Next-gen privacy-preserving biometrics

Nothing to remember. Nothing to steal. You are the key.
Keyless is a deeptech cybersecurity company founded by renowned security experts, experienced technologists and business leaders, backed by top-tier VCs, bringing 10+ years of research in biometrics and cryptography to life.

Keyless provides a next-gen, privacy-enhancing biometric authentication solution combining proprietary multi-modal biometrics and advanced cryptographic technology in a distributed architecture.

Our zero-knowledge biometric solution eliminates the need for businesses to store and manage biometric data, passwords, and any other sensitive information without compromising on convenience or privacy.
Enable everyone to seamlessly access any digital service from any device, at any time, while keeping personal credentials safe, private and under control. Nothing to remember. Nothing to steal. You are the key. At Keyless, we believe in a world where people can be in control of their privacy and identity.
the world is going passwordless

51% of passwords are reused across services
(University of Oxford)

$5bn Facebook fine for years of privacy violation
(Reuters)

2.3bn credentials stolen in 2017 alone
(Shape Security)

Simplicity vs. Privacy vs. Security

“By 2022, Gartner predicts that 60% of large and global enterprises, and 90% of midsize enterprises, will implement passwordless methods.”
why now

Accounts Hacked:
- Yahoo: 3 billion
- MySpace: 500 million
- Facebook: 267 million
- Equifax: 143 million
- LinkedIN: 117 million

1960s
- PASSWORDS
  - Single Factor

1990s
- HARD TOKENS
  - Two Factor

2000s
- SOFT TOKENS
  - SMS or App TOTP

2010s
- BIOMETRICS
  - Fingerprint, face
    - Local authentication
    - Centralized authentication
The future is private

Introducing the world's first, privacy-preserving biometric authentication and personal identity management platform.

Unique combination of multi-modal biometrics and privacy-enhancing technologies for seamless digital identification.

Existing biometric methods have fundamental limitations

**Local Authentication**
- **Local**: User tied to one device
- **Reach**: Not universal
- **Immutable**: Leakage of data possible
- **Privacy**: User not in control of data
- **Security**: Easy to hack (single factor)

**Centralized Authentication**
- **Security**: Central honeypot
- **Privacy**: User not in control of data
- **Immutable**: Leakage of data possible when sent to server

### Problems

- **Fundamental limitations**

---

**Facebook to Pay $550 Million to Settle Facial Recognition Suit**
It was another black mark on the privacy record of the social network, which also reported its quarterly earnings.

---

**The Growing Legal and Regulatory Implications of Collecting Biometric Data**

The growing legal and regulatory implications of collecting biometric data are significant. The accuracy, efficiency, and effectiveness of the biometric authentication experience under the actual collection and storage of data is challenging. Security risks are also significant.
Keyless provides a next-gen, privacy-enhancing biometric authentication solution combining proprietary multi-modal biometrics (facial and behavioral) and advanced cryptographic technology.

Unparalleled benefits...

- Software only solution - accessible through any device, platform and application
- Enables multiple use cases in zero-trust authentication, digital identity and beyond
- No biometrics stored anywhere, not on device, not on a central database
- 300x faster than general purpose MPC (100ms instead of tens of seconds)
- Highly computationally effective (no battery drainage)

Recognized by:

- Gartner
- BNP Paribas
- Integrium Security
- Telsy

MFA by design – Distributed biometric matching

Eliminates security risk such as fraud, phishing and credential reuse

Exceeds strictest regulatory req. – GDPR, CCPA, PSD2

Authenticate the end-user, not just the device / end-point
Gartner IAM Hype Cycle Jul 2020

**Biometric Authentication**

- **Benefit Rating**: Moderate
- **Market Penetration**: 5% to 20% of target audience
- **Maturity**: Early mainstream
- **Sample Vendors**: Auraya Systems, FaceTec, iProov, ImageWare Systems, **Keyless Technologies**, OneVisage, SensibleVision

---

**Hype Cycle for Identity and Access Management Technologies, 2020**

- **Benefit Rating**: Moderate
- **Market Penetration**: 5% to 20% of target audience
- **Maturity**: Early mainstream
- **Sample Vendors**: Auraya Systems, FaceTec, iProov, ImageWare Systems, **Keyless Technologies**, OneVisage, SensibleVision
**how it works**

1. Capture biometrics
2. Split into shares and encrypt
3. Send to multiple independent servers and match encrypted shares against encrypted patterns
4. Recombine secret for one-time use

---

- **Locally on user’s device**
  - Nothing to remember
  - Enroll once, use everywhere, any platform, any device

- **Distributed on Keyless network**
  - Nothing to steal
  - No central honeypot, no data on user devices

- **Locally on user’s device**
  - User in control
  - Fundamental privacy preserving technology

Note: For further information on the technology, enrollment and authentication flow, please click [here](#).
Zero-knowledge proofs for device identity

- Zero-knowledge proofs to securely verify authentication requests are being launched from a user's trusted device
- No information about user's identity can be obtained

AI and cryptography at the edge

- Deep learning on user's device to extract biometric template
- Irreversible transformation of data into shards using Shamir's Secret Sharing
- Permanent deletion from device, after shares sent to servers in Keyless Network

Distributed private computation

- Processing of authentication with advanced secure multi-party computation protocols in the cloud
- Independent validation of authentication requests without learning anything about the user's biometric data
multi-factor by design

User-friendly visible protection

Privacy-preserving device recognition (ZKP)

Use anywhere from any device and any channel

Continuous and dynamic multi-factor authentication

AI-driven state-of-the-art anti-spoofing

Invisible protection

Zero-knowledge, AI-driven physical and behavioral biometrics

Factor agnostic, multiple biometrics; private by design

Distributed private computation (sMPC, SSS)
product lines

Keyless Authenticator

Workforce Auth [B2B]

Enables business to adopt zero-trust passwordless authentication and protect their remote workforce
✓ Employee identification and device verification
✓ HW / OS agnostic – same experience for all employees from laptop and mobile
✓ Cost and time saving

Keyless Mobile SDK


Enables businesses to strongly authenticate their consumers under PSD2 in one simple action
✓ Enroll once – use everywhere and on any device
✓ Meets Strong Customer Authentication requirement (PSD2)
✓ No risk of consumer PII/biometrics

Keyless PIM SDK and PIM Wallet

Personal Identity Mgmt. [B2C]

Enables individuals to easily and securely manage their own personal info and privacy
✓ Self-provisioning and management of user own personal data
✓ Selective disclosure of personal data in a private, secure manner

Coming in 2022
Passwordless MFA across all employee touchpoints

workforce authentication

One authenticator for many use cases

Passwordless SSO
Keyless integrates with your existing IdP to enable passwordless MFA for your enterprise apps in minutes.

Desktop MFA
Keyless eliminates passwords from your Windows 7,8 and 10 login experience and offers built-in MFA with one look.

Remote Login
Keyless enables your workforce to securely authenticate to your VPNs - on any device, from any location.
consumer authentication

Many use cases, easy to integrate

**PSD2 SCA**
Produce your customers with a unified experience with built-in MFA that eliminates fraud, phishing and credential reuse

**Customer KYC and MFA**
Integrate superior passwordless security that authenticates people, not devices, in minutes - for all users, on any device

**E-signature**
Provide your users the ability to electronically sign documents using their face biometrics, from any device
unique capabilities powered by breakthrough technology

Software Based - Hardware Agnostic
Keyless does not rely on the device hardware or sensors, and can thus be deployed on a large set of devices and appliances
No reliance on Face ID or other 3rd party tech

Enroll Once - Use Everywhere
Users enroll once in a 5-second process and can use it across all devices and touchpoints and enable seamless recovery
Multi-device support and simple recovery

Authenticate Users - Not Devices
Keyless identifies users across every touchpoint, so you can make sure that the user who is logging in is actually the correct user
Unique identity for every user

No Biometrics/PII Stored Anywhere
Keyless exceeds strictest privacy compliance requirements since no PII/biometric data is stored anywhere
Exceeds privacy compliance beyond GDPR
Secure remote access for virtual exams

In response to COVID-19 lockdowns, LUISS Guido Carli University partnered with Keyless and Cisco, to allow their students to sit their summer exams remotely.

- **12,000** Students
- **6,000** Virtual exams
- **2,200** Auth/day
- **10** Days to go-live

Keyless Authenticator™
Simple, secure, and above all, private

- **Nothing to remember**
  - No central honeypot
  - No data on user device
- **Anti-fraud protection**
  - Eliminates phishing and man-in-the-middle
- **Nothing to steal**
  - One look multi-factor authentication
- **Privacy compliance**
  - GDPR compliant
  - Private by design
- **Ubiquitous experience**
  - Any platform, any device, anywhere
- **Easy to deploy**
  - Integrates with all identity providers

"The integration with LUISS and Keyless is a concrete example of the potential that can be unleashed when best available technologies come together. We’ve each approached this integration with openness, flexibility and safety in mind. In doing so, we’ve been able to ensure thousands of students can continue with their studies, pass their exams and graduate," said Agostino Santoni, CEO of Cisco Italy.

Keyless ZKB™: Zero-Knowledge Biometric Authentication
Passwordless MFA for Remote VPN Access

In response to COVID-19 lockdowns, a European digital bank partnered with Keyless to secure their remote workforce with seamless, secure remote access to VPNs and remote desktops.

- 1K Employees
- 2+K Auth/day
- <2 Sec/auth
- 1 Day deployment

Enhancing security and login experiences
- Anti-fraud protection
- Privacy compliance
- Easy to deploy

Reducing friction and increased productivity
- Nothing to remember
- Nothing to steal
- Ubiquitous experience

Rapid deployment and saved costs
- Eliminates phishing and man-in-the-middle
- GDPR compliant, private by design
- Integrates with all identity providers

Eliminating passwords in the financial sector
- Enhanced security and login experiences
- Reduced friction and increased productivity
- Rapid deployment and saved costs
Next-generation passwordless biometric authentication, on the edge.

Global telcos and Keyless are partnering to enable new digital experiences and enhanced security using 5G, mobile edge compute (MEC) and advanced privacy-enhancing technology.

- 28% Latency Reduction
- <0.3 Seconds per auth
- 11% Average speedup
- <2 Hour deployment

Enhanced user experiences, faster identification

- Enhanced security and login experiences
- Reduced friction and increased productivity
- Rapid deployment and saved costs

Nothing to remember
No central honeypot, no data on user device

Nothing to steal
One look multi-factor authentication

Privacy compliance
GDPR compliant, private by design

Ubiquitous experience
Any platform, any device, anywhere

Anti-fraud protection
Eliminates phishing and man-in-the-middle

Easy to deploy
Integrates with all identity providers

Rapid deployment and saved costs

Enhanced friction and increased productivity

Easy to deploy
Integrates with all identity providers

Rapid deployment and saved costs
Thank you!

🌐 https://keyless.io
✉️ info@keyless.io
🔗 @KeylessTech
Attractive Market Opportunity
- Clear paradigm shift to passwordless methods underway
- Large addressable market comprised of IAM, CIAM, SSI / PIM, all growing at 10%+ CAGR

Easy Deployment & Integration
- Seamless integration with existing systems
- Infrastructure agnostic – accessible through any platform and supporting SaaS, on-prem and cloud applications
- Requires minimal efforts from internal IT teams

Superior User Experience
- User-friendly, easy to use
- Nothing to remember - passwordless
- Enroll once, use everywhere through any channel and on any device

Cutting-Edge Technology
- Combines proprietary novel biometrics and advanced cryptography
- Universal biometric-key-management technology powering multiple use cases in zero-trust authentication
- Software only solution; true multi-device platform

Uncompromising Security
- Nothing to steal – no central honeypot, no data on user device
- Eliminates fraud, phishing and credential reuse
- Dynamic built-in MFA with just a look; authenticating the user, not the device

Privacy-Preserving
- GDPR, CCPA and PSD2 compliant
- Neither biometrics nor personal identifiable information are stored
- Enables selective disclosure of personal data in a private, secure manner

Overview

unique technology
Distributed cloud architecture

**Network**
Scalable dockerized multi-cloud setup without limitation (e.g., region, provider)

**Client**
Application can either be first- or third-party, depending on customer preference and use case, i.e. workforce vs. consumer authentication
breakthrough technology

Keyless Protocol: world’s first commercial implementation of MPC-based biometrics

A unique combination of multi-modal biometrics and privacy-enhancing technologies that offers secure, privacy-preserving biometric authentication, that exceeds regulatory requirements under GDPR/PDPA/CCPA

Breakthrough technology, multiple use cases

An AI-driven platform running on the user’s device extracts, encrypts, and splits the user’s biometric features into shares; following suite a distributed protocol reconstructs the irreversibly encrypted shares into cryptographic keys

- User’s device can then use these keys to generate tokens, sign documents, perform verifiable claims or securely authenticate the genuine user
- Combines inherence and possession factors to provide user-friendly, secure and universal multi-factor security

Unparalleled security and performance

- 300x faster than general purpose MPC (100ms instead of tens of seconds)
- Highly computationally effective (does not drain battery of end user devices)

Keyless Protocol
PCT/2020/017511
Cryptography

Novel cryptographic technique for securely and efficiently generating key material from multiple sources of entropy, including biometric signals

- Time- and energy-efficient privacy-preserving biometric authentication and key management via a unique cryptographic protocol
- Biometric Authenticated Key Exchange (BAKE)
- Method for securely and consistently generating high-entropy cryptographic keys from noisy low min-entropy signals using a trusted device and one or more semi-trusted servers

Core technology

New protocols for linking privacy-preserving distributed biometric authentication with legacy identity providers

- Method for separating data privacy domains in identity provider authentication flows

Keyless-enabled identity management

A fresh look at identity and password management, enabled by our groundbreaking cryptographic technology

- Vault-less password and identity manager
- Method for securely associating multiple devices to a single user account
from authentication
to the future of identity

**siloed**
- Users manage too many keys.
- Identity landscape is fragmented and concentrated in the hands of few.

**federated**
- For user-centric future, personal cryptographic keys need to be managed; but this is extremely complex.

**decentralized**
- Decentralized identity services enable people to self-provision and manage their own personal data and privacy in a virtual wallet using blockchain or another distributed ledger technology (Gartner).

**Keyless** enables users to control and selectively disclose their personal data in an intuitive, private and secure way.
authenticating people, not devices

When using device-native biometrics, the device is authenticated – not the user.

When device biometrics are used, the signing key is associated to the device rather than to the user. All enrolled users will authenticate using the same device key.

When Keyless is used, the signing key is generated directly from the user’s biometrics. Each enrolled user will authenticate only with her unique key, allowing the service to identify the user.
enroll once, use everywhere

Save on onboarding costs and user friction by ensuring users don’t go through a long, tedious onboarding process for each device.

1. User enrolls on her first device, after going through onboarding process. Her device is linked to her biometric template.

2. User adds her second device by scanning a QR code on her first device. Both devices are linked to the same template. No onboarding needed.

3. User can add and revoke devices from any of her linked devices – fully self service.
backup and recovery

Self-service identity recovery in case of a lost or stolen device without storing any biometric data.

1. User enables backup via the Keyless Authenticator app
2. User loses access to all his devices and acquires a new device and installs the Keyless app
3. User clicks “Restore from backup” instead of re-enrolling all over again
4. User authenticates to Keyless and to a 3rd party storage and backup is restored automatically by Keyless

How is backup stored?

Up to you.

- Keyless backup information can be stored either on the user's personal cloud storage account (iCloud/Gdrive) or on a Keyless hosted service.
- In both cases, no biometric data or PII is stored.
Keyless can fallback to leverage a time-based OTP which is generated by scanning a QR code via the Keyless Authenticator app.

1. User enables backup via the Windows desktop client

2. When no internet connection is available, the user selects the "offline login" option from the Windows lock screen

3. User scans the QR code presented on the desktop using his mobile app

4. User inserts the TOTP generated on his mobile device into the Windows lock screen

The Offline Access Mode can be activated by the user to perform a workstation login when there is no internet connection either on the workstation or the user's mobile device.