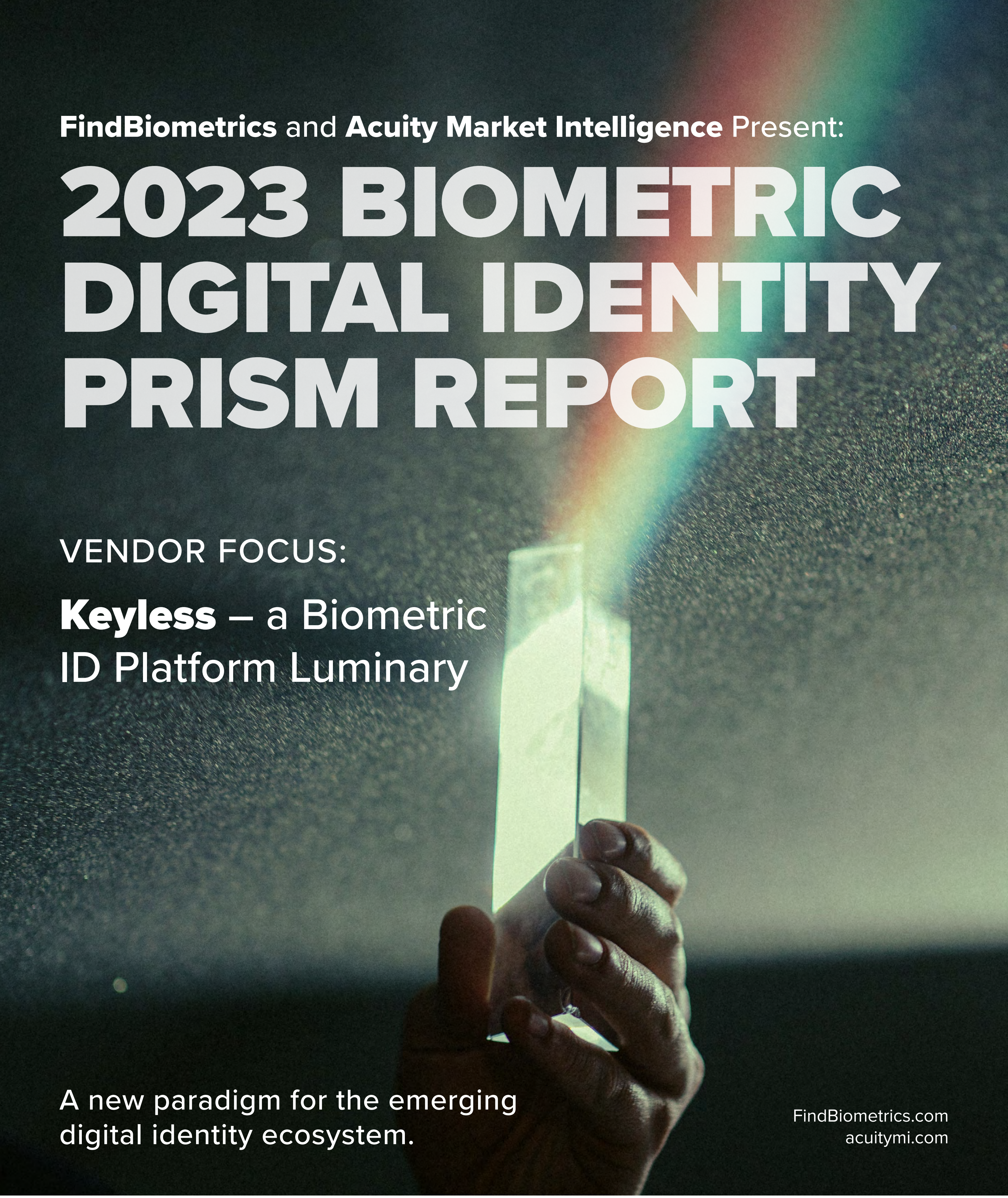


FindBiometrics and **Acuity Market Intelligence** Present:

2023 BIOMETRIC DIGITAL IDENTITY PRISM REPORT

VENDOR FOCUS:

Keyless – a Biometric ID Platform Luminary

A new paradigm for the emerging digital identity ecosystem.

FindBiometrics.com
acuitymi.com

FINDBIOMETRICS GLOBAL IDENTITY MANAGEMENT

ACUITY MARKET INTELLIGENCE

KEYLESS

Table of Contents

The Biometric Digital Identity Prism Report

Introduction

Biometric digital identity is no longer a novelty. As the mounting fraud crisis around the globe accelerates, users the world over are seeking to take control of their privacy, and public and private organizations are looking for security. Biometric digital identity has emerged as the only true solution to the problem of moving people across digital and physical spaces safely, securely, and intuitively.

Advances in biometric digital identity have evolved in parallel with Web3, artificial intelligence, mobile infrastructure, and data regulations. In the winter of 2023, FindBiometrics and Acuity Market Intelligence reframed the landscape. This innovative model reveals how technology vendors play an integral role in the converged physical digital identity ecosystem. The Biometric Digital Identity Prism was launched in September 2023 to wide acclaim.

But that was not the end of it. The Prism is an ongoing research program from FindBiometrics and Acuity Market Intelligence aimed at providing education and strategic guidance for influencers and decision makers seeking to understand, innovate, and implement digital identity technologies, across a wide range of vertical markets. The second phase of the Prism program includes supplemental reports on stand-out vendors, highlighting their role in the rapidly shifting identity ecosystem. Keyless, a Biometric ID Platform Luminary, is one of those select companies.

In this Vendor Focus Prism Report you will find:

- The core concepts shaping the future of biometric digital identity.
- An updated Biometric Digital Identity Prism landscape reference model.
- An assessment and profile of Biometric ID Platform Luminary Keyless.
- An interview with Fabian Eberle, COO & Co-founder, Keyless.

As industry advocates and evangelists of human identity, the authors of this report and its related supplements hope to level-up constructive and collaborative discussions among identity industry players and the relying parties with stakes in the growth of this industry. This Vendor Focus serves to continue that conversation in a time of accelerated industry development, providing an example of how an industry-leading platform provider is contributing to an identity-safe future.

The Biometric Digital Identity Prism Report is made possible through the participation of industry leaders like Keyless. If you would like to participate in the 2024 Biometric Digital Identity Prism, slated for release in Q2 2024, please contact the authors of this report and get involved with our research efforts.

Sincerely,
Report Authors

For inquiries about the use of this report, please contact editor@findbiometrics.com

Prism Identity Paradigm

The Biometric Digital Identity Prism is a living research project that is constantly adapting to developments in the ever-shifting market landscape. As vendors merge, acquire or develop new capabilities, grow, innovate, and deploy their technology, they move through the Prism. Companies may travel between beams and enter new classifications. New evaluation criteria will emerge, and new beams will be born.

But the Prism does have a foundation. Core concepts inform a philosophy of identity underlying our framework, motivating all of the dynamic elements at play. To understand the Prism, one must start with the following rhetoric.

Moving Beyond the Password Comparison

Biometrics are not analogous to passwords. Yes, password-replacement has long been the flagship mainstream use case for biometrics, but a shared application is not grounds to equate two fundamentally different ideas: knowable secret data and unique public physical traits. Biometrics are only similar to passwords in terms of what they attempt to achieve: restricting access to digital or physical assets to an individual user. That's where the similarities end.

Passwords are secret strings of data that can be used by anyone who knows them, guesses them, cracks them, or buys them. They can be forgotten. They can be reset. They can be phished. The integrity of a password-based system depends entirely on its secretive nature. By contrast, biometrics represent something public: you. Your fingerprint, iris, voice, and face are all unique parts of you that are used for identification online and offline by virtue of their plainly visible nature. When you phone a parent, you know them by the sound of their voice, not by the secret code you ask them for at the beginning of every call. Likewise, you know your coworkers by their faces, not a secret handshake.

And yet, the comparison between passwords and biometrics persists, encouraging a false dichotomy between security and identity. If we don't move away from this comparison, we are fated to build our biometric digital identity systems around leftover measurements and concepts from a bygone era of knowledge-based identity. We know KBA is failing us, and we have a better framework for identity. For that framework to succeed we need to ensure it is not simply built using the part of the old systems that failed us.

While a password is asking for a data-based key, biometrics aspire to something more organic: to bring the unique, irreplicable aspects of your physical identity into the digitized world, so that only you can access your accounts, credentials, finances, healthcare, and government services, as if the institution you interact with knows you like family.

The biometric digital identity industry has matured to the point where this ideal is within reach, so it is time to shed the password comparison and start embracing the powerful potential of digital ID.

Bringing Carbon-Based Life Forms into the Digital World

Biometrics – whether they are fingerprint, iris, face, voice, palm, or even your ear – represent the carbon-based lifeform at the end of a transaction. Anything else, be it passwords, security keys, one-time passcodes, or authenticator apps, simply prove a user has an authenticated device. And while sometimes it might feel like our phones are extensions of our bodies, a device is not your identity.

Detractors of biometric digital identity frequently attack the probabilistic nature of biometric matching. In a completely device-based system, you can have 100 percent assurance that all the doors are locked—a binary yes or no if a device or session is authentic. The issue, of course, is that fraud by its definition occurs within authenticated sessions. All the doors are properly secured, but a bad actor got the keys or learned the password. The security threat of identity is only addressed by solving for the carbon-based lifeform at the end of the transaction.

Bridging the gap between the carbon-based lifeform and their digital ecosystem can only be achieved through biometrics. This is why the Prism prioritizes biometrics at the core of identity platforms. Identity is a human trait, so digital identity must include the human element.

Government Systems of Record and Regulation Are Integral to ID Empowerment

From our current standpoint, the biometric digital identity industry is bringing us toward the reality of a privacy-enhancing, user-asserted, interoperable digital identity that empowers the user at its core. This is not a new idea—the early days of Web3 and blockchain technology gave rise to the idea of Self-Sovereign Identity (SSI). But many models of SSI lacked the core assurance of strong identity proofing during the onboarding process, a challenge that has been addressed by contemporary mobile ID programs which leverage government systems of record to anchor a user's biographical identity.

As the identity landscape evolves, and mobile/digital ID programs emerge in real world deployments—be they mobile drivers licenses in the United States, European eIDs, or national registries in Africa and South East Asia—it is becoming clear that a government system of record is a key building block for a fully realized biometric digital identity. And while this may run against the government agnostic philosophy of early SSI concepts, the end result—if supported by international standards and regulations—will be effectively similar: users will have control over their identity data, with the ability to assert the credentials they need on a transaction-by-transaction basis. But in this version of identity, relying parties will have the confidence of government identity at the root of every digital identity on their network, even in anonymous or pseudonymous transactions like age checks.

Taking Aim at Identity Excellence

Human identity is complex and so are our digital lives. That's why the biometric digital identity prism is divided into eight segments we call "Beams." Consistently, while conducting the evaluation on this report and taking a high-level view of the industry landscape, we have seen that the highest-performing vendors are those with well-defined target markets and use cases.

Something as fundamental as identity technology has a wide breadth of applications. A biometric digital identity solution can theoretically protect banks, optometry clinics, DMVs, chocolate stores, hotel rooms, and dating profiles. In the wake of the COVID-19 pandemic, a massive wave of biometric vendors flooded the identity and authentication markets to serve the urgent needs of remote work and digital transformation. Despite the plethora of potential customers in a range of industries, the most successful of these companies followed well-defined strategies laser focused on serving specific use cases in well-defined target markets.

The top performing Prism vendors have succeeded by understanding their key differentiators and being purposeful in what they do. Seeing beyond technology-driven responses to immediate needs, they recognize the opportunity that accelerated digital transformation in one facet of an organization can define, drive, and open doors for larger scale evolutionary change across the entire enterprise.

Understanding the Prism Framework

Just as a beam of light contains all colors, the biometric digital identity ecosystem is comprised of many vendors contributing to the grand idea of digital identity. FindBiometrics and Acuity Market Intelligence conceptualize this relationship through the Prism: a proprietary market landscape model intended to help reflect the components of the emerging reality of identity in a digitized world.

The Prism Framework is divided into Beams representing key segments of the biometric digital identity ecosystem. Each Beam is stratified into three classifications: Pulsar, Catalyst, and Luminary.

Biometric ID Platforms

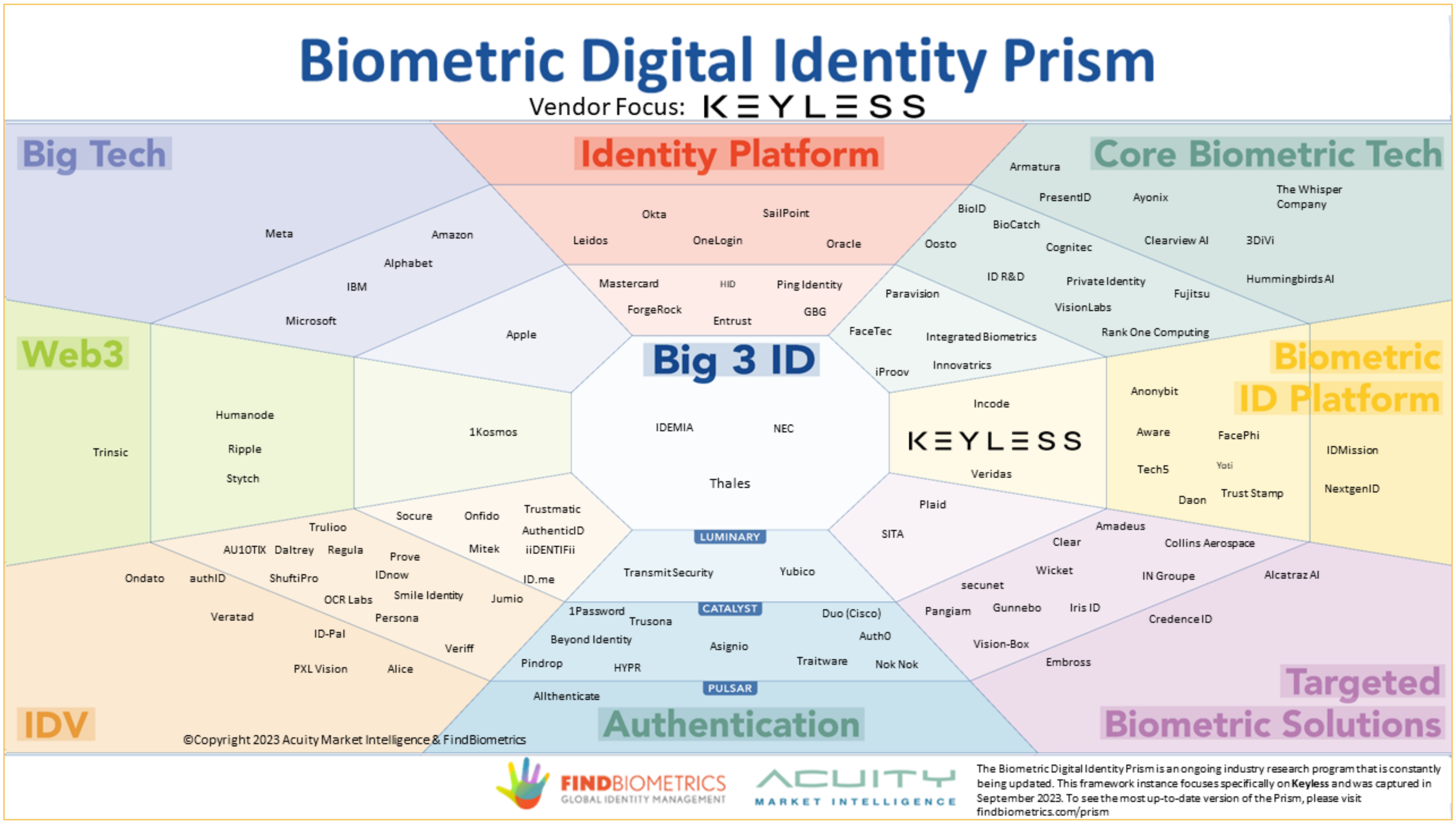
Biometric identity platforms provide secure, reliable biometric-based identity foundations on which full spectrum scalable, versatile, and end-to-end digital identity solutions can be built. Keyless operates within this Prism Beam with aplomb, providing identity orchestration with biometrics at the core, and offering advanced features like automated biometric account recovery.

Vendors in the Biometric ID Platform Beam are evaluated on a unique Prism XFactor: Solutions Expertise/Capability. Keyless rates high in this area, as a platform provider, demonstrating high performance across the identity journey it orchestrates.

Luminary

Luminaries like Keyless are the guiding lights of their industry segment. They show the highest level of proficiency in their beam and are often responsible for setting trends in their fields.

Keyless in the Prism



The Biometric Digital Identity Prism is an ongoing industry research program that is constantly being updated. This framework instance focuses specifically on **Keyless** and was captured in September 2023. To see the most up-to-date version of the Prism, please visit findbiometrics.com/prism

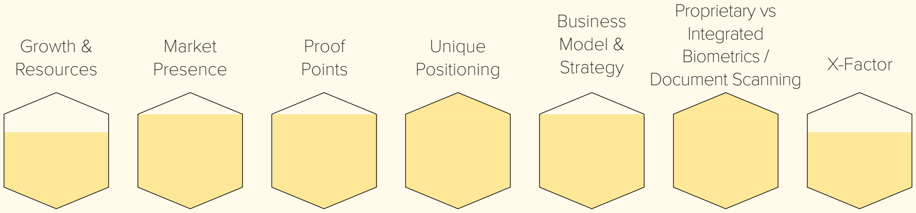
Important Note on Prism Beams:

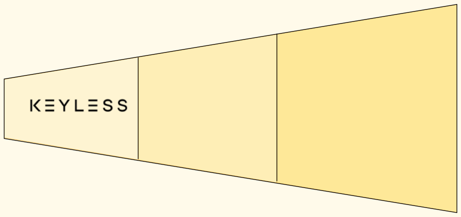
The Prism Beams and the classifications within represent important components of the emerging biometric digital identity landscape, and group vendors by the role they play therein. It is modality agnostic. Because of the broad nature of Prism Beams, many companies in the same areas are not direct competitors but represent the leading providers of their given solutions.

Keyless

keyless.io

BEAM: **Biometric ID Platform** / CLASSIFICATION: **Luminary**





Keyless is carrying the torch for platform-based biometric digital identity. This Prism Luminary extends the traditional security perimeter to include the end user with its proprietary cryptography and face biometrics technology. Frictionless experiences, strong security, regulatory compliance, and rapid ROI are major selling points for Keyless' biometric authentication platform—offered through flexible deployment models, including cloud-native, hybrid, and on-prem—and the company prides itself on meeting all global compliance and data sovereignty requirements, including GDPR and CCPA, and regulatory requirements such as PSD2 SCA, with certifications pertaining to FIDO Biometrics, FIDO2, information security management, quality management, and more. This all adds up to a strong biometric authentication platform ready to move organizations—particularly those in the financial sector—into an era that relies less on traditional (and phishable) keys like passwords, tokens, and magic links.

Leveraging True User Identity with Zero-Knowledge Biometrics

Keyless is not simply replacing passwords with biometrics—its MFA-by-design solution positions true user identity as the primary credential for all transactions. Capturing two authentication factors in one look, Keyless defends against deepfakes and spoof attacks. It's great for user experience, too. With a single selfie upon enrollment, a user can continue to authenticate and assert their identity through every interaction on a Keyless-protected service, across any device. This is all facilitated through the company's trademark and patented Zero-Knowledge Biometrics, a unique zero knowledge cloud computing model designed for privacy and compliance. With Keyless, biometrics are stored neither on devices nor in the cloud, simplifying compliance with data privacy regulations. Our researchers see this as a realization of a core concept of the Prism: that biometrics are not analogous to passwords.

Account Recovery in the Age of Automation

A persistent challenge for all post-password authentication systems is the account recovery step. When a user loses access to strong credentials, a system's weakness is revealed: many biometric authentication systems revert to a password or magic link for account recovery, making them as vulnerable as legacy systems, while solid device-based authenticator apps demand lengthy and costly call center processes that can take days. With Keyless, account recovery is a simple process that can get a verified user back on the platform as quickly as taking a selfie. As automated account recovery becomes an increasing priority for the identity ecosystem, Keyless is among the handful of vendors leading the way.

Fulfilling the Promise of Full-Lifecycle ID

User experience is a priority of Keyless, and that is on display with its various controls to reduce friction, even beyond the enrollment and login steps. Modeled after the mainstream IAM single sign-on experience, the company has integrated with risk platforms to enable step-up authentication when it is needed based on the weight of the transaction. In taking this approach, Keyless helps its partners move beyond a defensive stance that treats every user like a potential liability, enabling them to operate from a position of active customer satisfaction.

Contact Keyless: info@keyless.io

Interview with Fabian Eberle, COO & Co-founder, Keyless

What are some of the key decisions you made in the past five years that you attribute to your current leading position as a Biometric ID Platform Luminary?

Fabian Eberle, COO & Co-founder, Keyless: Some of the key decisions we took were to put user privacy first, authenticate the entire identity lifecycle, and focus on specific verticals. For reasons we will detail below, we have understood that there was a need for a system that could authenticate genuine users with high accuracy whilst still safeguarding their privacy. Keyless is the only biometric authentication platform that unifies authentication across the identity lifecycle whilst eliminating the risks that come with processing and storing biometric data.

We encrypt a user's biometric data before it leaves their device to remove any personal identifiers, or PII. This means that a user's data cannot be tied back to them if it is intercepted or stolen. In addition to the biometric, we also provide built-in, transparent device binding. We do this by cryptographically verifying the device leveraging zero-knowledge proofs, in tandem to the user's biometrics, providing two independent authentication challenges in one go (inherence + possession). We apply this methodology across the entire user journey. From enrollment and login to transaction signing, step-up actions, and account recovery, Keyless provides built-in multi-factor authentication with a single selfie, without exposing biometric data to anyone.

We also recognize the importance of trust and security in sectors with higher data privacy and security requirements such as the banking and wider financial services sector. As a result, Keyless was built to cater to these traditionally conservative sectors by protecting their accounts from fraud and help them comply with payment-specific regulations such as PSD2.

We've attained several key certifications that prove the value of what we've achieved so far. These include ISO27001 and ISO9001, as well as the unique combination of both FIDO2 and FIDO Biometrics certifications, of which we are the only company to achieve both. These accolades, alongside recognition from authoritative bodies like Gartner and KuppingerCole, combined with a host of industry awards, have helped bolster our standing as a trusted leader in the biometric ID domain.

Our approach to expansion has been equally deliberate. We've diversified our solutions to cover a broad spectrum of use cases, ensuring that our platform is versatile and adaptable. By forming strong partnerships with industry giants like Experian and Microsoft, among many others, we've amplified our capabilities and expanded our routes to market.

2023 saw a mainstream push to device-based identity mechanisms like Passkeys, which critics worry will funnel fraud toward vulnerable account recovery mechanisms. What is Keyless' approach to securing this part of the identity lifecycle?

Fabian Eberle, COO & Co-founder, Keyless: As the industry gravitates toward passkeys, which are tied to individual devices, businesses are encountering the challenge of verifying that passkeys are being used by the legitimate account creator. In short they don't prove genuine identity.

We offer an end-to-end multi-factor authentication solution that does prove identity across the entire lifecycle, from onboarding, login, transaction signing (PSD2/SCA), step-up actions, and crucially, account recovery. We are able to deliver lightning-fast, banking-grade identity assurance with an authentication time of 500 milliseconds, making it multiple times faster than conventional face-matching technologies.

Our integrated approach ensures that authentication remains consistent and secure, from the initial enrollment to the recovery stages. Our technology is device agnostic - an iPhone user can authenticate on an Android device - and encrypt biometric data so that we don't need to rely on the security of cloud servers.

In essence, we fill the gaps presented by passkeys by providing a robust, device-agnostic, and frictionless authentication technology that guarantees the integrity of the user's digital identity at every step of the user journey, including during critical recovery operations.

Keyless is uniquely flexible as a biometric ID platform when it comes to deployment options. What is the philosophy behind offering hybrid, cloud-native, and on-prem options to your customers?

Fabian Eberle, COO & Co-founder, Keyless: Our philosophy is centered on customer-centric flexibility. We recognize that our clients come from a myriad of backgrounds with distinct operational needs and security considerations. Whether they're leaning towards a hybrid, cloud-native, or an on-premise deployment, we're equipped to deliver. This flexibility underscores our commitment to tailor our solutions to each client's specific circumstances, ensuring we provide not just a one-size-fits-all product, but a secure, efficient, and bespoke platform that integrates seamlessly into their existing infrastructure.

Budget, privacy concerns, cybersecurity, internal resistance, and executive buy-in are the most imposing digitization obstacles cited in our survey data. How have you helped your customers to overcome implementation challenges and deploy biometric digital identity technology?

Fabian Eberle, COO & Co-founder, Keyless: To address these common challenges, we've made our biometric identity solutions exceptionally easy to integrate. Our technology is not only proprietary but also comes fully vetted and certified, which simplifies the adoption process for our customers. We offer seamless, plug-and-play integrations with a wide array of ecosystem players such as identity providers, core banking systems, and cybersecurity firms, among others. We further support any device that comes with a simple 720p camera, completely independent from any hardware manufacturer or operating system, unifying authentication experiences across the user base.

A key to overcoming budgetary constraints and internal resistance is demonstrating tangible ROI. Keyless eliminates costs associated with account recovery, fraud, SMS OTPs and password resets, whilst significantly improving the authentication experiences across the board. We deliver significant, tangible business value to our customers across the identity lifecycle, from seamless onboarding to instant and selfie-service account recovery.

Additionally, we tackle privacy and compliance concerns head-on, with our technology undergoing independent legal reviews to assure compliance with stringent data protection standards such as the GDPR and associated consent requirements. This commitment helps ease executive concerns and secures buy-in by aligning each business with necessary global data protection and sovereignty requirements.

Seeing Biometric ID Platforms in a New Light

Since the original publication of the 2023 Biometric Identity Prism Report, Keyless has succeeded in raising more funding, and announced its separation from former parent company Sift. Both the funding and the newfound independence are set to enable Keyless to advance its market strategy without compromise, targeting customers in the crucial banking and financial services sectors. In the words of CEO Andrea Carmignani, "Being independent allows us to better serve the needs of these markets."

Keyless' independence will enable it to make uncompromising decisions and act quickly as the biometric digital identity industry continues to rapidly evolve. As the Prism shifts to accurately represent the industry landscape, Keyless is positioned to remain a vendor of note.

About the Authors

Maxine Most

Internationally recognized biometrics and digital identity thought leader celebrated for provocative market insights, accurate market predictions and forecasts, and unbiased, pragmatic market intelligence. Tenacious strategic marketer with a prolific career hallmarked by success designing and executing ground-breaking strategies for technology innovators and leaders.

Maxine Most (@cmaxmost) is the founding Principal of Acuity Market Intelligence (www.acuity-mi.com), a strategic consultancy recognized as the definitive authority on global biometrics market development. Throughout her 30-year career, Ms. Most has evangelized emerging technology on five continents. Since 2001, she has focused on biometric and digital identity markets where she has earned a stellar reputation for innovative thought leadership and a proven ability to accurately anticipate biometric and digital identity market trends.

As an executive strategist, Most has provided expertise in emerging markets such as biometrics, authentication, and digital identity, e-commerce, interactive services, and 2D and 3D visualization and image processing. She has worked with startups, established technology market leaders, Global 1000's, and a range of organizations in between. Most leverages her deep understanding of technology evolution, emerging market development, and the process through which industry leaders are created to provide candid strategic analysis, highly targeted implementation plans, and quantifiable, measurable results.

Ms. Most is the author of numerous biometric and digital identity research reports including Face Verification & Liveness for Remote Digital Onboarding," "The Global Automated Border Control Industry Report: Airport eGates & Kiosks," "The Global Biometrics and Mobility Report: The Convergence of Commerce and Privacy," "The Global National eID Industry Report," "The Global ePassport and eVisa Industry Report," and "The Future of Biometrics," as well as a contributor to several books including "Digital Identity Management" edited by digital identity thought leader David G. Birch.

Ms. Most regularly offers insight and analysis in on and off-line publications, is quoted often in industry, business, and consumer press, and presents regularly at industry events on the evolution and development of biometrics and digital identity markets. She is a graduate of the University of California, San Diego with a multi-disciplinary degree in Mathematics and Computer Science and minors in Visual Arts and Economics.

Peter Counter

Peter Counter writes about technology and culture. As Editor in Chief of FindBiometrics and Mobile ID World he brings a multitude of technology writing experience, having covered industry news and written features on topics as diverse as dark fiber, call center solutions, satellite technologies, robotics, Augmented Reality, Internet of Things, telematics, IPTV, healthcare tech, and gaming. With a decade of biometrics and identity industry experience, Peter has been a four-time judge for the prestigious GSMA Global Mobile (GLOMO) Awards and is the host of the ID Talk Podcast.

Counter hosts the FindBiometrics Virtual Identity Summits – a series of full-day online events, presented quarterly, designed to educate and motivate vertical market decision makers on their path to stronger identity practices. With a strong focus on ethics and privacy, the Virtual Identity Summits spearhead FindBiometrics' mission of connecting digital identity leaders with their future strategic partners.

As the head of FindBiometrics' Research Team, Counter has provided guidance, strategy, and communications expertise to the world's leading digital identity and biometrics companies operating in financial services, government, healthcare, and travel vertical markets.

Alex Perala

Alex Perala is a writer and journalist covering biometrics, cybersecurity, and artificial intelligence. He is the author of FindBiometrics' daily ID Tech newsletter and weekly AI Update. He can be found on X at @alex_perala, and on Substack at @alexperala.

The Future is Prismatic...

Let Acuity Market Intelligence and FindBiometrics be your guiding light!

Contact info:

Maxine Most
Principal Researcher, Acuity Market Intelligence
cmaxmost@acuity-mi.com

Peter Counter
Ambassador & Editor in Chief, FindBiometrics
pcounter@findbiometrics.com

Lisa Sherman
Sales Executive, FindBiometrics
lisa@channelpronetwork.com

Dan Krippner
Sales Executive, FindBiometrics
dan@channelpronetwork.com

About FindBiometrics:

FindBiometrics is your leading industry resource for all information on biometric identification and identity verification systems and solutions. We have the latest daily news from the global biometrics and identity management business community, a comprehensive vendor list, informative articles, interviews with industry leaders, exclusive videos, links to biometric associations and a calendar for the most important and current industry events and conferences.

http://www.FindBiometrics.com

FindBiometrics is part of the ChannelPro Network, a division of EH Media LLC, a leading U.S. business-to-business media company and conference producer. http://www.ChannelProNetwork.com

About Acuity Market Intelligence:

With decade of practical expertise in the unpredictable and volatile world of emerging technology, Acuity Market Intelligence consistently delivers consistently original, thought-provoking, and reliable insight and analysis. Proud, self-proclaimed technology business development and marketing geeks, Acuity is globally renowned for its uniquely customized business and marketing strategies and for creating and deploying innovative programs that integrate digital and traditional channels and platforms.

Visit acuitymi.com and let us help your organization thrive.