the services re-start, which is often / typically measured in a handful of seconds. Even during this downtime, authentications will still be processed (by another server) it is only new registrations that will fail.

As we work on an agile basis, sometimes we do not upgrade / restart the service for months, and other times we may do an upgrade once, maybe even twice a month, but as noted above, each such upgrade will only affect new registrations, and as such, will only be for a small number of seconds.

Service Constraints

No constraints on performance and service hosted on a leading cloud provider allowing elastic increase/decrease of resources as required at the time of authentication. service availability and support hours as agreed between the Buyer and MIRACL. Maintenance and service updates carried out outside of business hours and last seconds, to minimise planned downtime.

Customisation includes Buyer logo, colours, service name.

MIRACL International Limited (Registration No 14713119) | 71-75 Shelton Street, London, WC2H 9JQ, United Kingdom
T: +44 (0) 20 8191 9262 | E: info@miracl.com | www.miracl.com

Service Levels

MIRACL provides 100% SLA. Support from a 48 hour email response through to a 24x7 telephone. In addition to the standard service levels, a tailored one can be discussed and agreed prior to an order being placed with the Buyer.

Outage and Maintenance Management

MIRACL has architected the service around 100% availability. This includes using predictive auto-scaling on elastic cloud servers that scale based on usage.

We run not only internal availability tests, but also continuously run actual authentications from 6 points on the globe to ensure absolute knowledge about end-to-end availability of the service, and this information is used to define our downtime statistics.

Financial Recompense Model for not Meeting Service Levels

Service Level Agreement Credit. We provide a credit on monthly fees should our service level be less than we are bound to provide. SLA credit is not a refund, cannot be exchanged into a cash amount, requires you to have paid any outstanding invoices and expires upon termination of your customer contract. SLA credit is the sole and exclusive remedy for any failure by MIRACL to meet its obligations under this SLA. Look down the left column to find the service level you are contracted for. Look across the column headings to find what the uptime of the service was for the month and the cell intersection shows the credit calculated as a percentage of fees paid for the period being assessed. Please see "Service Level Guarantee" table for a detailed breakdown of support levels.

		Achieved			
		100%	**98% to 100%**	**95% to 98%**	**Less than 95%**
Service Level Guarantee	100%	0%	10%	25%	50%

Figure 7 Service Level Guarantee

MIRACL International Limited (Registration No 14713119) | 71-75 Shelton Street, London, WC2H 9JQ, United Kingdom
T: +44 (0) 20 8191 9262 | E: info@miracl.com | www.miracl.com

4. Provision of the service

Customer Responsibilities

The Customer acknowledges that the data held by MIRACL in connection with the Service is minimal and shall, unless otherwise agreed, be limited to the username and email address of each user. The Customer shall own the right to all of the Customer data and has the sole responsibility for the legality, reliability, integrity, accuracy and quality of all such Customer data.

The Customer acknowledges that the Services may enable or assist it to access the website content of, correspond with, and purchase products and services from, third parties via third-party websites and that it does so solely at its own risk. MIRACL makes no representation, warranty or commitment and shall have no liability or obligation whatsoever in relation to the content or use of, or correspondence with, any such third-party website, or any transactions completed, and any contract entered into by the Customer, with any such third party. Any contract entered into and any transaction completed via any third-party website is between the Customer and the relevant third party, and not MIRACL. MIRACL recommends that the Customer refers to the third party's website terms and conditions and privacy policy prior to using the relevant third-party website. MIRACL does not endorse or approve any third-party website nor the content of any of the third-party website made available via the Services

Furthermore, the Customer shall, without affecting any of its other obligations:

- comply with all applicable laws and regulations with respect to its activities under the Agreement;
- ensure that the Authorised Users use the Services and the Documentation in accordance with the Agreement and shall be responsible for any Authorised User's breach of the Agreement;
- be responsible for all actions and omissions of its Users, including but not limited to the addition by Users of any applications or the subscription of additional features relating to the Services;
- obtain and shall maintain all necessary licences, consents, and permissions necessary for MIRACL, its contractors and agents to perform their obligations in connection with the Services;
- ensure that its network and systems comply with any relevant specifications provided by MIRACL from time to time; and
- be, to the extent permitted by law and except as otherwise expressly provided in the Agreement, solely responsible for procuring, maintaining and securing its network connections and telecommunications links from its systems to the MIRACL's data centres, and all problems, conditions, delays, delivery failures and all other loss or damage arising from or relating to the Customer's network connections or telecommunications links or caused by the internet.

Technical Requirements and Client-Side Requirements

MIRACL Trust Proof only requires an active internet connection and works on all browsers on any device.

If the Buyer wishes to integrate MIRACL Trust Proof with their native mobile then iOS8 and Android 4.1 or later are required.

Outcomes/Deliverables

The client will get industry leading passwordless multi factor digital signing for all their users.

Development life cycle of the solution

MIRACL uses the Agile software methodology, working in two weeks sprints. This gives us immense flexibility over the project duration to assign additional resources, or bring in other assistance if required. Tasks are prioritised and categorised to include:

- issues / bug-fixes
- customer feature request
- product improvement
- strategic product change

MIRACL uses a CI/CD (continuous integration/continuous deployment) methodology to continually integrate, deploy and test all code changes. Production changes are also automated, but under manual control (of 2 people).

After-sales Account Management

At MIRACL we pride ourselves in great customer satisfaction and strive for long-term successful and growing business relationships. We will manage the relationship with frequent communication as agreed. Whilst we will work in any reasonable way requested by our clients, typically we allocate an account manager to every client who will be the first point of contact for queries and requests as well as the channel via which customer product improvements and suggestions can be requested.

Termination Process

MIRACL Trust Proof is a software only solution so the termination process is very simple with a one month minimum period, which is automatically renewed on a month-by-month basis if the buyer continues using the service. To terminate, the buyer simply needs to stop using the service and the contract will be terminated at the next month's renewal date. There are no early termination costs. The customer has complete ownership and flexibility should they want to wind-down the service. We will provide every assistance to them should they want to do this.

MIRACL International Limited (Registration No 14713119) | 71-75 Shelton Street, London, WC2H 9JQ, United Kingdom
T: +44 (0) 20 8191 9262 | E: info@miracl.com | www.miracl.com

5. Our experience

Case Studies

Banking

MIRACL's client is using Miracl Trust Proof for transaction signing to meet PS2D requirements for Strong Customer Authentication (SCA) and dynamic linking.

MIRACL was chosen for its industry leading digital verified signature scheme and to avoid the cost and complexity of PKI schemes while at the same time benefiting from our unique single step authentication at every point of user interaction for the best user experience.

Clients

Our clients include:

6. Contact Details

Michael Tanaka
Chief Commercial Officer

m: +44 (0) 77 6777 6141

t: +44 (0) 20 8191 9264

e: michael.tanaka@miracl.com