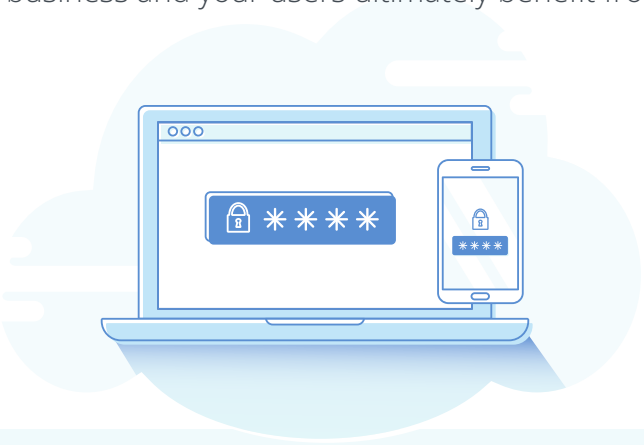
MIRACL Trust® Ensures the Secure Future of Your Business

MIRACL Trust® is true two-factor authentication which is designed to grow with your business whilst eliminating the need for any outdated security practices such as PKI , SMS and password databases. MIRACL Trust can easily be tailored to meet your security goals, it is easy to integrate into your business and your users ultimately benefit from a simplier login experience.



WEB AND MOBILE APPS
Remove password threats completely

CLOUD SERVICES
Establish integrity in cloud security

INTERNET OF THINGS
Instant trust between "things"

MIRACL Trust® Multi-factor Authentication For Enterprise Employees And External Users

- Meets "strong authentication" requirement for PSD2
- No vulnerable password database
- Mitigates against Man-in-the-middle, Phishing, Fraud, Identity Theft
- No valuable security information stored on device or in the cloud
- No valuable security information sent across web or SMS
- No directory synchronization required for service
- Improved customer onboarding (PIN vs password)
- End user self-service support for "I forgot'

MIRACL Security for the Cloud

- **Hardware Infrastructure:** From chipset to hardware, ensure the identity of a device.
- **Service Deployment:** Authenticate virtualized applications and provide secure connectivity.
- **User Identity:** Remove password risk for end user authentication into cloud apps.

MIRACL Security for IoT

- **Strong:** Every device gets key or key share at manufacture. No key database to secure.
- **Stronger:** Stored key and secret in trust zone on hardware. Scalable security without overhead hassles.
- **Stronger & Slimmer:** Hardware PUF secures part of the secret. Same strength/reduced cost. Availability across chipsets.

MIRACL Trust® Delivers a Strong, Simple Multi-Factor Authentication Solution For PSD2 And More

Provides Strong Customer Authentication for PSD2 And A Better User Experience For Customers

MIRACL Trust® is a cloud-based service that provides secure, multi-factor authentication to external users, employees and partners without sending authentication credentials across the web for storage in the cloud. Users independently demonstrate possession through a software token located in a web browser or mobile application, and knowledge by providing the 4-digit PIN chosen during authorization.

Demonstrates Possession: No Security Information Stored In Whole Form At Any Time.

End users of MIRACL Trust® multi-factor authentication receive a software token in their web browser or mobile application during the registration process. The information in this token is incomplete and does not reveal any information about the identity of the user or the authentication system itself. The MIRACL Trust® authentication system does not store, or require you to store, any valuable security information in any place at any time, nor do we require you to upload any of your authentication data into our service.

Demonstrates Knowledge: No Information Sent In Whole Form Across Any Network

MIRACL Trust® Authentication uses a Zero-Knowledge Protocol, which means that an individual can prove they know a secret, without actually revealing that secret to the verifying service. No security-related information is stored on our servers or yours which means that there is nothing for a hacker to steal. User authentication takes place on the device (against an incomplete software token in a web browser or mobile application) and is secure against database breaches and man-in-the-middle attacks because no credentials are exchanged between clients and servers in whole form (unlike passwords and two-factor).

Supports Multiple Authentication Factors / Notification Channels You Currently Have In Place

MIRACL Trust® easily integrates into any point of your web and mobile application security process, and can support the authentication mechanisms you have planned / in place (including biometrics) to provide a nonrepudiable audit trail of the people, devices, and transactions being authenticated by your users or machines.

Eliminates Multiple Points Of Compromise Within Your Existing Security Systems

Current sources of security origination (e.g. digital certificates, password databases) can be compromised, provide a single point for a cyber-attack, and cannot scale for the future of business (e.g. cloud, IoT). MIRACL Trust® employs the principle of distributed trust (i.e. the authentication server and client keys are generated independently by two autonomous, distributed trust authorities (DTA). A DTA can be located in any cloud environment, and does not store the key material it provides, nor does it have any information about the other material required to create an identity key. A MIRACL Trust® customer can host one of the DTA's within their infrastructure if required as part of the registration process controls. MIRACL would run the other.

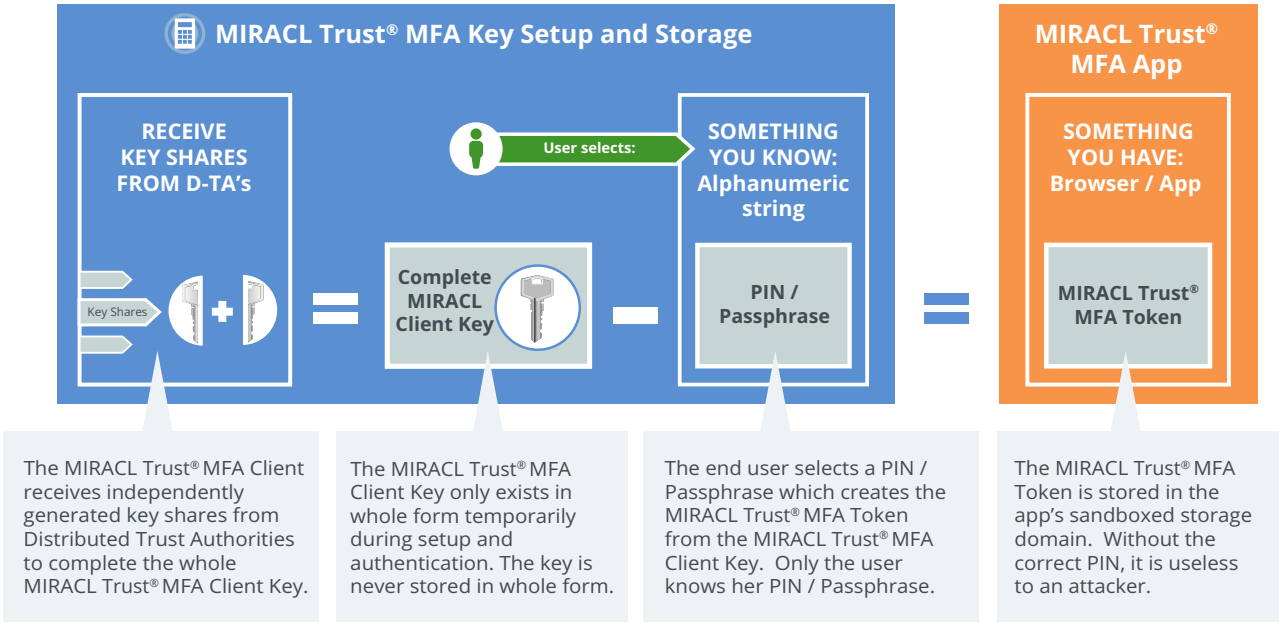
Scales To Support Identity Credentials Across Almost All Business Security Challenges

MIRACL Trust® multi-factor authentication for external end-users as part of PSD2 is only the first security challenge we can solve for your digital business. Our single security platform can change entirely the concept of identity credentials across your organization including authentication into VPN, replacing digital certificates and their maintenance, enabling digital verified signatures in your web and mobile applications, and more. Start with PSD2 today and let us help you address other challenges when your timeline allows.

MIRACL Distributes Trust to Eliminate Single and Multiple Points of Cybersecurity Compromise

Distributing Trust Removes 'Point of Origin Compromise' Security Risk

- Current MIRACL Trust® multi-factor authentication requires an end user to authenticate to a web or mobile service using identity key material provided by two independent Distributed Trusted Authorities (DTA).
- A DTA does not store the key material it provides, nor does it have any information about the other material required to create an identity key.
- You or your customers can run a DTA to produce one of the two unique keys needed to connect a client to a digital service.
- MIRACL's Distributed Trust Authority (D-TA) architecture is an advancement in elliptic curve cryptography that results in eliminating single points of compromise without affecting the customer's privacy of or security efficacy.



User Setup – Splitting MIRACL Trust® Client Key into MIRACL Trust® Token and PIN or other factors

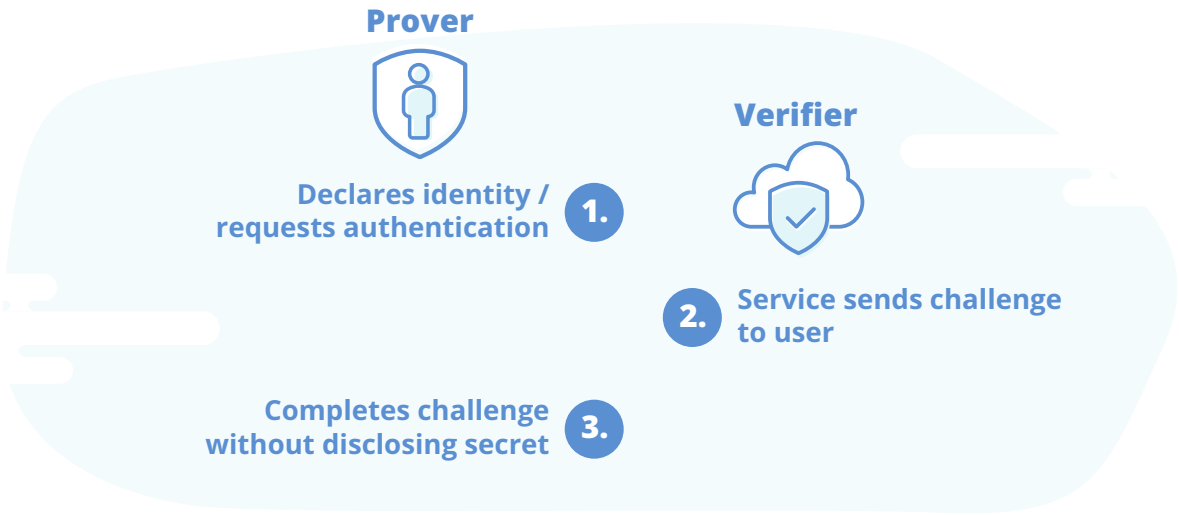
The MIRACL Trust® Identity Key

- End users choose their PIN, which is not stored anywhere (something user knows)
- PIN extracted from MIRACL Trust® Client Key, ONLY MIRACL Trust® TOKEN is stored in sandboxed app domain (something user has)
- Neither PIN nor Token, or combination of two, is ever exchanged or stored in whole form (benefit of zero knowledge proof protocols)

MIRACL Reduces Risk Of Malware and Man-In-The Middle Attacks Through Use Of Zero-Knowledge Proof

Process: Prove You Know A Secret Without Telling The Secret To Me

MIRACL Trust® utilizes an ISO/IEC approved zero-knowledge proof, which means that the end user can prove that they know a secret, without revealing that secret to the verifying service. Because no data is transmitted in whole form at any time, the service and its users are not vulnerable to the "man-in-the-middle attacks" (as with password and SMS two-step authentication).



Possession: No Security Information Stored In Whole Form At Any Time.

End users of MIRACL Trust® multi-factor authentication receive a software token in their web browser or mobile application during our / your registration process. The information in this token is incomplete and does not reveal any information about the identity of the user or the authentication system itself. The MIRACL Trust® authentication system does not store, or require you to store, any valuable security information in any place at any time, nor do we require you to upload any of your authentication data into our service.

Knowledge: No Information Sent In Whole Form Across Any Network

MIRACL Trust® multi-factor authentication asserts the identity of a user through the software token on a web or mobile device, and does not store valuable security data about any user, or the service in whole form at any time. Entry of a user's 4-digit PIN must be correct (within specified number of attempts) to validate a user's identity through the token and the device, and the authentication system does not send any security data in whole form across the web or SMS in the response back to the cloud. This not only removes the risk of man-in-the-middle attacks (since there is nothing to steal in transit) but also removes entirely any password database risk to you and your end users. Users are more likely to onboard successfully into your service with a 4-digit PIN (vs a complex password) and are able to reset their 4-digit PIN at any time without assistance from your teams.

Deliver Strong Authentication Into Any Web Or Mobile Application Quickly and Easily For PSD2 Compliance

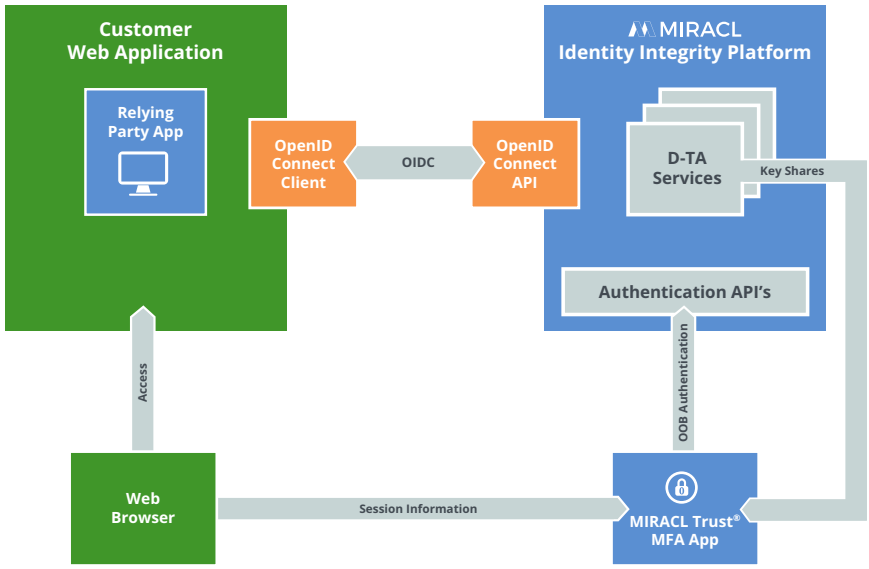
MIRACL Trust® for website login in-browser or with a smartphone application is designed to work at an internet scale; delivers multi-factor authentication to your external audiences with no disruption of the service; improves the user experience; and minimizes customer churn when deploying additional security, all at a fraction of the cost of the competition. After registering an app (standard, SSO or RADIUS) with the MIRACL Trust® MFA Authentication portal (trust.miracl.cloud) you will be issued the keys to integrate MIRACL authentication into your product.

MIRACL Trust® – Multi-factor Authentication is federated to web applications through the use of the OpenID Connect Protocol, an IETF standard.

OpenID Connect is extensible, allowing participants to use optional features such as encryption of identity data, discovery of OpenID Providers, and session management, when it makes sense for them.

MIRACL OpenID Connect SDKs enables you to offload authentication to your server through an identity layer above the OAuth 2.0 protocol. Download the relevant SDK and follow the sample app tutorial. When a user clicks the login button, end users can then use the MIRACL Trust® mobile app and pin pad to register and login to your service. Mobile SDKs are also available for creating your own branded version of the mobile app.

Strong Authentication is federated to web applications through the use of the OpenID Connect Protocol, an emerging IETF standard



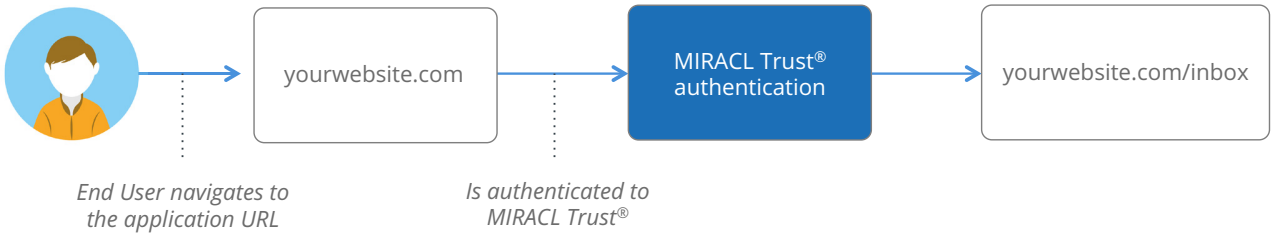
MIRACL Trust® for mobile login can secure end users into mobile applications with the same multi-factor authentication solution through our software development kits (SDKs) for Android or iOS. SDKs also allow you to prevent installation of your authentication application onto a rooted mobile device and reduces risk from malware and "man-in-the-middle-attacks". After integrating MIRACL Trust® into your mobile application through our cloud-based portal (trust.miracl.cloud) your business can successfully onboard end users through the same identity verification and PIN creation process they would find in a web-enabled application.

iOS

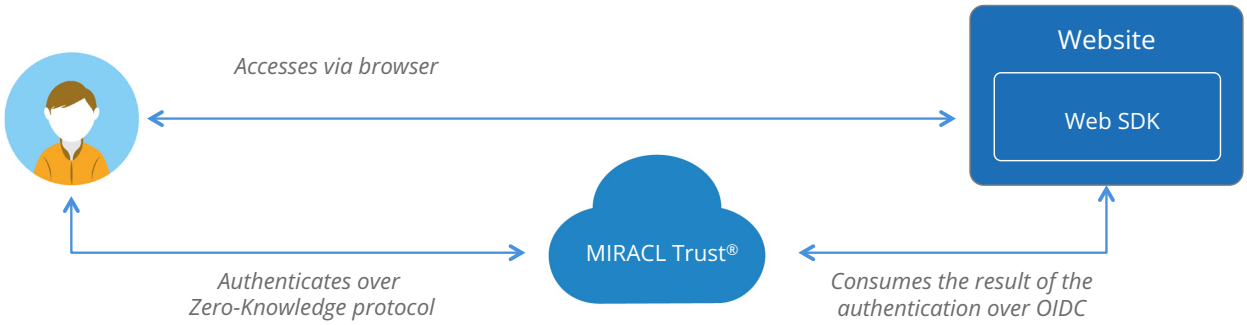
android

Simple, Secure End-User Authentication Into Web and Mobile Apps With Self-Service PIN Management

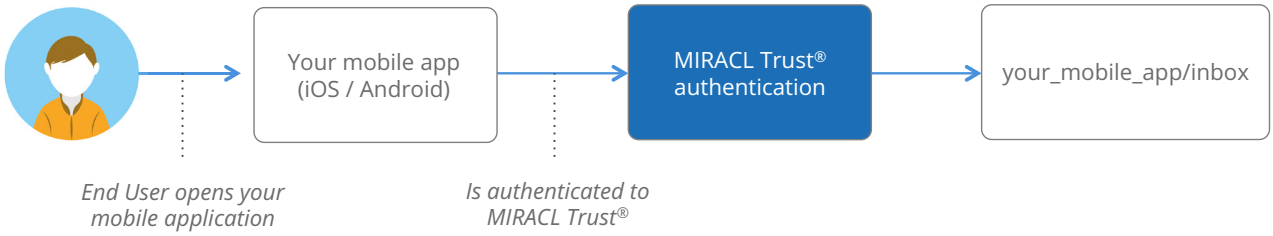
MIRACL Trust® for website application (in-browser) login: user flows



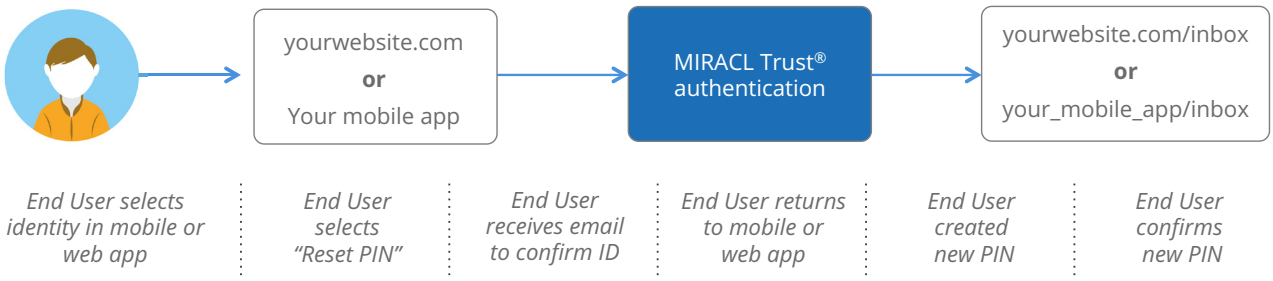
MIRACL Trust® for website application login with mobile authenticator



MIRACL Trust® for mobile application login



MIRACL Trust® End User Self-Service PIN Reset For Web and Mobile MFA Access



Lower the Total Cost of Security Ownership Across Your Business with One Secure and Easy-to-use Platform

- Delivers PSD2 strong authentication requirement
- Provides security simply for web or mobile applications
- Integrates into any web and mobile app easily with SDKs
- 24/7 NoC support and 99.999% guaranteed uptime
- Authentication to web apps through OpenID Connect
- Single platform for all credentials including VPN, certificate replacement, digital verified signatures
- Extends platform to enterprise users, cloud, and IoT

Learn more at www.miracl.com

About MIRACL

- UK cryptography company focused exclusively on strong security
- Our M-Pin protocol is currently used by Experian to protect UK taxpayers (Level of Assurance 3)
- Founded by authority in cryptography (Google Scholar i10 index=52)
- Our crypto library is proven with over +30 years usage under open-source license
- M-Pin cryptographic protocol published as IETF (draft)
- Our security does not store or send any critical security information in whole form
- Our platform removes password and credentials database risks completely
- We provide scalable “strong authentication” solution which meets the PSD2 requirement

“Protecting people and giving them a good user experience is a key goal, MIRACL is a pioneering company that helps us achieve that”

Nick Mothershaw, UK&I Dir of Identity & Fraud

experian

For more knowledge about MIRACL Trust MFA:

Michael Tanaka, Chief Commercial Officer
michael.tanaka@miracl.com