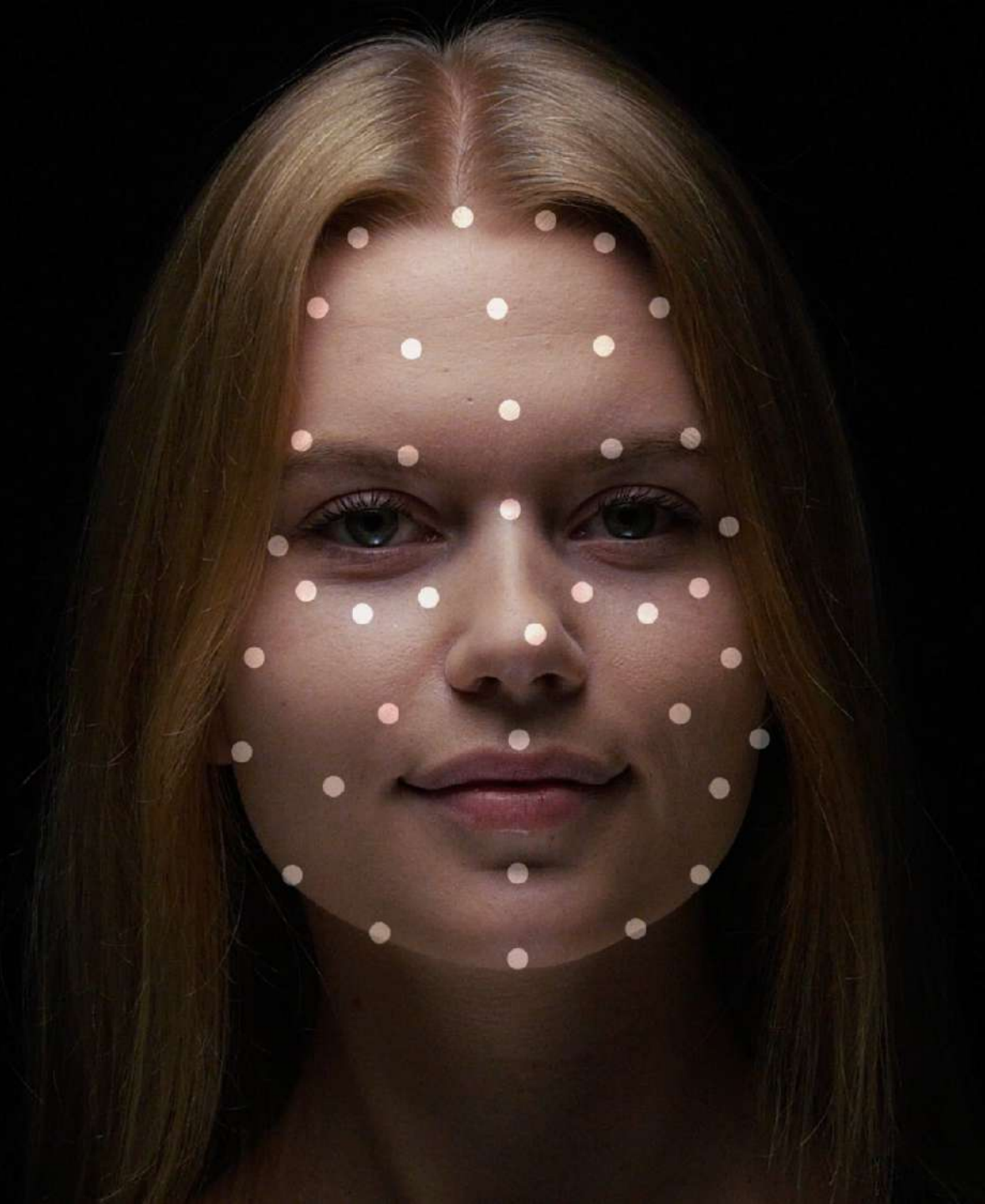


Passwordless is just the beginning. The future is Keyless

Adopt zero-trust authentication to protect your remote workforce and enable strong customer authentication with just a look.

KEYLESS



passwords are of the past

**Strong customer authentication
shouldn't compromise user experience**

55%+

of consumer banking traffic was
malicious logins in 2019

(Forrester Research)

94%

of breaches start with phishing
attacks targeting people

(Verizon Data Breach Report 2019)

\$ 14.7B

fraud incidents and losses with
mobile phone account takeovers

(Identity Fraud Study, Javelin 2019)

600%+

Increase in phishing attacks
during COVID-19 pandemic

(InfoSecurity Magazine 2019)



Shared secrets



Password reuse



Lost/stolen tokens



Keyloggers



Phishing

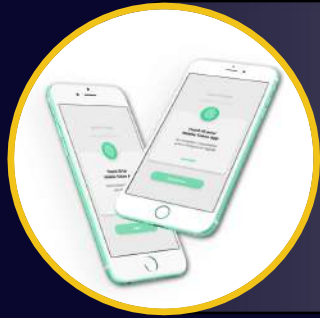


Credential stuffing

problem

limitations with authentication today

Existing biometric methods have fundamental limitations



Local Authentication



Microsoft



TRUSONA



okta

transmit
security



the growing legal and regulatory implications of collecting biometric data

Although biometric technologies make the authentication experience easier, the actual collection and storage of the data is presenting new security risks.

the Growing Biometric Recognition Technologies Threat To Privacy?

September 12, 2019

recognition have gone beyond Facial recognition technologies to lasers detecting and microbiome. Rapid technological innovation has also led to an increase in privacy regulations



Centralized Authentication

BIOCATCH
Less Friction. Less Fraud.



callsign

facetec

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.

Where GDPR goes next: digital privacy is taking over the world

on from the EU introducing its impact is

As biometric facial recognition technology spreads, privacy concerns follow

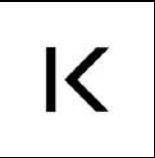
Jun 6, 2019 | Chris Burt

CATEGORIES Biometrics

With the introduction of new privacy laws on an almost monthly basis, struggling to understand how they are affected and if so, what the



Biometric facial recognition will soon play a major role in a range of activities from travel to shopping and buying fast food, according to a new CB Insights report describing the technology's use by more



unique capabilities powered by unique 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

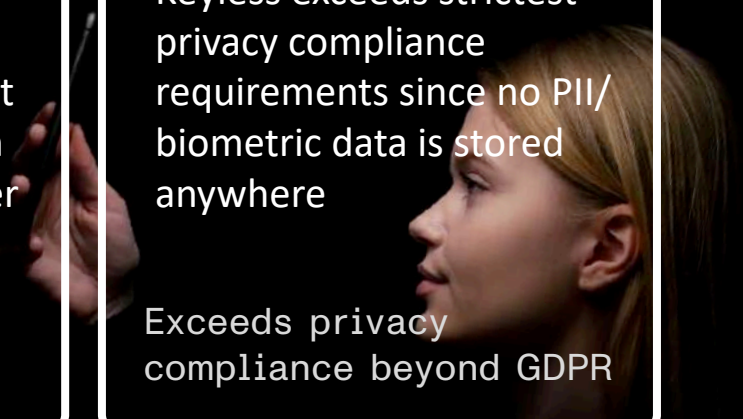
Unique identity for every user



No Biometrics/PII Stored Anywhere

Keyless exceeds strictest privacy compliance requirements since no PII/biometric data is stored anywhere

Exceeds privacy compliance beyond GDPR



unique technology

- 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

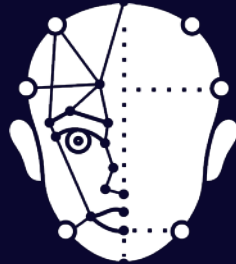
multi-factor by design

User-friendly visible protection

Invisible protection



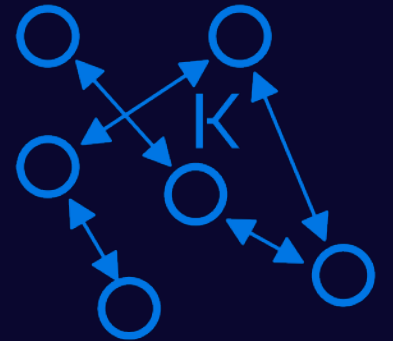
+



+



+



Privacy-preserving
device recognition (ZKP)

Zero-knowledge, AI-driven
physical and behavioral biometrics

Distributed private
computation (sMPC, SSS)

Use anywhere from any
device and any channel

Continuous and dynamic
multi-factor authentication

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

Factor agnostic, multiple
biometrics; private by design

PSD2 SCA done right

Embrace PSD2 compliant strong customer authentication to eliminate fraud, phishing and credential reuse while enhancing customer experience

➡ Nothing to remember

Streamline and unify the user experience across channels and devices

Multichannel biometric experience

- Unify the experience across devices
- Improve consumer experiences
- Reduce friction and MFA fatigue

🔒 Nothing to phish

Eliminate phishing and account takeover risk with interoperable, built-in MFA

Authenticate people, not devices

- Offer built-in anti-fraud protection
- Eliminate password-based attacks
- Reduce operational cost and risk

✅ PSD2 SCA compliant

Meet PSD2 SCA requirements with built-in MFA in just one look

SCA with just one look

- Eliminate the need to copy/paste OTPs
- Meet GDPR and PSD2 SCA requirements
- Build trust with your end users

🛡️ Easy to deploy

Lightening fast integration and deployment, on all platforms across all devices

Rapid time-to-value

- Integrate seamlessly in any native app
- Roll out across all devices and platforms
- Enroll once, use across all consumer touchpoints

Keyless Mobile SDK



Many use cases, easy to integrate



PSD2 SCA

Provide your customers with a unified experience with built-in MFA that eliminates fraud, phishing and credential reuse



Customer 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



Secure access to your applications with just a look

Customer MFA

Integrate superior passwordless security that authenticates people, not devices, in minutes - for all users, on any device.



Unified UX across all customer devices, hardware agnostic



Make sure the right person is authenticating by uniquely identifying your users

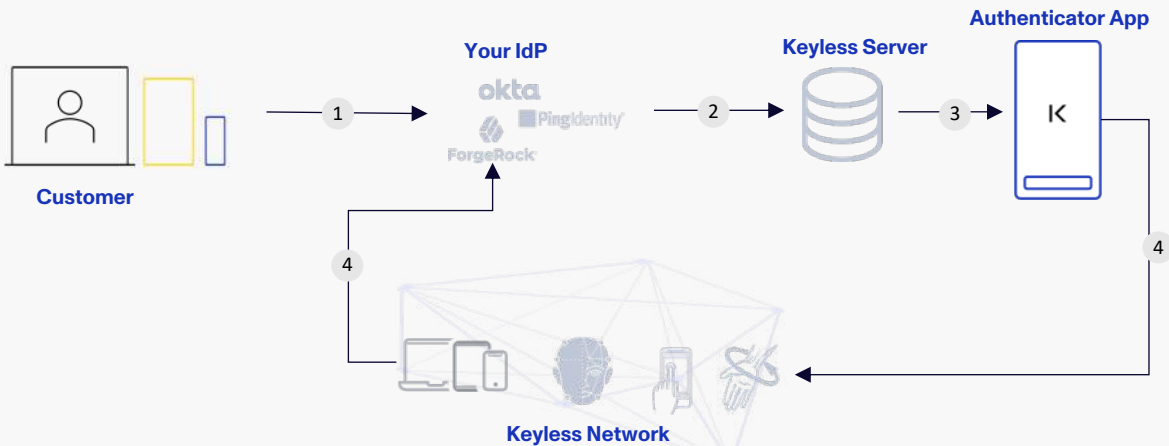


Minimize the risk of phishing, credential reuse and account takeover



Comply with GDPR by delivering biometric SCA without storing and processing PII data

Passwordless login for your customers



KEYLESS

Integrate with your existing identity provider:



PingIdentity

Okta



ForgeRock



Reduced IT time & costs



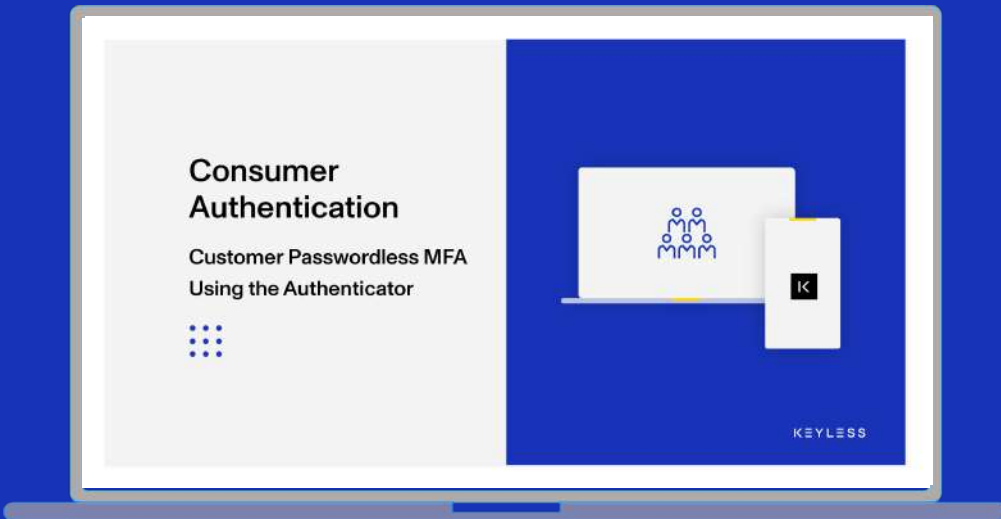
Rapid time-to-value



Better user experience



Strong security posture



\$ 4M is the average total cost of a data breach

(Ponemon Cost of Data Breach Report 2019)

Authorize payments with just one look

PSD2 SCA

Provide your customers with a unified experience with built-in MFA that eliminates fraud, phishing and credential reuse.



Frictionless authentication for your users with no reliance on Face ID or other hardware-based biometrics



Integrate seamlessly in your app in less than a day, with step-by-step documentation



Multiple devices, one identity – no need to re-enroll on every new device



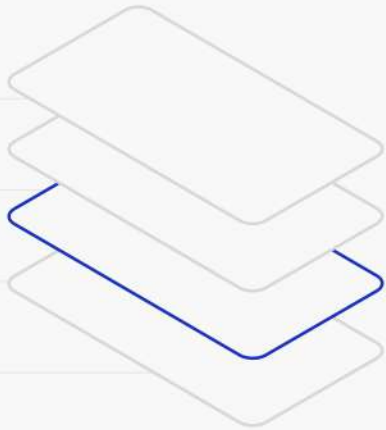
Comply with GDPR by delivering biometric SCA without storing and processing PII data

Your app

Your code

Keyless SDK

Your platform



Android



iOS



React Native



Reduced friction

Remove the authentication pain from your customers



Rapid time-to-value

Lightening fast integration and deployment, on all platforms



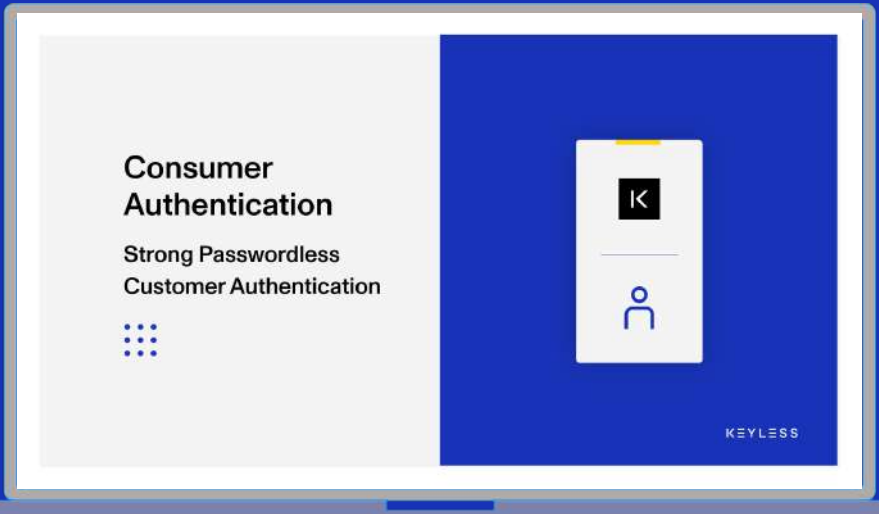
Better user experience

Customized UX for your app and users



SCA, PSD2 compliance

Eliminates risk by keeping your users' data secure and private by design



49% password-driven cart abandonment rate (Visa); and 51% of passwords are re-used across different services (University of Oxford)

the competitive edge



		 KEYLESS	 Hardware token	 Mobile Push	 OOB SMS or Email	 Server-side biometrics	 Local biometrics
UX	Any device w/ camera (HW/OS agnostic)	✓	✗	✓	✓	✓	✗
	Consistent experience across all devices	✓	✓	✓	✓	✗	✗
Security	Built-in MFA with just one look	✓	✗	✗	✗	✗	✓
	Spoofing-proof, phishing resistant	✓	✗	✗	✗	✗	✗
Compliance	Exceeds GDPR compliance	✓	✓	✓	✗	✗	✓
	No PII stored or processed anywhere	✓	✓	✓	✓	✗	✗
Costs	No password related support calls	✓	✗	✗	✗	✓	✓
	Easy integration and maintenance	✓	✗	✓	✓	✗	✗

case study



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

13+K

Students

6+K

Auth/day

2.2K

Virtual exams

10

Days to go-live



Keyless ZKB™ : Zero-Knowledge Biometric Authentication

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

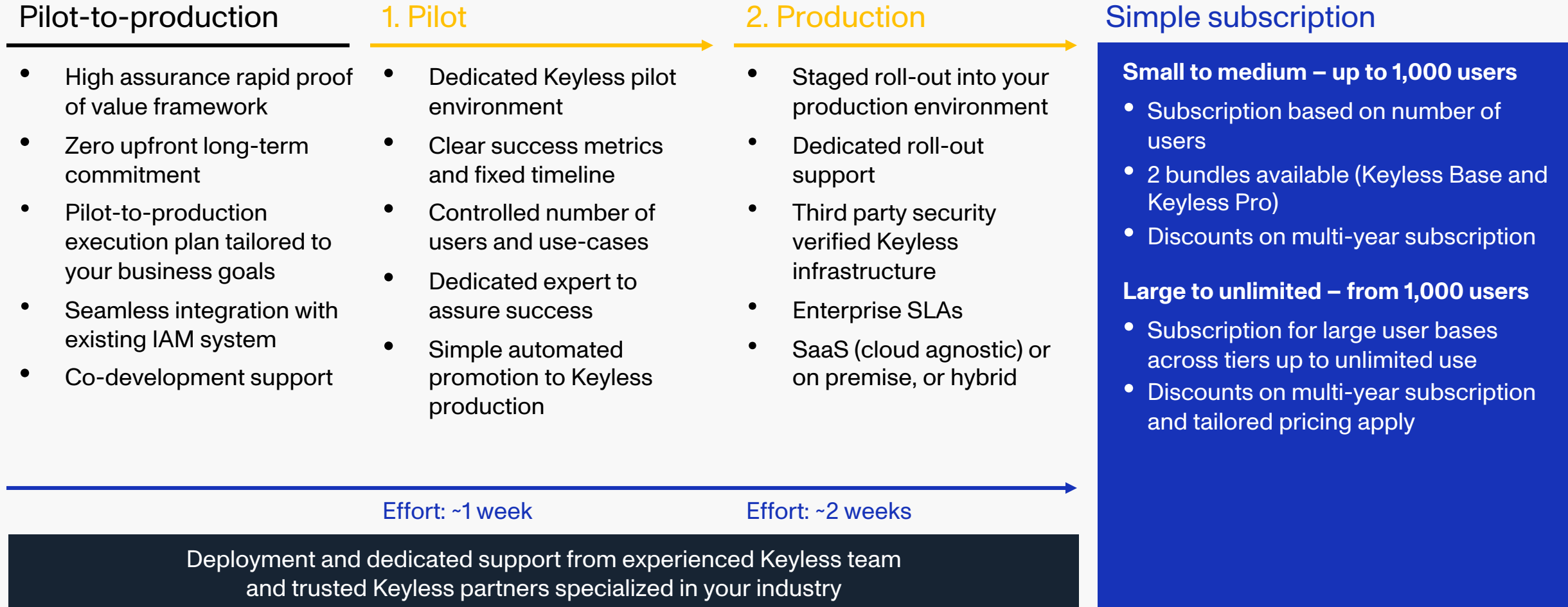
Privacy compliance
GDPR compliant,
private by design

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.

rapid proof of value

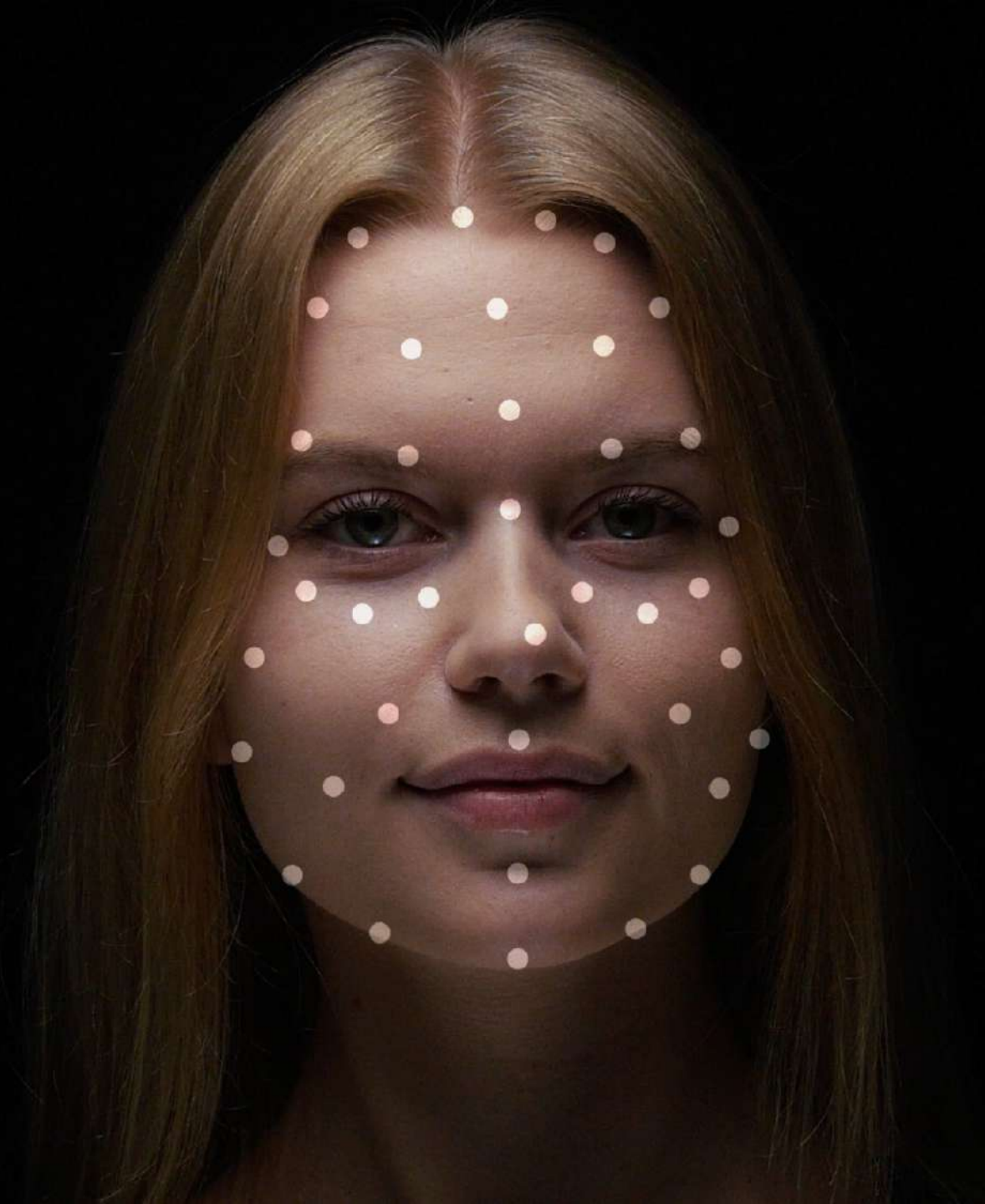


Thank you!

 <https://keyless.io>

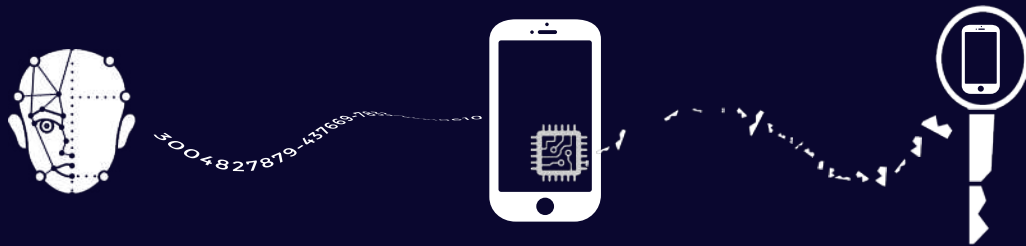
 info@keyless.io

 [@KeylessTech](#)



Authenticating people, not devices

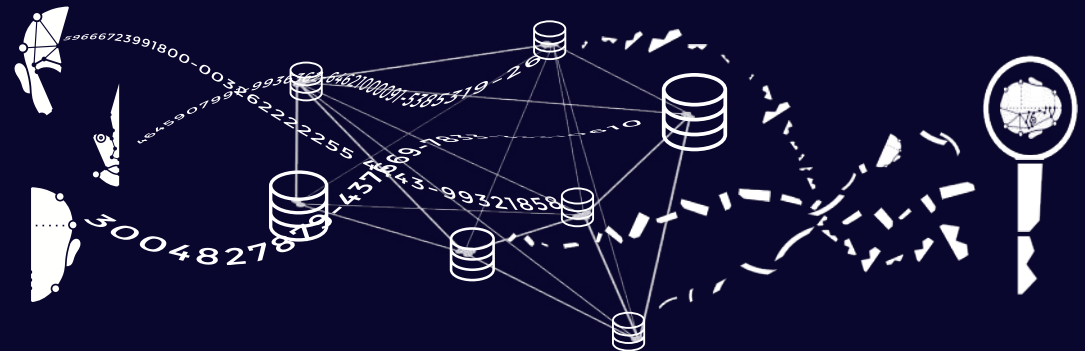
When using device-native biometrics, the device is authenticated – not the user.



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 his 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 his first device, after going through onboarding process. His device is linked to his biometric template.



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



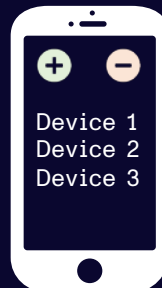
iPhone 7






Android 6



- 3 User can add and revoke devices from any of his linked devices – fully self service.



solving SCA challenges

For the Customer	 Zero-trust multi-factor security	With Keyless zero-knowledge distributed architecture, data can never be stolen or lost because no private information is accessible to anyone but the user; patent-pending secure multi-party computation and cryptographic mechanisms achieve MFA with just a look
	Built-in anti-fraud protection	Protect your customers from credential stuffing and phishing attacks; fraud-proof payments and secure user login with cryptographically signed transactions - eliminating the use of passwords and other shared secrets across mobile and web applications
	 Enhanced customer experience	Unify your authentication journeys across all customer touchpoints, on every channel and device ; there is nothing to remember, nothing to type, nothing to lose or to forget ; accelerate mobile adoption and transaction speeds
For the Bank	Easy to deploy	Leverage SCA in your application with one simple SDK ; deploy and operate Keyless Zero-Knowledge Biometrics (ZKB™) your way – on prem or as a service ; Keyless plugs into your current IAM using standard protocols or native plugins, and is compatible with all end user device types and platforms
	 Privacy compliance	Comply with GDPR even as privacy regulations change over time and across jurisdictions by delivering unified biometric SCA without storing and processing personal identifiable information

supporting materials (1/2)

Document

Link

Company presentation

[click here](#)

Product presentation

[click here](#)

One-pager - Workforce

[click here](#)

One-pager - Consumer

[click here](#)

Use case: Financial Services

[click here](#)

Use case: Keyless for PSD2

[click here](#)

Whitepaper

[click here](#)

Technology : How it works

[click here](#)

Videos

Link

Strong Customer Authentication

[click here](#)

Customer MFA

[click here](#)

Windows Login

[click here](#)

Windows Login - Workstation

[click here](#)

Workforce MFA

[click here](#)

VPN Authentication

[click here](#)

RDP Authentication

[click here](#)

VDI Authentication

[click here](#)

Demo - OKTA Integration

[click here](#)

Demo - ForgeRock Integration

[click here](#)

Demo - Auth0 Integration

[click here](#)

supporting materials (2/2)

Thought Leadership

- Why you must go passwordless
- Embracing user-friendly authentication as strong security in Europe
- Identity is the new perimeter — how can companies protect it?
- What is Strong Customer Authentication?
- How Keyless uses zero-knowledge proofs to protect your privacy
- Why legacy security models don't work?
- What is zero-trust security?
- The 10 most common cybersecurity threats

News and awards

- Official Partnership Microsoft Azure AD B2C
- Debut in Gartner's Hype Cycle for IAM
- Live with LUISS University and 10K students in partnership with Cisco
- #1 B2B Startup in South Europe (\$500K prize)
- #1 Biometric Authentication Solution in Banking Tech Awards
- #1 Startup in Italy - Telsy challenge
- #1 Startup in BNP Paribas challenge (€20K prize)
- #3 Startup in Slingshot 2020 Global (\$50K prize)
- #4 Top 7 Passwordless solution
- #Top 10 anti-phishing solution