BIOMETRIC DIGITAL IDENTITY PRIVACY AND COMPLIANCE PRISM REPORT

2025

A new paradigm for the emerging digital identity ecosystem.

the-prism-project.com

THE PRISM PROJECT

ACUITY MARKET INTELLIGENCE

Thank You to Our Sponsors and Partners

The Privacy and Compliance Prism Report is made possible thanks to the participation of our sponsors and partners. The biometric digital identity ecosystem depends on collaboration, and we are grateful to work with the following organizations.

SPONSORS

Anonybit
Daon
OVD KINEGRAM a KURZ company
Mitek
kantara INITIATIVE
fido ALLIANCE
European Association for Biometrics eab Human Identity in Europe
SECURE TECHNOLOGY ALLIANCE
AWARE
alcatraz
iddataweb
iiDENTIFii
KEYLESS
ZEROBIOMETRICS
PARAVISION
Corsound AI Voice Intelligence Technologies
ideem
IDEMIA
DUCK DUCK GOOSE
AUTHENTICID
ID R&D a Mitek company
wicket
PANINI
iProov

PARTNERS

IDENTITYWEEK GLOBAL • TRUSTED • VISIONARY
ID TECH
KYC AML GUIDE
PEAK iDV

The Prism is proudly independent. While participants benefit from increased visibility and vendor profiles in this report, sponsorship does not affect a vendor's evaluation of placement within any aspect of the Prism Project.

©Acuity Market Intelligence 2025: All rights reserved. www.acuitymi.com. The material contained within this document was created by and is protected under copyright by Acuity MI, LLC. The Author and Publisher do not guarantee the views, opinions, or forecasts contained herein. Non-sponsor vendors are not guaranteed inclusion. Sponsors are guaranteed inclusion but sponsorship has no impact on vendor evaluations and assessments. No part of this report including analysis, charts, forecasts, text extracts, quotes, nor the report in its entirety may be reproduced for any reason without explicit consent of Acuity Market Intelligence.

Table of Contents

Prism Ver. 1.0 © 2025 The Prism Project

Prism Ver. 1.0 © 2025 The Prism Project

Introduction

Welcome to the Biometric Digital Identity Privacy and Compliance Prism report. This is the seventh report from The Prism Project—a research, analysis, and market education initiative created by Acuity Market Intelligence to bridge the gap between the identity technology intelligentsia and the enterprise professionals evaluating and deploying digital identity solutions to meet the challenges of digital transformation.

Utilizing a holistic framework informed by hundreds of organizations and relying party evaluations, The Prism Project is grounded in a philosophy of identity, based on four key pillars:

- Digital identity belongs to the person it describes.
- True identity empowerment relies on government systems of record.
- Identity must be consistently and continuously orchestrated in both physical and online channels to remain secure.
- Biometrics must be at the core of any sustainable, reliable, and secure digital ecosystem, and be implemented with the understanding that identity flows freely between converging virtual and physical worlds.

This report drills down into two critical challenges facing every organization and user in our modern digital world: privacy and compliance. Through its 2024 analysis of biometric digital identity in financial services, government services, and travel and hospitality, as well as its June 2025 deep dive analysis of deepfake and synthetic identity threats, The Prism Project observed this common vulnerability. As relying parties across all market sectors achieve new levels of digitization, identity elements describing the humans interacting with various online entities—including biometrics, Personally Identifiable Information (PII), and contextual data—are at risk of exposure to malicious actors. Once exposed, these identity elements can be used to commit identity theft, to mint synthetic identities, to carry out fraud, and to gain wrongful access to restricted spaces online and in the physical world.

The first Prism report of 2025—the Deepfake and Synthetic Identity Prism Report—identified and categorized the most advanced forms of identity fraud threats, powered by AI. The report diagrammed the anatomy of a single digital identity in

The Prism Project would like to acknowledge the work of individuals and organizations for their contributions to the analysis in this report. The IDV process diagram, in particular, builds on work by the Kantara Initiative Deepfake-IDV Discussion Group—including specific contributions by Joey Pritikin of Paravision, independent consultant Mike Chaudoin, Daniel Bachenheimer of Accenture, and Acuity Market Intelligence's Maxine Most—as well as presentation attack points in biometric systems as included in ISO/IEC 30107-1:2016, and industry research by Stephanie Schuckers at CITeR.

Prism Ver. 1.0 © 2025 The Prism Project

relation to the processes it undergoes for verification, authentication, and account recovery—categorizing each identity element and placing it within the larger context of the various transactions it enables, as well as the data required every step of the way. This report leverages those diagrams, focusing on the identity elements themselves, what can be done to protect them at each step in the process, and how they can be safely managed throughout the entire identity lifecycle.

The core idea proposed in this report supports the larger mission of The Prism Project: to empower public and private sector influencers and decision-makers by providing the information and analysis they need to effectively evaluate and deploy digital identity technology and solutions. With the Privacy and Compliance Prism Report, we further this mission by presenting a privacy-first vision of the biometric digital identity ecosystem. A vision that can facilitate constructive engagement among all parties about how identity data should be collected and used in all identity transactions, from opening a bank account to entering a physical data center. The ultimate goal is to foster a culture of trust built on a shared understanding of inclusive human identity in the digital age.

In this report, you will find:

- A beginner's crash course in biometric digital identity that:
    - Introduces key concepts and definitions
    - Provides a synopsis of recent critical market dynamics and regulatory evolutions
    - Equips you with the foundation for understanding how privacy and compliance factor into the identity ecosystem
- An inventory of identity elements commonly used in digital identity transactions, categorized according to how they affect user privacy, and described using plain language and easy-to-read diagrams.
- A regulatory map, highlighting key privacy laws and trends around the globe.
- A breakdown of common challenges facing the relying parties that must handle these identity elements, examined by representative markets and through the proprietary Prism Lens model.
- A privacy and compliance-focused version of the proprietary Biometric Digital Identity Prism market landscape model.
- Evaluations of vendors, relying parties, and infrastructure

Download the 2024 Prism Reports:

BIOMETRIC DIGITAL IDENTITY TRAVEL AND HOSPITALITY PRISM REPORT
2024

organizations contributing to the collective effort to protect user privacy and ensure future-proof compliance.

- Profiles of significant players that prioritize user privacy and enshrine secure digital identity in their technology and solution offerings.

While it does build on the foundational market knowledge set out in previous Prism Reports, the Privacy and Compliance Prism Report can stand on its own as an independent resource. For further reading and context on the core philosophy that underpins this publication, we recommend that you supplement it with our 2024 Flagship Report and the 2025 Deepfake and Synthetic Identity Prism Report. Looking ahead, The Prism Project will publish our annual comprehensive industry update, the 2025 Flagship Prism Report, in Q4 of this year.

As ever, my collaborators and I are evangelists of strong identity and believe that the only way to move forward in our time of digital transformation is to take the ethics of human identity seriously in both the physical and digital realms. As a community, we believe the identity industry and its stakeholders are morally tasked with developing and implementing powerful digital technologies for the good of humanity. By reading and sharing our vision of a secure and convenient future of user-powered identity that ensures privacy and compliance, you are participating in the positive change required to close identity gaps. Together, we can usher in an identity-safe future for all.

Authentically yours,

Maxine Most

Founder
The Prism Project

Download the 2025 Deepfake and Synthetic Identity Prism Report:

BIOMETRIC DIGITAL IDENTITY DEEPFAKE AND SYNTHETIC IDENTITY PRISM REPORT
2025

A new paradigm for the emerging digital identity ecosystem.

How to Read This Prism Report

The Privacy and Compliance Prism Report is divided into seven sections:

Crash Course

The report opens with a crash course on the identity arms race, designed to bring you up to speed on the past decade and a half of innovation and evolution in biometric digital identity, with a focus on how we arrived at the current moment of vulnerable identity elements and compromised user privacy. As key terms are introduced, they are defined in the sidebar. **The crash course sets the stage for the privacy and compliance opportunity overview.**

Privacy and Compliance Opportunity Overview

Using plain language and supported by intuitive diagrams, the second section of this report classifies and categorizes the various identity elements collected and processed in digital transactions of all kinds. These transactions are placed in the context of the Prism Project's Identity Hierarchy, helping contextualize the relationship between human identity and data privacy. An inventory of privacy-enhancing solutions and fraud countermeasures is explored and presented in a holistic context to illustrate the multilayered approach required to protect identity elements in a world where digital identities and digital identity ecosystems are increasingly becoming entwined with critical physical and digital infrastructure. **The Opportunity Overview provides the core ideas and lexicon for understanding privacy and compliance in biometric digital identity.**

The Prism Lens (Challenges and Solutions)

The third section of this report draws from Prism Project research into digital transformation trends. The Prism Lens is a holistic visualization of the key strategic challenges relying parties face, in this case, relative to privacy and compliance. Each of these eight strategic challenges are defined, then and individually analyzed from the perspective of how biometric-centric digital identity solutions can address them. **The pain points highlighted in the Prism Lens serve as the basis for the practical applications of biometric digital identity highlighted**

Prism Ver. 1.0 © 2025 The Prism Project

later in the report.

Vertical Market Breakdown

To illustrate the real-world scope of privacy and compliance opportunities, the fourth section of this report applies the challenges identified in the Prism Lens to specific representative markets. **The Vertical Market Breakdown lays the final groundwork for the evaluations in the rest of the report.**

The Prism

The fifth section is the proprietary biometric digital identity industry ecosystem framework: the Prism. This version of the Prism ecosystem is fine-tuned to show how various biometric digital identity parties collaborate with relying parties and infrastructure players to enhance privacy and ensure compliance. **The Prism is a living research program, providing a framework for understanding how these digital identity players work together to fight fraud, improve user experience, and empower people in an era where compromised privacy has become routine.**

Evaluations and Profiles

The sixth section lists the organizations depicted in the Prism framework next to their evaluations. Each organization is evaluated in context—based on their capabilities, accomplishments, and market aspirations—and grouped according to their primary contribution to the biometric digital identity ecosystem. These organization categories of the Prism framework are called Prism Beams. After each set of evaluations, profiles are presented to demonstrate how the solutions offered by sponsors of this report can address the challenges defined in the Prism Lens and Vertical Market Breakdown sections. (While many organizations can and do operate across multiple Prism Beams, for the purpose of creating an ecosystem model, each is assigned a primary position within the Prism framework. Sponsor profiles include visualizations called Luminosity Graphs that illustrate their true multibeam positioning.) **The evaluations and profiles provide insight into how organizations across the Prism landscape operate within the biometric digital identity ecosystem.**

The Prismatic Future of Identity

The seventh and final section of this report contains strategic guidance and recommendations based on this report's research. It also includes author information, an overview of the Prism Project, and information on how to get involved in

Prism Ver. 1.0 © 2025 The Prism Project

future Prism reports. The conclusion lights your way to the next steps on your digital identity roadmap.

Each section of this report stands on its own, but taken together, the end-to-end report provides a unique, comprehensive view of the current state of an industry-wide initiative to protect user privacy while enabling human identity-powered transactions in an increasingly digital world.

Crash Course: The Evolution of Modern Identity Privacy

To understand how privacy and compliance are integrally linked to **digital identity transactions** and the users initiating them, it's essential to have a basic understanding of how **biometrics** entered the mainstream and impacted the evolution of **personally identifiable information (PII).** It's a fascinating portrait of a rapidly evolving technology whose adoption far outpaced corresponding policy and regulation, and how consumer education and end-user perception can both fuel technological misconceptions and inform emerging frameworks. From a consumer mass adoption standpoint, the story begins in 2013, when biometrics became a consumer product, laying the foundation for biological human identity to become a critical component of digital transactions.

This crash course is designed to familiarize the uninitiated with key digital identity definitions and concepts, contextualize them within the past decade of widespread digital transformation, and demonstrate how concepts of privacy have evolved in tandem with regulatory developments.

The Basic Idea Behind Biometrics and Digital Identity

In digital spaces, we don't have bodies, so our interactions are enabled or limited based on the **identity elements** we provide at the time of a transaction to prove we are who we claim to be. This same essential dynamic is at play during in-person transactions facilitated by digital technology. There are three types of identity elements we can provide to corroborate our identity claim: something we know **(knowledge-based authentication (KBA))** or personal identifiable information (PII), something we have token or **device-based authentication (DBA)**, a key, or a physical ID), and something we are (biometrics).

Knowledge-based authentication is the most commonly used authentication factor, but it can be guessed, shared, stolen, forgotten, or cracked. Token or device-based authentication is analogous to a traditional physical key. These factors can't be cracked or guessed, but they may be shared, lost, damaged, or stolen. Biometrics, however, stand apart as a stronger level of

Key Definitions:

DIGITAL IDENTITY TRANSACTION: An interaction, either online or in a physical space, that requires specific permissions related to an individual's identity. The scope of these transactions is broad-reaching and includes accessing email, making online purchases, verifying your age in person or online, and accessing secure physical spaces.

BIOMETRICS: Technology that uses some kind of sensor (camera, microphone, fingerprint reader, etc.) to measure or capture an image of a user's unique biological trait—most commonly a face, voice, fingerprint, or iris—and represent it via an algorithm as a **biometric template** for the purposes of identification, authentication, or security.

BIOMETRIC TEMPLATE: An algorithmic representation of a captured biological trait, stored as a mathematical value that cannot be reverse engineered to recreate a representation of the original biological trait.

PERSONALLY IDENTIFIABLE INFORMATION (PII): Data that describes foundational, biographical, and contextual details about an individual—from date and place of birth, to social security number, to address history, and more. PII linked to biometrics creates the foundation for digital identity.

IDENTITY ELEMENT: A component part of identity. In this report, an identity element refers to a biometric, a document, or metadata. An identity element can be authentic or counterfeit.

KNOWLEDGE-BASED AUTHENTICATION (KBA): A form of identity security based on knowable information. Common examples are passwords, PINs, and SMS codes.

TOKEN OR DEVICE-BASED AUTHENTICATION (DBA): A form of identity security that depends on physical possession. Common examples are keys, key cards, FOBs, USB security keys, cryptographic keys, virtual tokens, and mobile devices like smartphones when used for authentication.

Prism Ver. 1.0 © 2025 The Prism Project

assurance.

Biometrics have long represented the pinnacle of identity elements because your actual face, fingerprint, or voice cannot be shared, stolen, lost, forgotten, or easily guessed. This is a game-changing development in the rapidly converging world of digital identity transactions, spanning both physical and online spaces.

By incorporating biological identity elements into the non-corporeal interactions of online life, digital transactions approach the levels of trust we enjoy in the physical world. Things that used to require in-person interactions and painstaking identity checks, like opening a bank account or renewing a driver's license, can be performed remotely when the **relying party** (a bank or DMV in this case) can trust that a user whose biometrics match the ones associated with their digital identity is authentically themselves. This is in contrast to a person with a password or a hardware token, who can only prove they know something secret or possess something special, rather than proving they are a specific, unique human. In short, biometrics give you a body in digital spaces.

Meanwhile, physical interactions benefit from a similar boost in assurance and convenience. Unmonitored in-person transactions, such as entering a controlled workspace or a high-security restricted area, can also be secured when an individual's biometrics are verified in real-time. Whether the biometric is matched against a centralized server, locally on a door-mounted access control device, or on a personal device presented to a reader for verification, biometrics prove that the right individual at the right time with the right permission is granted physical access to restricted spaces.

To see how biometrics make this possible, and the ways in which it impacts privacy, it's essential to understand the three phases of the biometrics lifecycle:

- Enrollment: A new user submits their biometrics for the first time, creating a biometric template that will be used as the comparison for future authentication transactions. Enrollment can be strengthened with the addition of other identity elements, such as data from government-issued IDs, in a process known as i**dentity verification (IDV)**.
- Authentication: An enrolled user submits their biometrics for the purposes of matching with a template. The user's biometrics are compared to the template, and a positive match results in an authenticated transaction.

RELYING PARTY: An organization that drives end-user adoption by leveraging identity technology to improve and automate security, operations, and/or customer experience.

IDENTITY VERIFICATION (IDV): A class of identity technology that compares a user's face biometrics to the image on an identity card or credential (usually government-issued) and/or a database that stores the content of the government-issued credential, to prove a user is who they claim to be. This enables **biometric binding** as well as compliance with **Know Your Customer (KYC)** and **Anti-Money Laundering (AML)** regulations, and is most commonly used for remote onboarding and account opening applications.

KNOW YOUR CUSTOMER (KYC): A set of global guidelines and regulations for the mandatory process of identifying and verifying the identity of a client when opening an account and throughout the customer lifecycle.

ANTI-MONEY LAUNDERING (AML): A set of global laws requiring that regulated entities implement measures to detect and prevent suspicious financial activities.

BIOMETRIC BINDING: The act of connecting live-captured biometric data to trusted personal information on a trusted identity credential to verify user identity.

- Account Recovery: A user who has lost access to an account or privilege engages with a relying party or device to regain access. This can take many forms, ranging from recovery codes and call center interactions to in-person recovery processes or fully automated smartphone transactions, providing varying levels of assurance.

As you can imagine, biometrics represent a significant step-up in trust and assurance when it comes to linking a person to their accounts, transactions, and privileges. Biometrics were the missing piece when it came to connecting various identity elements back to the carbon-based lifeform they describe. And, the more identity elements linked to the biological factor that verifies the individual, the greater the level of trust and assurance. Digital identities became more powerful as a result, and in turn, this increased the value of identity elements, not just for relying parties and their customers or users, but to marketers, researchers, governments, and, of course, bad actors.

The core conflict between accurately describing a physical human being in a digital space and outside parties that seek to collect the identity elements of consumers, citizens, business contacts, in both legal and illegal contexts, has brought forth a decade and a half of regulatory evolution, ethical debate, education, and technological innovation. This period is still underway, but new developments in mobile IDs, data encryption, **liveness** detection, and identity element storage are bringing all the players within and dependent on the identity community closer to an agreement on how best to empower end-users with privacy-enhancing identity technologies. And just in time—with the emergence of synthetic identities and deepfake technologies that trade in **counterfeit identity elements** and threaten to destabilize the very foundation of digital identity, enshrining user privacy is essential if we are to realize the promise of digital transformation.

LIVENESS: The quality of authenticity in a biometric. The term is most commonly used in the context of liveness detection software, which is a support technology designed to detect and prevent **presentation attacks** by verifying a live human being is present at the time the biometric is captured. More recently, liveness has been applied to identity documents as well to ensure they are not digital replicas of authentic or counterfeit documents.

PRESENTATION ATTACK: The act of presenting **counterfeit identity elements** to a sensor in an attempt to trigger a false positive signal, enabling a fraudster to wrongfully authenticate a transaction.

COUNTERFEIT IDENTITY ELEMENTS: Biometrics, documents, and metadata that have been created or modified—by digital or physical means—by a bad actor for the purposes of deception or fraud. This includes (but is not limited to) deepfakes, fake IDs, and misleading or altered metadata.

The Mobile Revolution – Apple Launches Touch ID

Before 2013, online security was primarily confined to knowledge-based authentication (KBA) methods, such as passwords, PINs, and one-time passcodes. In high security scenarios, KBAs could be supplemented by physical tokens—something you have, like a card or FOB. This limited application security because things you know and things you have can be shared, stolen, lost, damaged, or forgotten. The use of a passcode or physical key did not prove that the human being using them to assert a privilege (logging into an online account, authorizing a payment, opening a door, etc.) was the actual human entitled to that privilege. If a password was compromised, or a token or card key was stolen, then whoever had the authenticator also had the privileges it granted.

That began to change in 2013, when—after many years of innovation in mobile technology and experimentation with biometric sensor technology—Apple launched the iPhone 5S, which featured Touch ID: a fingerprint sensor embedded in its home button. It wasn't the first biometric sensor on a mobile phone, but it was the first that was widely adopted, the "killer application" that introduced a third concept to consumer authentication: something you are.

Apple's embrace of fingerprint-based screen unlock popularized biometrics as a convenient way to open a phone, putting fingerprint sensors on the radar of the average smartphone user. Samsung and LG followed course, and within a year, fingerprints were being touted as a password replacement. Software-based face and voice biometrics began to emerge, too, and we started to see a wild west of biometric authentication factors arise.

These were relatively primitive biometrics, however, and severely limited in scope.

The Device Vs. Server Debate

The privacy conversation around the mobile revolution was initially characterized by two privacy philosophies: **on-device biometrics** and **server-side biometrics**. The debate boiled down to this:

- One side argued that because biometric data is uniquely valuable, access to that data should be severely limited; therefore, it should remain only on the **secure element** of the user's device to whom it belongs. All biometric matching should be on-device only.
- The other side argued that without connection to a **system of record** outside the transacting device, a biometric was insufficient for proving identity.

In short, the most privacy-enhancing option—on-device only—lacked sufficient identity elements to form a digital identity, while the more versatile solution for digital identity—centralized server-based—was considered too insecure. This debate raged on for the better part of a decade, but as technologies evolved alongside our understanding of what data is required for a trusted

ON-DEVICE BIOMETRICS: Biometric authentication solutions in which enrolled identity elements are stored and matched in a secure element and never leave the smartphone, computer, or smart card they're on.

SERVER-SIDE BIOMETRICS: Biometric authentication and verification solutions in which enrolled identity elements are stored and matched on a centralized server. This requires secure transmission of biometric data between the sensor and the server.

SECURE ELEMENT: A cloistered part of a mobile device or computer system that applications or network features cannot access.

SYSTEM OF RECORD: A database of foundational identity elements maintained by a trusted organizational body, like a government or educational institution.

identity transaction, a hybrid paradigm emerged that enabled a decentralized approach to biometric processing, with assurance provided by a system of record. This approach would eventually become central to the next-generation mobile IDs of the 2020s, discussed in the privacy solutions section of this report.

NSA's Prism Program

The privacy debate around consumer biometrics coincided with one of the first modern digital privacy scares, when Edward Snowden leaked information on the NSA's PRISM initiative (no relation). PRISM was a top-secret program ostensibly set up to collect data for national defense purposes. Snowden's leak exposed highly invasive data capture and sharing of US citizens' PII. While this had no direct relation to consumer biometrics, the high-profile nature of the PRISM leak, combined with the timing and novelty of technologies like Touch ID, created a flashpoint of paranoia and misconception. Thanks to the participation of tier 1 American technology and telecommunications companies in the NSA's program, a public fear of biometrics being stolen from iPhones marred the excitement of smartphone-based biometrics, even though Touch ID, the most popular consumer biometrics at the time, was on-device only.

While fears that the NSA was harvesting biometric data were based on a misconception, the related privacy concerns over the collection and storage of biometric data were valid. This validation came in the form of a 2015 data breach at the US Office of Personnel Management (OPM), which resulted in the compromise of 5.6 million fingerprint records stolen by hackers. These records included a slew of other identity elements, including social security numbers, names, addresses, health, and financial data. At the time, mainstream media focused on the irrevocability of biometric data, noting that fingerprint images cannot be reset. Identity industry leaders were quick to highlight that the OPM had violated the most basic principles of secure data storage, as the data was unencrypted and fingerprint images, not biometric templates, had been stored. While also emphasizing the need for multifactor authentication, including increasing reliance on biometric verification.

The End of Security

The OPM breach was the canary in the coal mine. In 2017, Yahoo! reported a massive data breach—the largest in history at the time—which affected all three billion user accounts. Biographical, contextual, and transactional identity elements, including usernames, emails, encrypted passwords, and birthdates, as well as account recovery information like security questions and backup email addresses, were all exposed. The fallout resulted in monetary damages of $350 million, sounding the alarm on the nature of user identity data: identity elements are valuable, sought after by bad actors, and inadequately protected.

In the following years, data breaches continued to be reported worldwide. Equifax suffered a breach in 2017, impacting approximately 148 million US citizens, exposing data like Social Security Numbers. A year later, India's national ID program, Aadhaar, was exposed by a security researcher, potentially compromising the biographical and biometric data of over 1.1 billion people. In 2019, Facebook and Capital One each suffered a breach. Then at the dawn of this current decade, LinkedIn, Syniverse, Epic Games, Ticketmaster, and the Shanghai Police all followed suit with significant data breaches of their own.

The result was a perforated security landscape in which user data could not be considered secure. The companies that suffered these incursions took hits to their reputations and their bottom lines, but many of the end users whose data was compromised were impacted far more gravely. The Identity Theft Resource Center (ITRC), which tracks the business and consumer impact of identity theft enabled by data breaches, reports that many victims of identity theft consider suicide.

Strong authentication methods like biometrics began to be adopted to prevent these types of incidents. However, the ongoing widespread use and trust in more sophisticated and resilient identity technology require a concerted effort to strengthen user privacy alongside access control.

Right in the Face

Fast-forward to 2020, and enterprise **digital transformation** received a massive Black Swan inspired boost due to the COVID-19-driven need for remote authentication. The global shutdown of in-person commerce led to an explosion of biometric binding use cases, spawning an unprecedented outpouring of biometric identity innovation. Established identity players that had previously limited their offerings to traditional KBA and DBA authentication, along with established biometrics players, and a surge of hungry start-ups, offered biometric-based solutions to this new identity verification challenge of conducting public and private sector business remotely online.

DIGITAL TRANSFORMATION: The organizational process of integrating digital technologies and procedures into daily operations to increase efficiency, enhance accessibility, and boost customer experience.

While these solutions varied in terms of capabilities, user experi-

Prism Ver. 1.0 © 2025 The Prism Project

ence, deployment complexity, and several other factors, they all shared a similar approach to verifying an individual's identity through biometrics. They combined biometric face capture, most often via a smartphone, and matching technology (sometimes on device and sometimes on a server) with **optical character recognition (OCR)** and **computer vision,** enabling software to compare a human face to the picture on an individual's existing government-issued identity document, including passports, national IDs, and driver's licenses.

The addition of documents into the identity equation introduced another trusted human element, enhancing security in the digital space. But, along with the increased collection of identity elements, there was a growing need to protect them as the pace of data breaches accelerated. And soon, there would be consequences for those who failed to take this task seriously.

OPTICAL CHARACTER RECOGNITION (OCR): A class of computer vision technology that enables the reading of text on documents via a connected camera on a smartphone or computer.

COMPUTER VISION: A class of artificial intelligence that emulates object recognition through connected cameras.

The Mother or Regulations

Parallel to the mobile revolution and the tidal wave of data breaches in the mid-to-late 2010s, the European Union was developing a regulation to protect citizens' data. The **General Data Protection Regulation (GDPR)** was in draft form as consumer biometrics began to gain traction in 2013. By May 2018, the regulation had become legally binding in the EU, meaning that any company worldwide handling data of a European Union resident was required to comply with its standards, which remain among the strictest on the planet to this day.

Under the GDPR, individuals residing in the European Union benefit from clearly defined data privacy rights, while relying parties that collect, process, store, and manage user data must adhere to key principles. Individuals must give explicit consent before their data is processed. Once it is, they have the right to easily access, edit, and transfer that data, or even have it erased under the regulation's "right to be forgotten." Relying parties, meanwhile, need to be transparent, legitimate, accurate, and accountable in their data management, lest they be subject to GDPR's penalties for non-compliance: up to 20 million Euros or 4% of global annual revenue (whichever is greater).

It was the law that signalled the rewriting of millions of privacy policies, and while it caused no shortage of headaches in terms of organizational change, the GDPR stands as the example of how to communicate the importance of protecting privacy.

GENERAL DATA PROTECTION REGULATION (GDPR): A European privacy law that came into effect in 2018, granting citizens rights over their personal data. The strict nature of GDPR and its focus on empowering end-users have been a strong foundational influence on similar consumer data protection and privacy laws around the world.

Prism Ver. 1.0 © 2025 The Prism Project

The American Privacy Acts

In the United States, where GDPR effects relying parties but does little to protect end users, two privacy acts with very sharp teeth picked up the slack. Illinois' **Biometric Information Privacy Act (BIPA)** predates the mobile revolution by five years, making it a sleeping giant as fingerprint and face recognition gained traction in security, access control, time and attendance, and surveillance applications. The law demands consent for every instance of biometric collection and disclosure, specifying why it is needed and for how long. The penalties have proven an existential threat to companies that run afoul of BIPA, with individuals able to recover $1000 in damages for negligent violations and $5,000 for reckless violations. The fines were originally per instance, so in cases where employees used biometrics multiple times a day, or had their faces scanned regularly, the ticket multiplied at a frightening rate. In 2024, the law was revised to allow repeated collections of the same biometrics to be counted as a single offense, thereby reducing the potential for massive fines.

BIOMETRIC INFORMATION PRIVACY ACT (BIPA): A 2008 Illinois privacy law concerning the collection of biometric data. Infamous for its heavy penalties, BIPA has led to landmark settlements in the wake of the mobile revolution, as biometrics have become increasingly ubiquitous.

While BIPA is a state-level law, it represents a landmark piece of legislation that, while a thorn in the side of companies that like to play fast and loose with compliance, further illustrates the importance of protecting identity elements like biometrics.

In California, a broader privacy act took effect on January 1, 2020. The California Consumer Privacy Act (CCPA) is the most significant privacy law in the United States and has served as the model for other legislation throughout the country. As essentially the American counterpart to GDPR, the California law empowers end users with rights regarding the transparent collection of their data and the ability to opt out of data sharing, limit its collection, and even have it deleted.

CALIFORNIA CONSUMER PRIVACY ACT (CCPA): One of the first successful privacy laws modeled after GDPR. Like its European counterpart, CCPA formalizes end users' rights to own, control, and delete their personal data.

Children of GDPR

Over the past five years, the rest of the world has followed the example of the European Union and California, enacting GDPR-inspired regulations. Many of these children of GDPR are in regions characterized by high levels of digital identity technology in their private and public sectors. In Brazil, where biometric digital identity technologies are used for shopping, banking, and pension collection, the LGPD (General Personal Data Protection Law) came into effect in 2021. Meanwhile, India, which boasts the most expansive biometric national ID program on the planet — the Aadhaar (Unique Identification Authority of India) —is building a legal framework for personal data protection in a similar vein. The UK is also making headway in its own post-Brexit priva-

Prism Ver. 1.0 © 2025 The Prism Project

cy legislation.

Forty-six out of 54 countries in Africa have a form of legislation governing privacy, many following the key ideas set forth in GDPR. The Asia Pacific region has diverse privacy laws, with Japan and Singapore showing clear signs of inspiration from EU law, and China making significant strides in enabling data sovereignty. Indeed, with privacy laws on every continent either in effect or undergoing rapid development, it's clear that compliance with data protection is no longer optional. The time for racing ahead of regulation in the name of profit and innovation is over. It's time to protect privacy and achieve compliance, or face the penalties.

Next Generation of Privacy

So, we know the situation: personal data, especially identity elements, are valuable and vulnerable. Lawmakers from around the globe have recognized this and, following in the footsteps of the European Union, have established regulations to protect user privacy and limit data exploitation by third parties, whether malicious actors, unscrupulous corporate entities, or even public organizations that are lax in their oversight. We need technologies that enable compliance and protect privacy, while still enabling the convenience and automation promised by digital transformation. Thankfully, the leaders in biometric digital identity have been working tirelessly to create innovative solutions that put users in control of their identity elements in ways that are naturally compliant with privacy laws in digital and physical contexts.

From **mobile IDs and mobile driver's licenses (mDLs)** to innovative encryption and storage solutions, like those offered by Privacy Paragon Anonybit, to widely available **passkeys**, to digitally signed biometric barcodes and on-demand, ephemeral biometrics—biometric digital identity solutions have continued to evolve. And while the regulations may change, the core concepts of privacy and identity remain the same. With the alignment on display from the global privacy community, relying parties seeking solutions for identity data protection will be best served by vendors that prioritize the protection of user data.

MOBILE ID/ MOBILE DRIVER'S LICENSE (MDL): A digital credential securely stored on a smartphone. The best mobile IDs and mDLs are validated against a government system of record, allowing users to control which identity elements they share on a transaction-by-transaction basis.

PASSKEY: a passwordless credential based on standards set forth by the FIDO Alliance. Passkeys allow users to sign in to apps and websites using device unlock mechanisms on their computers and smartphones. Because they are device-based, passkeys are privacy-by-design.

Where We Are Now

This brings us to our current moment in biometric digital identity, where relying parties are seeking solutions to help secure and protect identity in their digitally transformed businesses. And those solutions need to be compliant and privacy-first, not only because regulations demand it, but because, as we will see in this report, digital identity only works if bad actors can't hijack the identity elements that belong to the users.

The Privacy and Compliance Prism World Map

The Privacy and Compliance Prism World Map provides a high-level view of the current state of privacy and compliance laws and regulations worldwide. This snapshot of a rapidly evolving regulatory ecosystem provides an initial reference for deeper exploration and analysis.

The map is illustrative rather than exhaustive and doesn't highlight globally accepted standards like KYC and AML. Instead, it provides an introductory overview of the global privacy and compliance landscape.

North America

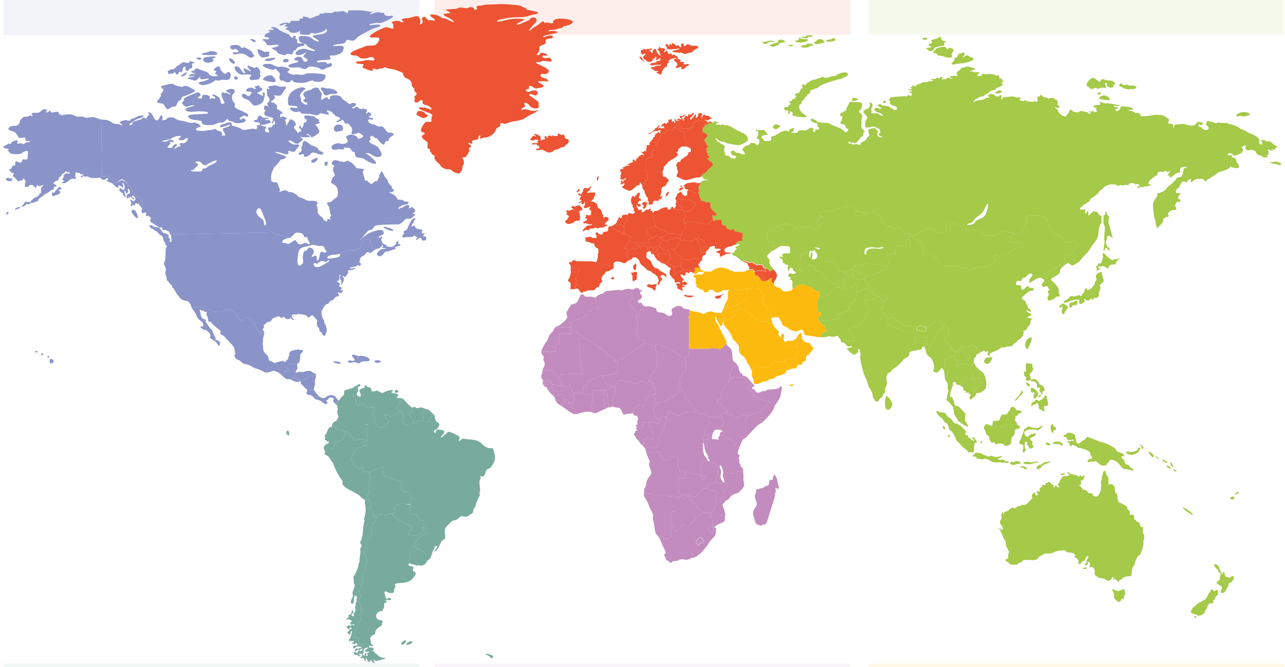
North America has a fragmented data privacy landscape that shifts across its constituent countries and states. This patchwork has evolved from various regional and sector-specific regulations that, in recent years, have been aligning more closely with GDPR.

Europe and the UK

Europe is the center of data regulations thanks to its landmark GDPR law, which has inspired nearly every other framework on the map. In the post-Brexit era, the United Kingdom was left to establish its own privacy law, aptly titled UK GDPR.

APAC

Many countries in the Asia Pacific region have enacted comprehensive data laws, as others update their existing legislation to meet the growing international consensus of how identity elements should be protected.



Latin America & South America

Many Latin American and South American countries have data protection laws that were either inspired by GDPR or predate the landmark regulation and are being updated to include provisions for newer requirements. Many countries are working towards regulatory harmony to ensure consistent requirements across regions.

Africa

Over 75% of countries in Africa have some kind of data protection law, and this number is rising. Marked by an emphasis on transparency, fairness, and data minimization, as well as end-user data rights, the data privacy laws in Africa face regional challenges, including resource constraints for enforcement. However, the growing ubiquity of these regulatory frameworks demonstrates the significant global impact the GDPR has had.

Middle East

Many Middle Eastern Countries have enacted GDPR inspired regulations that prioritize informed consent, data minimization, and security.

Prism Ver. 1.0 © 2025 The Prism Project

North America

North America has a fragmented data privacy landscape that shifts across its constituent countries and states. This patchwork has evolved from various regional and sector-specific regulations that, in recent years, have been aligning more closely with GDPR.

- United States
  - CCPA - The most prominent American privacy act, often compared to GDPR, California's regulation serves as the model for other states.
  - BIPA -An Illinois biometric privacy act that prioritizes user consent.
  - HIPAA - A data privacy regulation for patient health data with strict requirements on security, transferability, and end-user accessibility.
- Canada - PIPEDA - Designed to protect individuals' privacy, this national-level privacy act allows for "implied" consent, making it less privacy-forward than GDPR. It is superseded by provincial variants in Quebec, British Columbia, and Alberta.
- Mexico - LFPDPPP- A new law effective as of March 21, 2025, with provisions for consent and data protection. This law is similar to GDPR, but its definitions have their own regional nuances.

Latin America & South America

Many Latin American and South American countries have data protection laws that were either inspired by GDPR or predate the landmark regulation and are being updated to include provisions for newer requirements. Many countries are working towards regulatory harmony to ensure consistent requirements across regions.

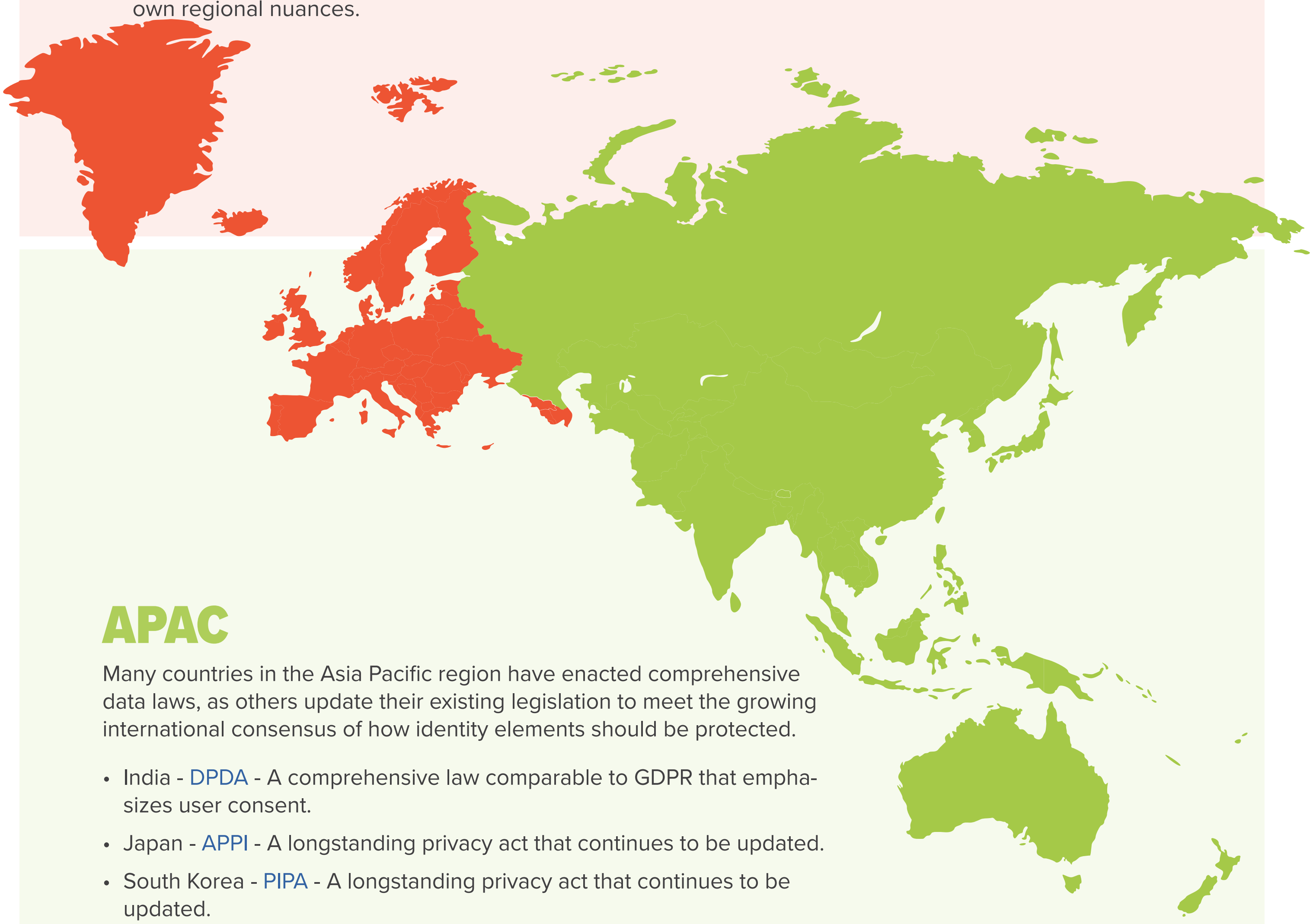
- Brazil - LGPD - a GDPR-inspired data protection regulation.
- Colombia - Law 1581 - a broad data privacy law that protects user data rights to privacy and rectification under the country's constitution.
- Chile - LPPD - a relatively new data protection law enacted in 2024.
- Uruguay - LPPD 2008 data protection framework - a legacy law for which updates are currently being considered.

Prism Ver. 1.0 © 2025 The Prism Project

Europe and the UK

Europe is the center of data regulations thanks to its landmark GDPR law, which has inspired nearly every other framework on the map. In the post-Brexit era, the United Kingdom was left to establish its own law, aptly titled: UK GDPR.

- European Union:
  - GDPR - The mother of all data protection regulations, this law prioritizes user consent and control over personal data, including identity elements.
  - EUDI - This regulation establishes a framework for EU-wide accepted digital identity wallets that put users in control of their identity elements. EU member states are required to provide access to the EUDI wallet by the end of 2026.
- United Kingdom: UK GDPR - A post-Brexit privacy regulation modeled after GDPR but with its own regional nuances.



APAC

Many countries in the Asia Pacific region have enacted comprehensive data laws, as others update their existing legislation to meet the growing international consensus of how identity elements should be protected.

- India - DPDA - A comprehensive law comparable to GDPR that emphasizes user consent.
- Japan - APPI - A longstanding privacy act that continues to be updated.
- South Korea - PIPA - A longstanding privacy act that continues to be updated.
- Singapore - PDPA - A 13 year old privacy law, recently update in 2020, which recognizes consent.
- China - PIPL - A comprehensive law comparable to GDPR with strict data processing and transfer rules.
- Australia - Privacy Act of 1988 - Based on 13 Privacy Principles that govern the collection, use, and disclosure of PII.

Middle East

Many Middle Eastern Countries have enacted GDPR inspired regulations that prioritize informed consent, data minimization, and security.

- UAE - Federal Decree Law No. 45 of 2021- a comprehensive regulation that specifically aims to align with international standards like GDPR.
- Saudi Arabia - PDPL - a newly enacted law modeled after GDPR.
- Jordan - JPDPA - a newly enacted law modeled after GDPR.
- Qatar - PDPL - a decade-old law that has evolved to include contemporary data protection provisions.

Africa

Over 75% of the countries in Africa have some kind of data protection law, and this number is rising. Marked by an emphasis on transparency, fairness, and data minimization, as well as end user data rights, the data privacy laws in Africa face regional challenges including resource constrains for enforcement. But the growing ubiquity shows just how much of a global impact GDPR has had.

- South Africa: POPIA - A data protection law governing the conditions for processing personal information, prioritizing consent and an individual's control of their data. It was amended in 2025 to further strengthen privacy protections.
- Nigeria: NDPA - A comprehensive law, enacted in 2023, modeled after GDPR, but with stricter rules for child consent and more lenient penalties.
- African Union: Convention on Cyber Security and Personal Data Protection - A 2014 treaty adopted to establish a framework across Africa for electronic transactions, data protection, cybersecurity, and cybercrime prevention. It is signed and pending ratification by many AU members, and is not yet a universally binding law.

Privacy and Compliance Challenge Overview

Privacy Versus Compliance

At the heart of the conversation about privacy and compliance are the questions: what is a digital identity, who does it belong to, and how should it be treated? Privacy is the perspective of the individual described by the identity, while compliance is the perspective of the relying parties and other organizations that interact with that user in digital contexts.

To understand these perspectives, we need to answer those key questions.

What is a digital identity?

A digital identity is a collection of data that describes a unique human being from the physical world. The data that best describes a human being is classified by the Prism Project as identity elements. Three categories of identity elements that combine to make a fully fleshed-out digital identity:

- **Biometric identity elements:** biometric templates based on an individual's face, voice, fingerprint, or other unique physical characteristic. This provides a biological element to the digital identity that links it to the user's physical body.
- **Biographical identity elements (PII):** information that literally describes an individual. This includes their name, address, date of birth, marital status, and anything else that describes who a person is, what they have accomplished, and what they are allowed to do. On the most fundamental level, this is provided in the onboarding process via a government-issued ID.
- **Contextual identity elements:** metadata that places an individual and their actions in a time and place. This includes (but is not limited to) location, device signature, transaction history, and behavior.

Who does it belong to?

A digital identity belongs to the person it describes. This is where the privacy perspective comes in. An individual with a digital identity uses it to transact across a wide range of digital and physical spaces and services—from banking and shopping, to chatting with friends, to filing taxes, to entering a workplace or going through security at the airport. While each of those scenarios requires outside parties to receive, transmit, process, and store many of a user's identity elements, the individual to whom they belong retains ownership and entrusts their data for proper usage only.

When an individual's identity elements are mishandled, exploited, or compromised through either misuse, negligence, or malicious means, their privacy is being violated. As such, privacy is the ethical component of identity transactions—a contract between the owner of the data and those who handle it.

A user's ownership of their identity elements provides them with entitlements that are supported by a growing number of privacy regulations.

- **Consent:** a user must consent to the sharing of their identity elements.
- **Access:** a user must have access to their own identity elements.
- **Maintenance:** a user may correct or update data associated with their digital identity.
- **Deletion:** a user may choose to have identity elements deleted.
- **Forgotten:** a step beyond deletion, a user may request that all records of their identity elements and associated transaction records be permanently and irrevocably erased.

How should it be treated?

As described in the Crash Course section of this Prism Report, numerous regulations have emerged in the past decade that have formalized the ethical contract of user privacy. Largely based on the European Union's GDPR law, a growing consensus is emerging worldwide regarding how identity elements should be handled when entrusted to a third party. For the general purposes of this report, best practices for compliance can be boiled down to seven principles:

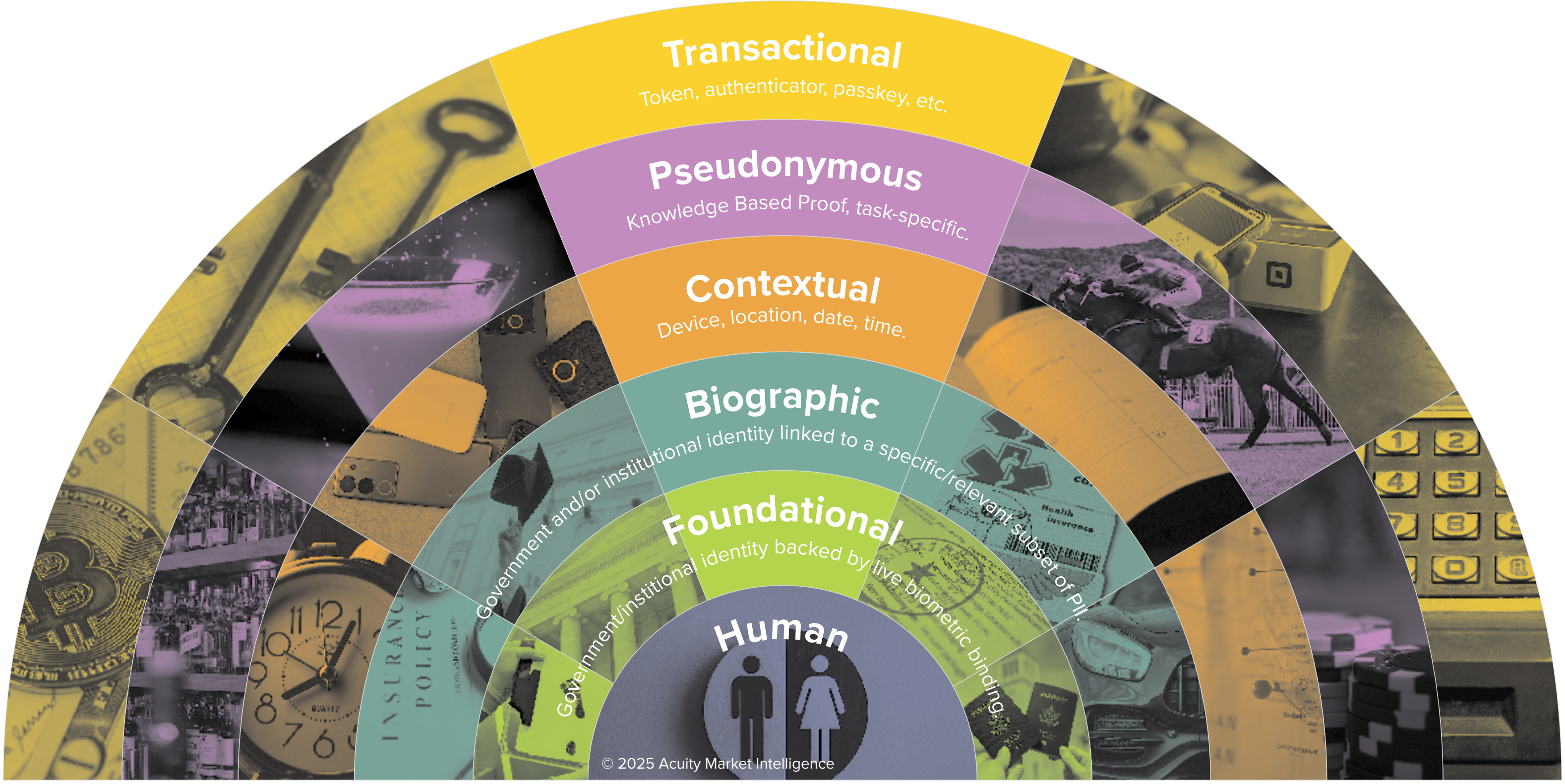
- **Transparency:** The collection and processing of personal identity elements must be done openly and with the user's consent, in accordance with all applicable laws.

- **Purpose:** Identity elements must only be collected and processed for clearly communicated, legitimate, and legal purposes.
- **Specificity:** Only the necessary identity elements required for a transaction should be collected or processed.
- **Accuracy:** Biographical identity elements should be kept up-to-date and remain editable by the user.
- **Temporality:** Identity elements should only be stored as long as they are required for the expressed purpose.
- **Security:** Stored and transferred identity elements should be properly secured.
- **Good faith:** Relying parties must participate in the privacy contract accountability in accordance with local regulations.

These principles are not legally binding, but do represent many of the common compliance requirements from around the globe. As with all information in this report, the practices on this page are recommendations but do not replace specific regulatory advice in your regions of operation.

The Identity Hierarchy

The Prism Identity Hierarchy was first introduced in the 2024 Government Services Biometric Digital Identity Prism Report. It represents the five layers of digital identity enabled through the use of biometrics—Foundational, Biographical, Contextual, Pseudonymous, and Transactional. Transactions at every level of the Identity Hierarchy require the collection, transmission, and storage of identity elements, and therefore present an opportunity for privacy and compliance-enhancing technologies and solutions.


Transactional
Token, authenticator, passkey, etc.
Pseudonymous
Knowledge Based Proof, task-specific.
Contextual
Device, location, date, time.
Biographic
Government and/or institutional identity linked to a specific/relevant subset of PII.
Foundational
Government/institutional identity backed by live biometric binding.
Human

© 2025 Acuity Market Intelligence

Foundational Identity

Foundational identity is the core of digital identity, and it has two components: government-issued identities and physical and/or digital credentials, and the biometrics that bind them to a real human being. It is on this foundational identity that all subsequent layers can be established with integrity. But in a digital world where biometrics linked to government-issued credentials are vulnerable to exposure, there are crucial considerations for privacy and compliance.

- **Privacy—**From a digital identity standpoint, foundational identity is the most sensitive data belonging to an individual, especially when bound to biometrics. As such, this primary layer of the hierarchy should be viewed through the perspective of sovereignty and guardianship: foundational identity elements belong to the user they describe, and the relying parties, organizations, or government entities that hold them are responsible for protecting them and the end user's right to access, revision, and deletion.Synthetic Identities aspire to the foundational level of the identity hierarchy. If a synthetic identity can be successfully built using counterfeit PII or deepfakes, then it can transact with the digital world as if it were a real human being.

- **Compliance—**On the compliance side of the equation, observing the above privacy best practices will go a long way in ensuring alignment with the growing number of citizen and consumer regulations, e.g, EU's GDPR (General Data Protection Regulation), CCPA (California Consumer Privacy Act), etc. This identity layer is also crucial for compliance with identity-based regulations, such as Know Your Customer (KYC) and Anti-Money Laundering (AML) provisions, which require relying parties to verify the personhood and legitimacy of individuals they interact with through due diligence. As such, the foundational identity layer poses a high risk but necessary challenge for compliance: it stands as table stakes for digital business, but also must be protected at all costs.

Biographical Identity

Biographical identity is the time-based element of a digital identity. Where a person was born, where they live, what school they attended, and how they make a living—these details are types of PII that serve a number of purposes where identity is concerned. Biographical identity provides the basis for certain authorizations (what benefits you can access, what rights and privileges you are entitled to) and a history that can further legitimize a digital identity.

- **Privacy—**Biographical identity is much more fluid than foundational identity. Addresses, employment details, education, and certifications—this data is slightly less valuable than foundational data, but it is much more challenging to manage. Identity data on this level has a limited shelf life, but it is also, in some cases, publicly available or voluntarily shared. For privacy concerns, users must have control over what they want to be public, what they want to be private, and what they want to be deleted and forgotten.
- **Compliance—**This layer of identity requires relying parties to be vigilant in terms of housekeeping, transparency, and customer service. Biographical data must be up-to-date to ensure licenses, credentials, and benefits remain valid. The identity elements here are also used for demographic marketing and research, which, under most privacy laws and regulations, requires active consent to collect. It is often collected, shared with third parties, and disseminated in violation of these laws and regulations. And finally, customers must have easy-to-use and understandable ways to interact with relying parties that enable them to opt in or out of sharing their biographical data, updating it, or deleting it.

Contextual Identity

Contextual identity is an element of digital identity that combines location, behavior, things you have, and things you know. Similar to biographical identity, the contextual layer is concerned with what a user typically does, where they typically are, how they typically behave, and with what devices they typically transact.

- **Privacy—**From a privacy perspective, the contextual layer of identity can be considered what a user does and where they do it in any given moment. Digital identity technologies rely on contextual identity elements to ensure personhood and detect fraud. But the collection, observation, and processing of this data veers into the realm of surveillance. Privacy demands that users have the right to dissociate contextual identifiers from their biographical and foundational data on demand.
- **Compliance—**Providing users with the ability to opt-in or opt-out of contextual data collection, like location services, remains a best practice for compliance. Users should be given the ability to review and delete their contextual history, while the benefits of that data are clearly communicated to them. In some cases, such as with Illinois' BIPA (Biometric Information Privacy Act) law, general surveillance for security purposes that uses biometrics must also be obtained through consent. Provisions for anonymizing facial recognition surveillance and regularly deleting collected data are a growing necessity.

Pseudonymous Identity

Pseudonymous identity is a transactional layer of digital ID that builds on the confidence of a strong foundation enhanced with biographical and contextual elements. In a situation with an authentic digital identity, a user can make transactions that leverage the permissions granted by their sensitive information without needing to share any additional information. An easy example is buying restricted substances: instead of sharing a driver's license with your name, address, date of birth, and license number clearly visible, a pseudonymous transaction simply asserts: yes, this ID holder is authorized (i.e., they are 16 or 21 and can purchase alcohol, marijuana, or have access to age-restricted digital services).

- **Privacy—**The pseudonymous layer of the identity hierarchy is privacy-empowering. Only achievable when all previous layers are in place and protected, pseudonymous identity describes the ability for individuals to fully control the scope of identity elements shared with relying parties in transactions, while also benefiting from the promised convenience of digitization.

- **Compliance—**If organizations are equipped to receive trusted pseudonymous identity transactions, they become implicitly compliant. Receiving trusted confirmation of a customer's access without having to collect or manage any actual identity elements means it is impossible to run afoul of privacy regulations.

Transactional Identity

Transactional identity is the outermost layer of the hierarchy. This is the world of payments and account logins. Unlike the other layers, transactional identity can be independent of the lower layers, as many everyday authorizations do not require contextual, biographical, or foundational identity assurance.

- **Privacy—**The transactional layer of identity is a dangerous place for privacy because, while the identity elements in play are largely impersonal, the digital spaces that can be accessed at this level often contain valuable contextual, biographical, or even foundational data. It is through the transactional layer that many historic data breaches have occurred, so while this outer layer may seem less important than the others, it is perhaps the most crucial for the actual protection of privacy.
- **Compliance—**For many relying parties, transactional data provides an alternative to holding the more sensitive identity elements traditionally used for marketing and demographic purposes. Because a transaction history can be wholly anonymous, relying parties can develop robust customer profiles without the need to manage personal data, thus significantly reducing the liability associated with holding customer PII. However, this is also the layer of data breaches, and organizations seeking regulatory compliance must strive to protect account access in order to prevent the massive leaks that have characterized the past decade and a half.

Privacy and Compliance Vulnerabilities

The Identity Hierarchy illustrates the relationship between individuals, relying parties, and identity elements. However, to protect these identity elements, we need to understand the identity verification and authentication processes through which data is collected, transmitted, processed, and stored

How Identity Verification and Authentication Work

First, we need to understand the infrastructure used to process biometrics and digital identities for both remote and in-person transactions.

Individuals can engage with this infrastructure in two ways:

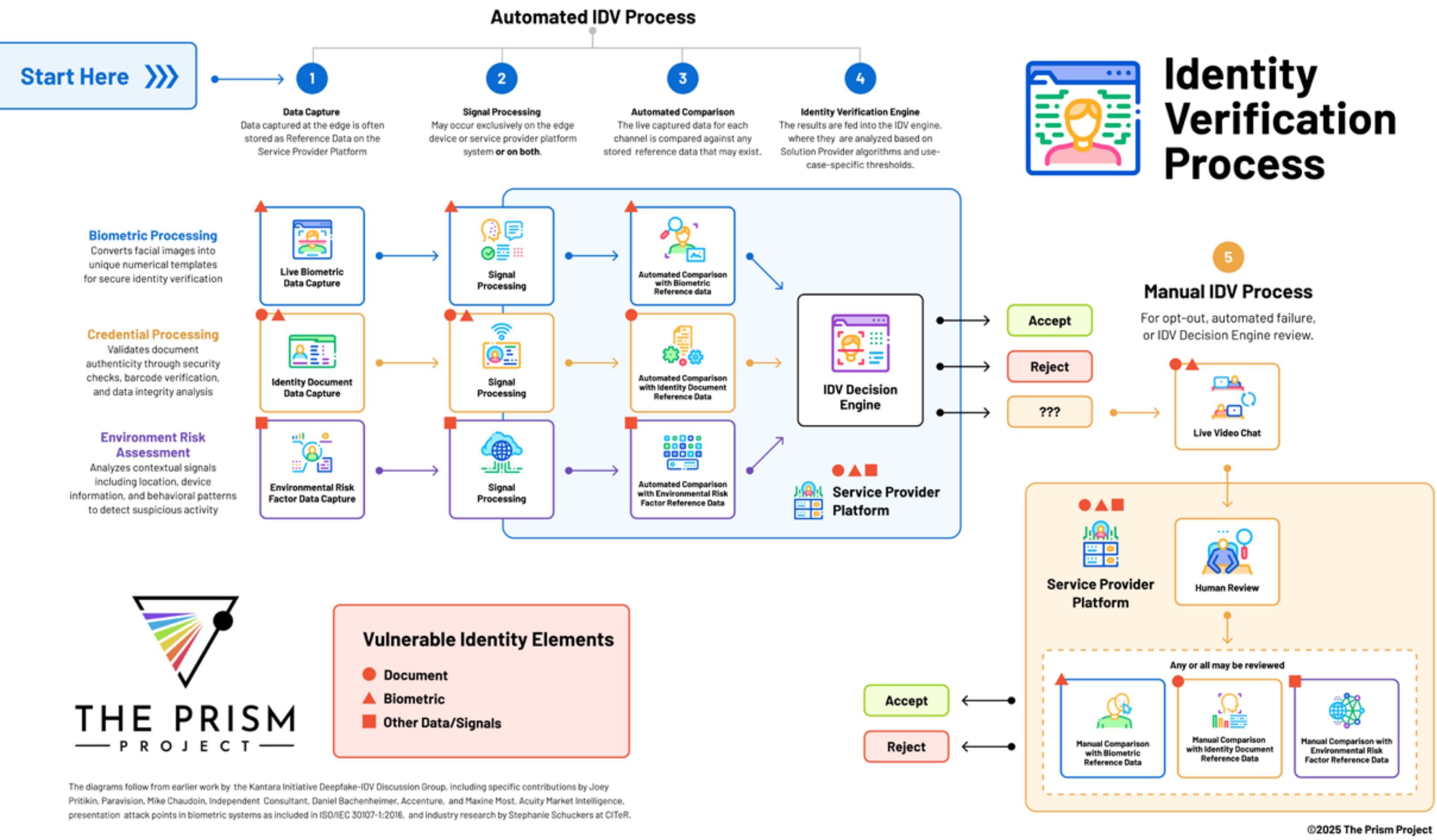
- **Automated** - A user-initiated process in which biometric, PII, and contextual data are submitted through edge device sensors like cameras and microphones.
- **Manual** - A host-initiated process in which a human reviewer interacts with an end user through a video channel, a voice channel, or face-to-face at a physical location.

The manual interface may stand on its own or serve as a backup for individuals who opt out of or fail the automated verification or authentication process. While all of these transactions are generally performed in remote contexts, the process can be adapted for in-person verification and authentication in host facilities like bank branches, government offices, or retail locations. For instance, enrolling in a physical access control system can be done via automated verification or in-person at a facility's security office. In all variations, the interactions surrounding identity elements remain the same.

At its simplest level, the identity verification and authentication processes can be broken down into four steps:

Data Capture - A user seeking verification submits data into a system. That data consists of three categories, spanning the identity hierarchy:

- **Biometric identity elements:** Foundational biological user data, typically in the form of face or voice; this represents the physical person subject to verification or authentication.
- **Biographical identity elements (PII):** Foundational and biographical user data, typically in the form of identity


Automated IDV Process
Start Here ❯❯❯
1
Data Capture
Data captured at the edge is often stored as Reference Data on the Service Provider Platform
2
Signal Processing
May occur exclusively on the edge device or service provider platform system or on both.
3
Automated Comparison
The live captured data for each channel is compared against any stored reference data that may exist.
4
Identity Verification Engine
The results are fed into the IDV engine, where they are analyzed based on Solution Provider algorithms and use-case-specific thresholds.
Identity Verification Process
Biometric Processing
Converts facial images into unique numerical templates for secure identity verification
Credential Processing
Validates document authenticity through security checks, barcode verification, and data integrity analysis
Environment Risk Assessment
Analyzes contextual signals including location, device information, and behavioral patterns to detect suspicious activity
Live Biometric Data Capture
Identity Document Data Capture
Environmental Risk Factor Data Capture
Signal Processing
Signal Processing
Signal Processing
Automated Comparison with Biometric Reference data
Automated Comparison with Identity Document Reference Data
Automated Comparison with Environmental Risk Factor Reference Data
IDV Decision Engine
Service Provider Platform
Accept
Reject
???
5
Manual IDV Process
For opt-out, automated failure, or IDV Decision Engine review.
Live Video Chat
Service Provider Platform
Human Review
Any or all may be reviewed
Manual Comparison with Biometric Reference Data
Manual Comparison with Identity Document Reference Data
Manual Comparison with Environmental Risk Factor Reference Data
Accept
Reject
THE PRISM PROJECT
Vulnerable Identity Elements
● Document
▲ Biometric
■ Other Data/Signals

The diagrams follow from earlier work by the Kantara Initiative Deepfake-IDV Discussion Group, including specific contributions by Joey Pritikin, Paravision, Mike Chaudoin, Independent Consultant, Daniel Bachenheimer, Accenture, and Maxine Most, Acuity Market Intelligence, presentation attack points in biometric systems as included in ISO/IEC 30107-1:2016, and industry research by Stephanie Schuckers at CITeR.

©2025 The Prism Project

documents; this describes the physical person.

- **Contextual identity elements:** The captured data is processed and transmitted to a host system for comparison and verification. The actual processing is solution and application-dependent. Processing is sometimes performed on the edge device, sometimes on the host system, or sometimes via a hybrid configuration.

Signal Processing - The captured data is processed and transmitted to a host system for comparison and verification. The actual processing is sometimes done on the edge device, on the host system, or via a hybrid configuration.

Reference Comparison - Captured identity elements are compared to reference data. The types of elements being compared will vary depending on the system used, the application requirements, and the identity transaction being completed.

For enrollment transactions:

- **Biometrics** are matched against the photo on a government-issued ID or the chip embedded in the document, and sometimes against profiles of previously enrolled users to ensure that a single individual is not linked or attempting to link to more than one identity within a reference database.

- **PII** is compared to government sources or records, watch-lists, and lists of counterfeit documents, as well as the profiles of other enrolled users.
- **Context** data is compared to known risk signals that indicate a high likelihood of fraud.

For authentication transactions taking place after enrollment:

- **Biometrics** are matched against biometric templates established on the previous enrollment.
- **PII** is rarely used in this step, but when it is, it is compared to government sources or records, watchlists, and/or counterfeit document lists.
- **Context** data captured on the end device is compared to behavioral profiles associated with a user's transaction history.

Decision - If the biometric and PII data captured match the biometric and PII data in the reference database, within specified thresholds, and if environmental risk analysis does not detect any anomalies outside acceptable ranges, verification is granted and transactions are authorized. If any of these identity checks fail to conform to established parameters, additional automated step-up measures may be deployed, verification may be withheld, transactions may be rejected, remote users may be redirected to a live video channel for human review, or, in an in-person scenario, additional security steps may be taken.

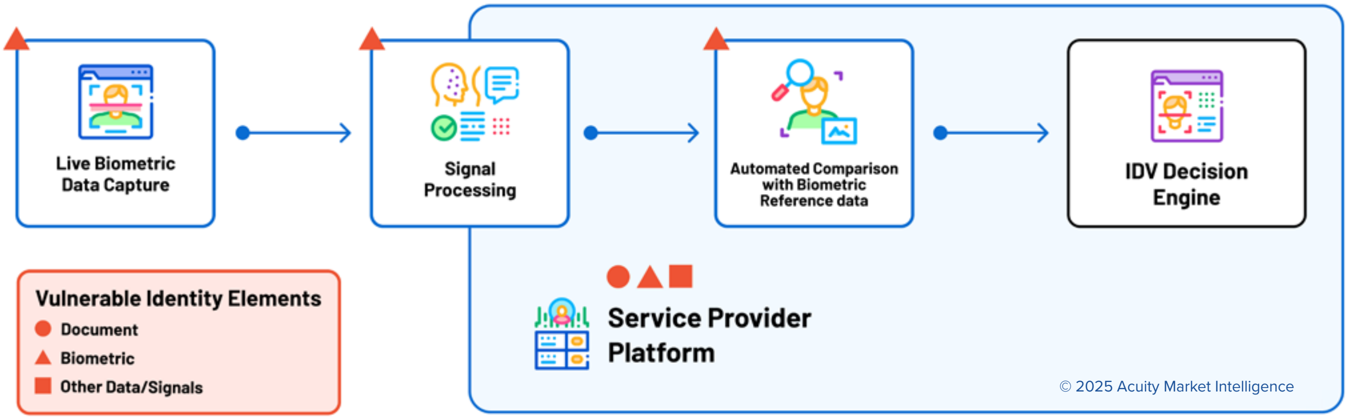
That four-step process requires interaction between two systems:

- **End User System (Edge Device)** - The device that allows a user to interface with the remote identity verification and authentication process through data capture and potentially some signal processing. This could be a personal device, like a smartphone, or it could be a fixed biometric and/or document capture device, like a fingerprint reader and/or a document scanner used in a government office or a bank branch.
- **Host System** - The identity verification decision-making ecosystem that includes the IDV software, reference databases, at least some (if not all) signal processing, and the decision-making engine. The host system also facilitates secure data transfer within the IDV system and with externally connected systems that rely on the IDV decision engine results. This may also include human reviewers for in-person

verifications or remote verifications that fail the initial thresholds for biometric and PII matching, or indicate an anomalous risk signal.

Automated remote identity verification and authentication methods are particularly vulnerable to threats from bad actors and run the risk of violating privacy principles as they rely on three separate channels for data capture and comparison. By examining each discrete identity data touchpoint, we can observe individual best practices for protecting privacy and ensuring broad compliance.

Automated Biometric Processing Channel Vulnerabilities


Live Biometric Data Capture
Signal Processing
Automated Comparison with Biometric Reference data
IDV Decision Engine
Vulnerable Identity Elements
● Document
▲ Biometric
■ Other Data/Signals
●▲■
Service Provider Platform
© 2025 Acuity Market Intelligence

Biometric Capture: Biometrics must only be captured with explicit consent from the individual they belong to. What data is being captured, why, how it will be used, and how long it will be stored must be clearly communicated at this step.

Signal Processing: The transmission and processing of biometrics require transparency and consent. Identity elements are vulnerable in transit, so they must be adequately secured using encryption if leaving a device.

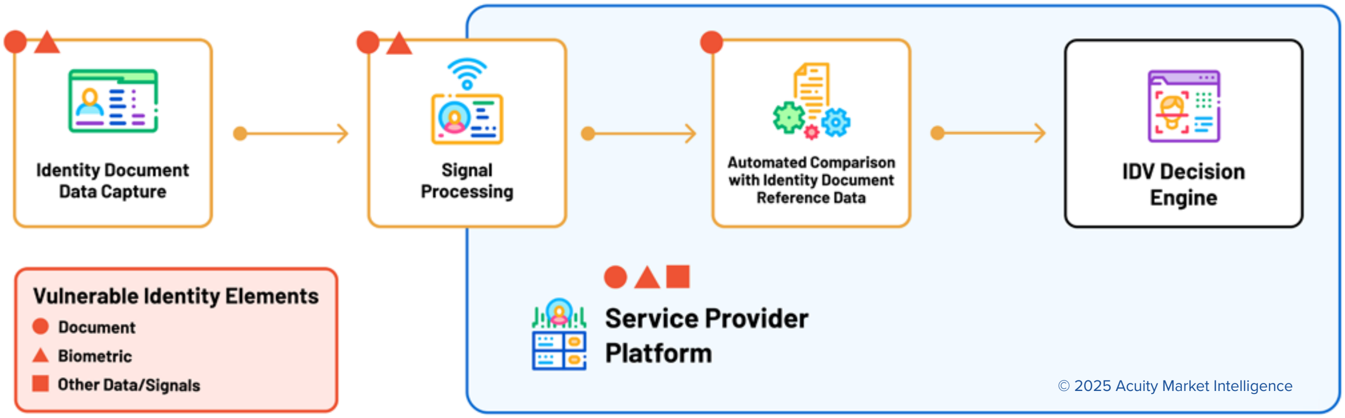
Comparison: The reference data used for comparison on servers or on devices must be in template form. Identity elements must not be exposed during the comparison process.

Decision: Biometric templates can be used as reference data, but any image data must be purged after a decision is made to mint a digital identity. Additional biometric data collected for anti-fraud purposes, like liveness data or video, must also be purged.

In some cases, identity elements, including face or document images, may be retained to combat **Velocity Attacks** for a specified period of time. The liability of holding this highly sensitive data is extremely high. It must be stored and managed with the highest level of security, and promptly deleted within the specified timeframe. Users must be informed about the identity elements that are being collected, how long they will be stored, and for what specific purposes they will be used.

VELOCITY ATTACKS: High-volume fraud attacks perpetrated in a very short period of time, where the same face may be linked to multiple identities—authentic or synthetic. For more on synthetic identities, download the Deepfake and Synthetic Identity Prism Report.

Automated Credential Processing Channel PII Vulnerabilities


Identity Document Data Capture
Signal Processing
Automated Comparison with Identity Document Reference Data
IDV Decision Engine
Vulnerable Identity Elements
● Document
▲ Biometric
■ Other Data/Signals
Service Provider Platform
© 2025 Acuity Market Intelligence

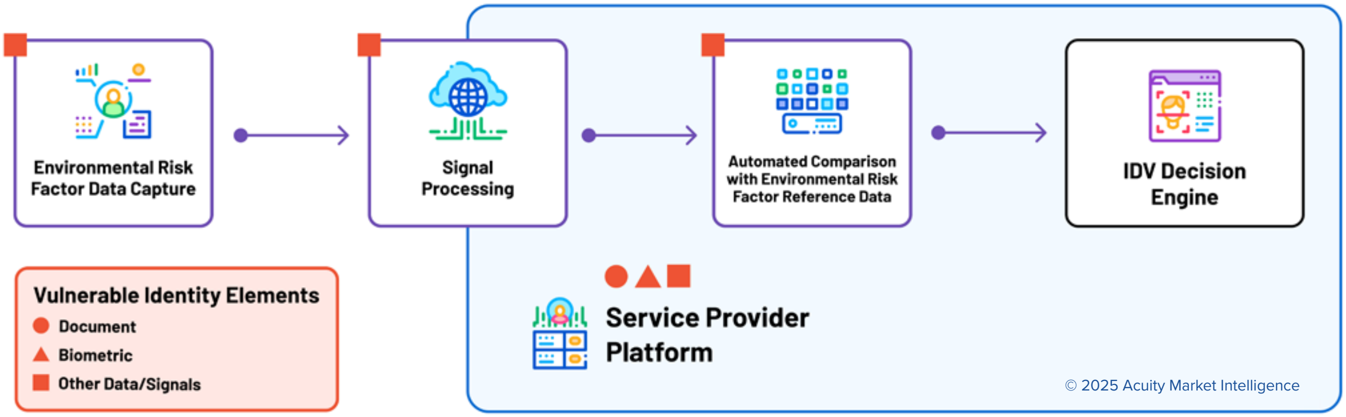
Identity Document Capture: Identity documents must only be captured with consent from their owner. What data is being captured from the document, why, how it will be used, and how long it will be stored must be clearly communicated at this step.

Signal Processing: Users must provide explicit consent to the processing and transmission of any data captured. Biographical identity elements must be properly secured in transit using strong encryption. What data is being captured, why, how it will be used, and how long it will be stored must be clearly communicated at this step.

Comparison: The data stored for reference comparison must be accurate, up-to-date, and only include identity elements required for a relying party's stated purpose. PII must not be exposed during the comparison process.

Decision: Any data not required for the stated purpose of the verification or authentication transaction must be purged. Out-of-date, inaccurate, or duplicate data should also be deleted.

Automated Environmental Risk Assessment Channel Contextual Data Vulnerabilities


Environmental Risk Factor Data Capture
Signal Processing
Automated Comparison with Environmental Risk Factor Reference Data
IDV Decision Engine
Vulnerable Identity Elements
● Document
▲ Biometric
■ Other Data/Signals
●▲■
Service Provider Platform

© 2025 Acuity Market Intelligence

Environmental Risk Factor Capture: Contextual identity elements also require consent for collection. Good faith efforts must be made to explicitly communicate to users what contextual data is being collected from them, for how long, and how they can opt out of its collection. The collection of this type of data is particularly contentious, as contextual identity elements are commonly used for other, often non-consensual purposes such as digital marketing.

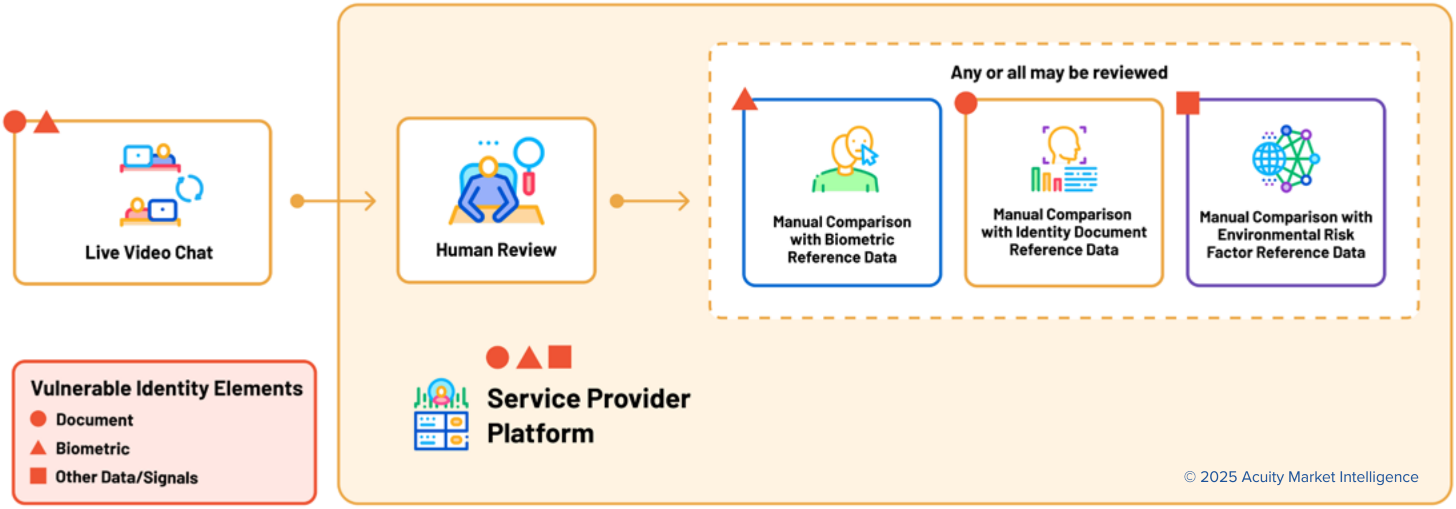
Signal Processing: Only metadata required for comparison should be transmitted. All identity elements must be secured when in transit using strong encryption.

Comparison: Reference data used for comparison with contextual identity elements should be minimal and securely stored. Contextual identity elements should only be stored if required by a relying party's stated purpose.

Decision: Once a risk assessment has been completed, contextual identity elements should be purged after they have been used to revise an individual's risk profile.

Prism Ver. 1.0 © 2025 The Prism Project

Manual Channel Vulnerabilities


Live Video Chat
Human Review
Any or all may be reviewed
Manual Comparison with Biometric Reference Data
Manual Comparison with Identity Document Reference Data
Manual Comparison with Environmental Risk Factor Reference Data
Service Provider Platform
Vulnerable Identity Elements
● Document
▲ Biometric
■ Other Data/Signals
© 2025 Acuity Market Intelligence

Live Video Chat: Explicit user consent must be incorporated into the human review process. The data must be relevant to the stated purpose of the authentication. Any physical or digital media created during the call that is not necessary for audit purposes or future identity transactions must be destroyed or deleted.

Human Review: Human reviewers must not share, tamper with, or make copies of any identity elements. Human reviewers must be adequately trained with up-to-date privacy best practices.

Proposed Solutions to Protect Privacy and Ensure Compliance

With the trend toward harmonization of regional data protection regulations around the globe, all in line with GDPR, the most critical identity privacy considerations revolve around user consent and control, data minimization, security, and transparency. Many biometric digital identity solutions leverage key technologies to center those concepts in their design philosophy. While many of the solutions described in the vendor profiles in this report are proprietary, there are general concepts and technologies that can reliably protect privacy and ensure compliance.

Secure Elements

Cloistered storage and processing spaces on edge devices like smartphones, wearables, or IoT objects where identity elements can be stored, matched, and processed without the need to transfer data. Decentralized by nature, this on-device identity technology is commonly used on consumer grade mobile devices for screen unlock and mobile payments.

Public Key Infrastructure

The protocols that enable authentication between secure elements and relying party services. When a biometric match is made on a secure element, a key is generated on the edge device that can be used to authorize transactions or grant access to controlled areas or accounts. Because PKI doesn't require the transfer of actual identity elements, it operates on the pseudonymous and transactional layers of the identity hierarchy.

Biometrics On Demand

An emerging anonymous form of biometric authentication. Biometrics On Demand solutions generate unique public keys that only exist during the authentication session. This means that biometric data is never stored on devices or servers, nor is it transferred between systems.

Biometric Templates

Now a standard practice in biometric digital identity, biometric templates are encrypted codes that are generated when a user scans their face, fingerprint, iris, or voice. As opposed to images, which can be used to create artifacts for presentation attacks, the best templates cannot be reverse engineered to create raw biometric data.

Encryption

A standard security measure, this is the process of transforming legible data into unreadable code. Encryption protects identity elements at rest and in transit.

Secure Servers

Servers are deployed in identity transactions for the storage and processing of identity elements in the cloud or on relying party premises. Because of the valuable nature of identity elements and the compliance requirement that they be adequately protected, servers need to be secured virtually and physically to prevent malicious actors from accessing honeypots. This may include sharding encrypted identity data across storage locations—digital and physical—to ensure there is no single source of PII that can be exposed.

Biometric Liveness

A support technology for biometric verification and authentication, liveness confirms that biometric identity elements presented to sensors are authentic (as opposed to counterfeit artifacts like masks). Biometric liveness is critical for detecting deepfakes and synthetic identities, which pose a threat to KYC and AML compliance.

Document Liveness and Counterfeit Detection

The biographic PII equivalent of biometric liveness, this support technology is used to detect fraudulent documents submitted in the identity verification process, as well as stolen images of authentic credentials. In addition to enabling proper KYC and AML compliance, document liveness prevents authentic identity elements from being onboarded with synthetic identities, minimizing potential data exposure.

NFC Reading

An increasing number of identity documents include NFC (Near Field Communication) readable chips that store identity elements, including high-resolution biometrics and PII. Biometric digital identity technologies that leverage NFC reading capabilities of edge devices like smartphones can process and match chip-side identity elements without the need to communicate with servers, which carry the highest level of authenticity.

Mobile ID, mDL (Mobile Drivers Licenses), Digital Wallets, VC (Verifiable Credentials)

This next generation of biometric digital identity fully embodies the converged physical/virtual paradigm required to enshrine user privacy and achieve widespread compliance while enabling transactions across the full range of the Identity Hierarchy. Combining the privacy-preserving elements of device-based technology with the assurance of government systems of record, this emerging class of biometric digital identity puts users in full control of their identity elements.

- **Digital Wallet** - An application for securely storing, organizing, and managing a user's set of digital identity credentials, including mobile IDs, mDLs and VCs. Because of the ubiquity required for this technology to be adopted, the most promising of these are built-in to consumer edge devices.
- **Mobile ID** - A broad category of digitized identity documents that can be linked to a user's foundational identity in order to enable identity transactions in virtual and in-person contexts. Examples include digital versions of driver's licenses and state IDs, mobile student IDs, digital health cards, and digital wallets for storing personal information.
- **mDL** - More than just a drivers license on your phone, an mDL is a biometrically-bound government issued digital credential, stored in a digital wallet, which gives a user full control over their identity elements.
- **VC (verified Credentials)** - Cryptographically signed attestations of attributes, skills, or qualifications, which can be biometrically-bound. These can be time-based, granting limited access to privileges, like the Digital Travel Credential (DTC), which enables privacy-first, biometrically-based seamless border crossing.

Prism Ver. 1.0 © 2025 The Prism Project

Training and Policy

While many identity processes are being automated and offloaded to the end user as individuals gain control of their data, the manual identity verification channel remains a prominent part of the identity ecosystem. As such, internal policies that can be easily understood and implemented are required to ensure the proper handling of identity elements and the minimization of insider threats.

Hybrid Centralized- Decentralized Models

The above solutions, each with its own strengths and weaknesses, largely depend on their use of on-device or on-server identity controls. Recent advances in encryption, groundbreaking work on protocols and standards, and innovation in the capture, storage, and generation of identity elements—especially biometrics—have enabled these paradigms to converge. Combining the privacy protection of decentralized identity with the trust and assurance offered by government attested centralization results in a powerful hybrid identity ecosystem; an ecosystem characterized by foundational identity leveraging centralized systems of record and maintained by digital signing, that empowers end users with the pseudonymity and anonymity allowed by secure elements and biometrics on demand. By merging these worlds, individuals benefit from the highest levels of privacy, consent, and control while relying parties confidently ensure compliance.

Privacy and Compliance Vulnerabilities by Vertical Market

Privacy and compliance are more than just goals that relying parties must strive for. The motivation goes beyond ethics regulations and the goodwill engendered by protecting authentic identity elements. As digital transformation demands proactive engagement across every market sector, relying parties must deal with identity in a privacy-and-compliance-first manner to preserve their reputations and to ensure their financial success. The following chart breaks down key privacy and compliance vulnerabilities that relying parties operating in various sectors must confront, highlighting notable data breach incidents that illustrate the privacy risks in key vertical markets.

Vertical Market	Deepfake and Synthetic Identity Threat
Financial Services	• The past decade has seen major data breaches reported by major financial institutions, including JPMorgan Chase (2014), Equifax (2017), and Capital One (2019). • IBM reports that the average cost of a breach in this sector can reach $6.08 million. • The financial services sector is highly regulated and requires compliance with KYC and AML laws, as well as regional directives like the European Union's PSD2.
Healthcare	• Health data regulations like HIPAA in the US carry harsh penalties for organizations that fail to properly secure patient data, while also making it available to users on demand. • Patient records are increasingly targeted by hackers in ransomware attacks, which were responsible for 69% of all patient records compromised in 2024.
Insurance	• Insurance companies are honeypots of sensitive customer information and are a frequent target of hackers seeking a PII jackpot.

Icons attributed to: Gregor Cresnar, arista septiana dewi, Saepul Nahwan from Noun Project (CC BY 3.0)

Vertical Market	Deepfake and Synthetic Identity Threat
Government Services	• Governments are the arbiters of citizen identity, issuing foundational identity elements and maintaining systems of record—this makes them highly valuable targets of hacking, ransomware, and other attack vectors, as well as susceptible to highly damaging data leaks due to negligence, corruption, or abuse. Globally, the past ten years have seen high profile data breaches that exposed citizen identity elements in India, Ethiopia, Iran, the USA, and China.
Retail & eCommerce	• Retail and ecommerce businesses store large volumes of biographical and contextual identity elements for demographic marketing. In addition to being invasive, regulations like GDPR are limiting the methods through which this data can be collected and how it can be used. • In 2025, a rash of cyberattacks affected high-profile retailers including Adidas, Victoria's Secret, Harrods, Cartier, The North Face, and Marks and Spencers, the last of which had its online services disrupted for months, causing it to estimate a £300m reduction in profits for the year.
Travel	• In 2023, Southwest Airlines and American Airlines experienced data breaches as a result of compromised third-party software, which exposed pilot credentials. This highlights the importance of incorporating privacy into identity solutions, as the vulnerabilities of business partners become liabilities for relying parties. • Facial recognition is increasingly deployed in travel terminals to enable seamless passenger experiences. This requires explicit consent for biometric capture, clear storage terms, and strict privacy policies.
Hospitality	• Marriott has been involved in multiple data breaches in the past decade, The most infamous occurred in 2018, exposing foundational identity elements of over 500 million guests. The company suffered reputational damage and regulatory penalties totalling $52 million. • Hospitality providers are often compelled to verify identity element including biographic data such as names, addresses, and ages, as well as review credentials like driver's licenses and passports., This puts these relying parties in high-risk compliance situations. • Moving toward a transactional mode of consumer profiling, in which pseudonymous transactions histories are used to understand purchasing habits, is an identity-powered, compliance ready alternative to using biographical and contextual identity elements.
Social Media	• The three foundational social media platforms all suffered major data breaches in 2021 affecting 533 million Facebook users, 221.52 million Twitter (now X) users, and 700 million LinkedIn users. • Social media is also a significant channel for scams that target users' identity elements, including passwords, financial data, and PII.
Gaming	• Gambling is a highly regulated industry that requires compliance with KYC and AML laws, as well as other regional policies, e.g., age verification. • Video game companies also increasingly collect and manage identity elements, and publishers including Ubisoft, Blizzard, and Nintendo have all experienced data breaches.
Controlled Substances, Products & Content	• Age checks traditionally require overexposure of biographical data, thanks to the reliance on human review of identity documents—pseudonymous age checks minimize the data shared while improving the assurance of the authentication.

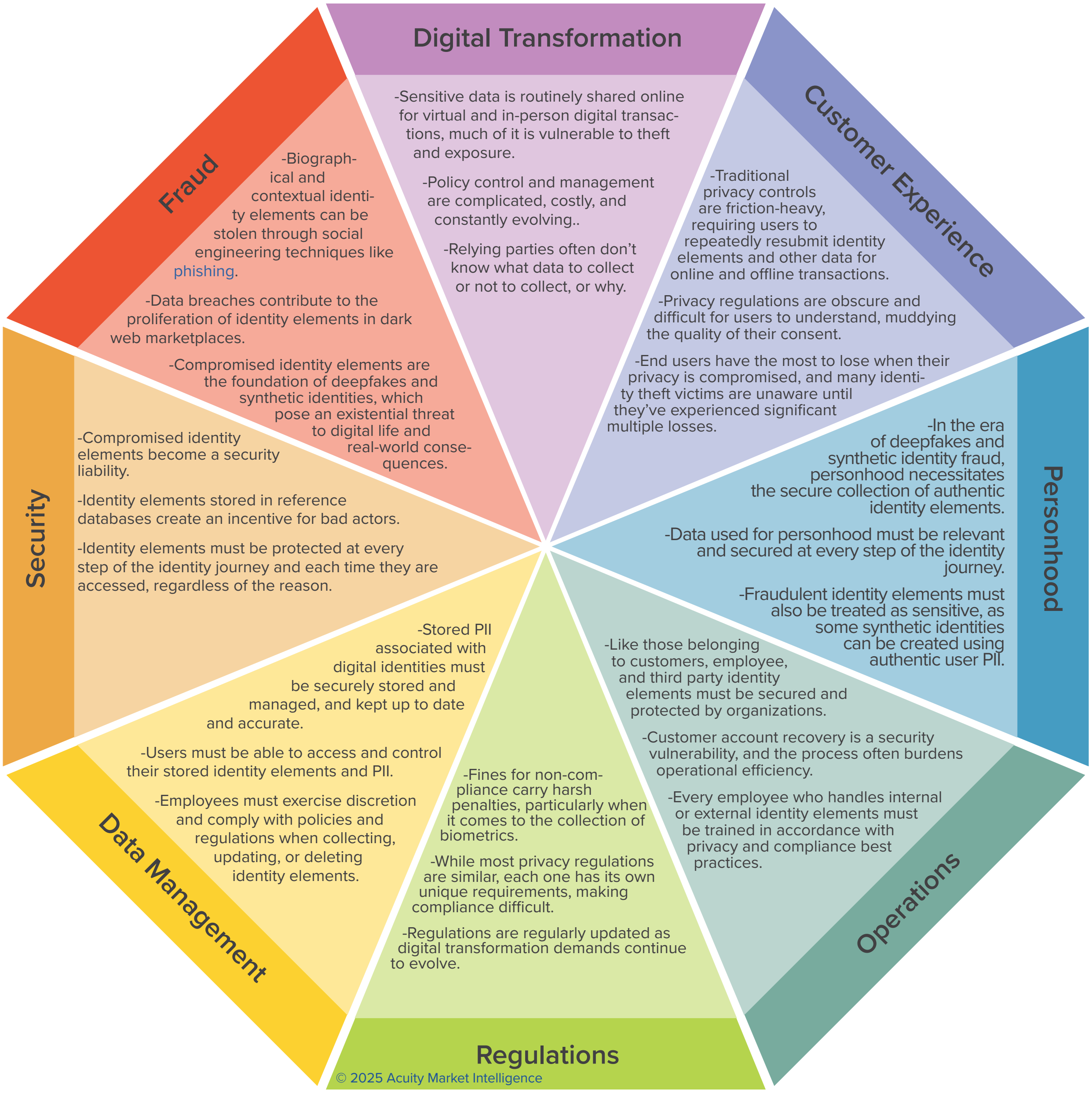
Icons attributed to: Adrien Coquet, PEBIAN, karyative, Omah Icon, Ria Fitriana, IconPai from Noun Project (CC BY 3.0)

Vertical Market	Deepfake and Synthetic Identity Threat
Fan Experience	• In 2024, over 560 million Ticketmaster customers had their data exposed in a massive data breach. The company suffered significant reputational damage, was subject to litigation, and had to cover the cost of credit monitoring for all those impacted. • Arenas and stadiums are increasingly integrating biometrics into fan entry, concession and merchandise transactions, and staff access. Explicit consent, privacy, and data management policies are required to comply with all relevant regulations, which may vary significantly across individual facilities. • The 2024 Stadium Connectivity Outlook Survey reported that 47% of respondents said biometrics for ticketing, access, and concessions were on their roadmap
Digital Entertainment	• As digital entertainment continues to integrate user customization features and hands-free controls, it is increasingly necessary to have consent controls in place for data collection. Provisions must also be in place for users to update or delete any data associated with their identity.
Border Control and Immigration	• Citizenship and visa application procedures require the collection and transmission of foundational and biographical identity elements between countries. • Increasing use of self-service automated border control solutions requires adherence to national and global standards for data collection, data management, and user consent and control.
National Security	• The digitization of all of the above sectors and more is creating an online warscape in which state and non-state sponsored bad actors are seeking out the identity elements of foreign nationals. Icons attributed to: Selot Lo, Febri Ardianto, Vectors Point, SITI NURHAYATI, Purple Iconix from Noun Project (CC BY 3.0)

This table is far from exhaustive, but the diversity of impacted sectors underscores the ubiquity of the collection, transmission, and storage of identity elements across our increasingly digitized world. The good news is that identity vendors and infrastructure organizations are working to build privacy into the next generation of digital identity. All that remains is for relying parties to identify their own vulnerabilities and prioritize adoption of privacy-enhancing technologies.

The Prism Lens

The Prism Lens is a knowledge framework that presents the most critical market challenges facing relying party executives, either within well-defined market sectors (as in previously published vertical Prism reports) or, in this case, within the context of a consequential issue with broad potential for disruptive impact across all market sectors. The Privacy and Compliance Prism Lens illustrates how the ethical imperative for privacy and the regulatory demands of compliance intersect with broader market drivers in an era of free-flowing data and AI-powered fraud.



Digital Transformation

-Sensitive data is routinely shared online for virtual and in-person digital transactions, much of it is vulnerable to theft and exposure.

-Policy control and management are complicated, costly, and constantly evolving..

-Relying parties often don't know what data to collect or not to collect, or why.

Customer Experience

-Traditional privacy controls are friction-heavy, requiring users to repeatedly resubmit identity elements and other data for online and offline transactions.

-Privacy regulations are obscure and difficult for users to understand, muddying the quality of their consent.

-End users have the most to lose when their privacy is compromised, and many identity theft victims are unaware until they've experienced significant multiple losses.

Personhood

-In the era of deepfakes and synthetic identity fraud, personhood necessitates the secure collection of authentic identity elements.

-Data used for personhood must be relevant and secured at every step of the identity journey.

-Fraudulent identity elements must also be treated as sensitive, as some synthetic identities can be created using authentic user PII.

Operations

-Like those belonging to customers, employee, and third party identity elements must be secured and protected by organizations.

-Customer account recovery is a security vulnerability, and the process often burdens operational efficiency.

-Every employee who handles internal or external identity elements must be trained in accordance with privacy and compliance best practices.

Regulations

-Fines for non-compliance carry harsh penalties, particularly when it comes to the collection of biometrics.

-While most privacy regulations are similar, each one has its own unique requirements, making compliance difficult.

-Regulations are regularly updated as digital transformation demands continue to evolve.

Data Management

-Stored PII associated with digital identities must be securely stored and managed, and kept up to date and accurate.

-Users must be able to access and control their stored identity elements and PII.

-Employees must exercise discretion and comply with policies and regulations when collecting, updating, or deleting identity elements.

Security

-Compromised identity elements become a security liability.

-Identity elements stored in reference databases create an incentive for bad actors.

-Identity elements must be protected at every step of the identity journey and each time they are accessed, regardless of the reason.

Fraud

-Biographical and contextual identity elements can be stolen through social engineering techniques like phishing.

-Data breaches contribute to the proliferation of identity elements in dark web marketplaces.

-Compromised identity elements are the foundation of deepfakes and synthetic identities, which pose an existential threat to digital life and real-world consequences.

© 2025 Acuity Market Intelligence

Solutions

When we break the Prism Lens into its component parts, we examine each challenge individually to see how the application of biometrics and strong identity verification controls can help uphold the privacy contract and achieve future-proof compliance.

Digital Transformation

-Pseudonymous identity transactions enabled by mobile IDs, mDLs, VCs, or passkeys limit the amount of data sharing while maintaining trust.

-Investing in privacy-first, biometric digital identity can future-proof compliance by putting users in control of their identity elements.

-Biometric digital identity technologies streamline the data collection process by creating a common language for identity transactions.

Customer Experience

-Privacy-first first biometric digital identity solutions improve customer experience and increase end user confidence.

-Compliance-forward technologies make privacy easy for users to understand and protect them from exploitation.

-Decentralized biometric digital identity solutions protect end users from being victimized in data breaches.

Personhood

Biometric digital identity supported by a privacy-first system of record can prove personhood without the transmission of identity elements.-

-Biometric liveness solutions can anonymize data used for deepfake detection, meaning that even if the data is compromised, it is useless.

-Biometric digital identity solutions deployed with sufficient deepfake and synthetic identity detection capabilities prevent fraudulent identity elements from entering a system at the time of onboarding.

Operations

-The same biometric digital identity solutions that protect consumers have privacy-enhancing applications in enterprise physical access control, time & attendance, and digital security.

-Biometric digital identity solutions can automate account recovery while securing the channel.

-Privacy-by-design biometric digital identity decreases the exposure of identity elements and sensitive data, minimizing employee liability.

Regulations

-Decentralized biometric digital identity can limit or even eliminate the need to transfer identity elements to a relying party.

-Biometric digital identity technologies that adhere to privacy best practices enable widespread compliance, making it easier to focus on unique regulatory requirements.

-By adopting biometric digital identity technologies and prioritizing the privacy contract with end users, relying parties will be well-positioned to evolve alongside regulations instead of playing catch-up.

Data Management

-Mobile IDs, mDLs, and VCs can be updated, revised, and revoked on-demand.

-Decentralized biometric digital identity solutions provide users safe 24/7 access to their identity elements.

-By putting users in control of their biometric digital identities, employee contact with identity elements can be minimized.

Security

-Hybrid centralized/decentralized identity solutions provide the assurance of system of record-based identity verification while limiting identity elements exposure in day-to-day transactions.

-Templatization, encryption, anonymization, and/or fragmentation of biometrics makes even compromised biometric identity elements useless.

-Biometrics on-demand, passkeys, and other device-based identity solutions ensure identity elements are never in transit.

Fraud

-PII and contextual identity data cannot be phished when bound to biometrics and foundational identity and protected with sufficient liveness controls.

-By its nature, decentralized biometric digital identity cannot be leaked at scale.

-Deepfake detection and synthetic identity countermeasures can bolster the integrity of authentic digital identities while also enabling compliance with data accuracy regulations.

Looking through the Prism Lens

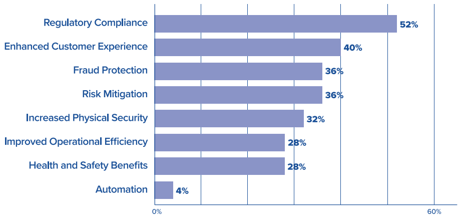
Let’s take a closer look at each fragment of the Prism Lens.

Digital Transformation

To call digital transformation a trend is starting to feel absurd. The embrace of digitization is almost ubiquitous, with Gartner stating that over 90% of companies globally are engaging with digital technologies. And that’s a change you can feel in your daily life—mobility and connectivity have become an expectation in our modern transactions with businesses, governments, and each other. But, as we explored in the Crash Course and Vulnerabilities sections of this report, the convergence between virtual and online worlds is driven by our ability to carry our identity across different contexts. And that means identity elements must be collected, processed, and stored with privacy and security at the forefront.

The Prism Project surveyed vertical market stakeholders on their digital technology adoption motivators:

Which benefits of digital transformation motivate your organization to adopt new digital technologies?



Every online account is a potential exposure point for PII, and every transaction is an opportunity for malicious actors to intercept identity elements. But the most crucial identity privacy vulnerability for the past decade has been the breach. Surfshark, a VPN company that publishes an annual online privacy report, estimates the total number of compromised online accounts in 2024 to be 5.5 billion. And while individual users end up being the ultimate targeted victims, the consequences of corporate data breaches are serious and twofold; companies suffer significant reputational damage as well as substantial financial damages, with IBM estimating an average of $4.44 million per incident.

Data exposure is a compliance nonstarter in the age of GDPR-style regulations. But the risk involved with handling identity elements is the cost of digital transformation. Biometric digital identity solutions can protect identity elements in a variety of ways—from decentralized storage and encryption to novel forms of anonymous biometric credentialing—putting users in control of their data for informed consent and alleviating the regulatory burden on relying parties.

Customer Experience

Privacy is not just a legal requirement; it’s also an increasingly important customer demand. In a survey of nearly 5000 individ-

Prism Ver. 1.0 © 2025 The Prism Project

uals across 19 countries, the IAPP (International Association of Privacy Professionals) found that 68% of consumers are either somewhat concerned or very concerned about their online privacy. And that fear is having an effect on transaction completion rates over digital channels. Cart abandonment rates online are consistently around the 70% mark, according to the Baymard Institute, and while the reasons behind that statistic vary, much of it is attributed to a lack of both convenience and trust when providing personal information during the onboarding process.

68% of consumers are either somewhat concerned or very concerned about their online privacy, according to IAPP's survey of nearly 5000 individuals across 19 countries.

Onboarding is a crucial transaction in the world of regulation, as KYC and AML laws are widespread and non-negotiable. Biometric identity proofing and verification technologies enable the automation of these processes, helping reduce friction at the first interaction between users and relying parties. And while some enrollment solutions do collect, process, and store large amounts of personal data that might give some users pause, the emergence of pseudonymous digital credentials like the US mobile driver's license (mDL), the EU's mobile ID, or ICAO's Digital Travel Credential (DTC) promise to satiate the need to provide KYC accountability while putting consumers in complete control of their identity elements.

Personhood

According to TransUnion, the problem of synthetic identities is a $3.3 billion issue. And it's certainly a pernicious issue: thanks to the stealth nature of synthetic identities, the scope of this AI-powered fraud threat is near impossible to quantify. But it is easy to see how it threatens the foundation of privacy and compliance in the age of digital transformation. On the one hand, accepting synthetic identities into a service runs afoul of KYC and AML regulations. On the other hand, many synthetic identities are built using authentic identity elements stolen from everyday users. That puts relying parties in a bind: they need to catch synthetic identities at the front door while also ensuring that the data introduced into their systems remains protected.

A full arsenal of synthetic identity countermeasures is illustrated in the Deepfake and Synthetic Identity Prism Report, and each is applicable in this privacy and compliance context. Liveness and deepfake detection can prevent counterfeit identity elements from being introduced into a database, while biometric search and match solutions can weed out duplicates or even find fraudulent accounts. By incorporating biometrics at the core of personhood, compliance comes with the added security and assurance.

Learn more about how biometrics protect personhood in the Deepfake and Synthetic Identity Prism Report.

Prism Ver. 1.0 © 2025 The Prism Project

Operations

Digital transformation isn't just front-facing. Employees from the C-suite to the mailroom, as well as third-party contractors and service providers, are all individuals with their own valuable identity elements. If any of these individuals engage with connected technologies—even something as run-of-the-mill as email—their privacy must be protected. Indeed, many historic biometric privacy lawsuits have been instigated by employees against their employers for failing to gain the proper consent for collecting their data or leaving it vulnerable. Employees who handle customer and third-party identity elements as part of their jobs are also responsible for their protection. This is routine for human resources, contract, and logistics professionals, and commonly arises in manual identity verification channels used for onboarding and account recovery. These processes themselves are resource-intensive, let alone the need to keep every employee's privacy training up to date.

New solutions from Prism Refractors like Anonybit and Luminaries like Keyless automate account recovery while minimizing or even eliminating the potential exposure of identity elements.

Biometric digital identity technology is a key operational advantage in this regard, thanks to a decade of innovation in striking a balance between convenience, security, and compliance. New solutions from Prism Refractors like Anonybit and Luminaries like Keyless automate account recovery while minimizing or even eliminating the potential exposure of identity elements. This kind of secure automation is possible at every point in the identity lifecycle, including account recovery. That means greater efficiency with stronger privacy.

Regulations

The penalties for non-compliance are no joke. According to Fenegro, KYC and AML fines increased 417% year over year, globally, for the first half of 2025, amounting to $1.23 billion across 118 fines. GDPR is also having a record year, with social media giant TikTok incurring a €530 million fee, contributing to the excess of €5 billion in penalties racked up by the EU law since 2018.

KYC and AML fines increased 417% year over year, globally, for the first half of 2025, amounting to $1.23 billion across 118 fines, according to Fenegro.

With GDPR-inspired regulations emerging around the world and digital transformation enabling cross-border transactions between companies and citizens of different nationalities, the need for comprehensive compliance is rapidly increasing. And with each regulation carrying its own nuances, which evolve along with trends and technology, the only surefire solution is to

Prism Ver. 1.0 © 2025 The Prism Project

focus on the privacy contract at the heart of digital identity.

By implementing biometric digital identity that prioritizes user consent and minimizes the exposure of identity elements at every step of the customer journey, privacy can be built into the core of a business, making regulatory compliance a natural part of the process.

Data Management

The identity elements that are collected, processed, managed, and stored by relying parties need to be properly protected and handled. That is the bulk of what it means to protect user privacy and prioritize compliance. The nitty-gritty of how this is done can pose a challenge for many organizations, which need to ensure users have access to their PII so they can revise, delete, or easily and securely have it ported to another service. Inevitably, many relying parties resort to manually managing identity elements, opening the data in question to potential exposure or theft.

Biometric digital identity solutions—mobile ID and mDL technologies in particular—streamline these critically important data management processes by putting the ball in the end user's court. Bolstered by a system of record and secured on the edge device, these next-generation digital IDs empower individuals by putting them in control of their identity elements during day-to-day transactions. This ensures every transaction is centered on consent while limiting the exposure of sensitive identity elements.

Security

Compromised identity elements are a security liability in many contexts. Not only are centralized databases major targets for hackers, they cause a cascading IT security effect when compromised—nearly 70% of data breaches are caused by compromised credentials, according to Verizon. And digital channels aren't the only paths vulnerable to malicious actors. Physical data centers are vulnerable to insider threats, which (according to IBM) cost companies an average of $4.92 million per incident.

Physical data centers are vulnerable to insider threats, which cost companies an average of $4.92 million per incident, according to IBM.

Biometric digital identity technologies can secure the logical and physical access points that are exploited in data breaches. When grounded in foundational identity and supported by liveness and deepfake detection, biometrics secure digital access points using credentials that can't be phished, spoofed, or stolen. In the facilities that house the data, biometric physical security solutions can keep intruders out and maintain accurate audit records that discourage insider threats. In addition, hybrid

Prism Ver. 1.0 © 2025 The Prism Project

centralized/decentralized identity solutions provide assurance of system-of-record-based identity verification while limiting the exposure of identity elements for day-to-day transactions.

Fraud

Biographical and contextual identity elements can be stolen through social engineering techniques, like **phishing**, and those elements can, in turn, be used to commit even more fraud, minting synthetic identities, making scams more convincing, and contributing to the estimated 24 billion usernames and passwords available on the dark web. Beyond compliance penalties and reputational damage, these scams have expensive knock-on effects: phishing is now the leading cause of ransomware attacks, which are predicted to reach $57 billion in 2025.

PHISHING: a cybercrime in which attackers impersonate legitimate entities—like banks, companies, or government agencies—to steal sensitive information.

Decentralized biometric digital identity solutions are unphishable. This is true of the most high-tech decentralized server to the most basic passkey solution. By prioritizing the adoption of the solutions described in this report, relying parties will protect themselves from today's AI-empowered scammers while playing a significant role in mitigating the fraud crisis.

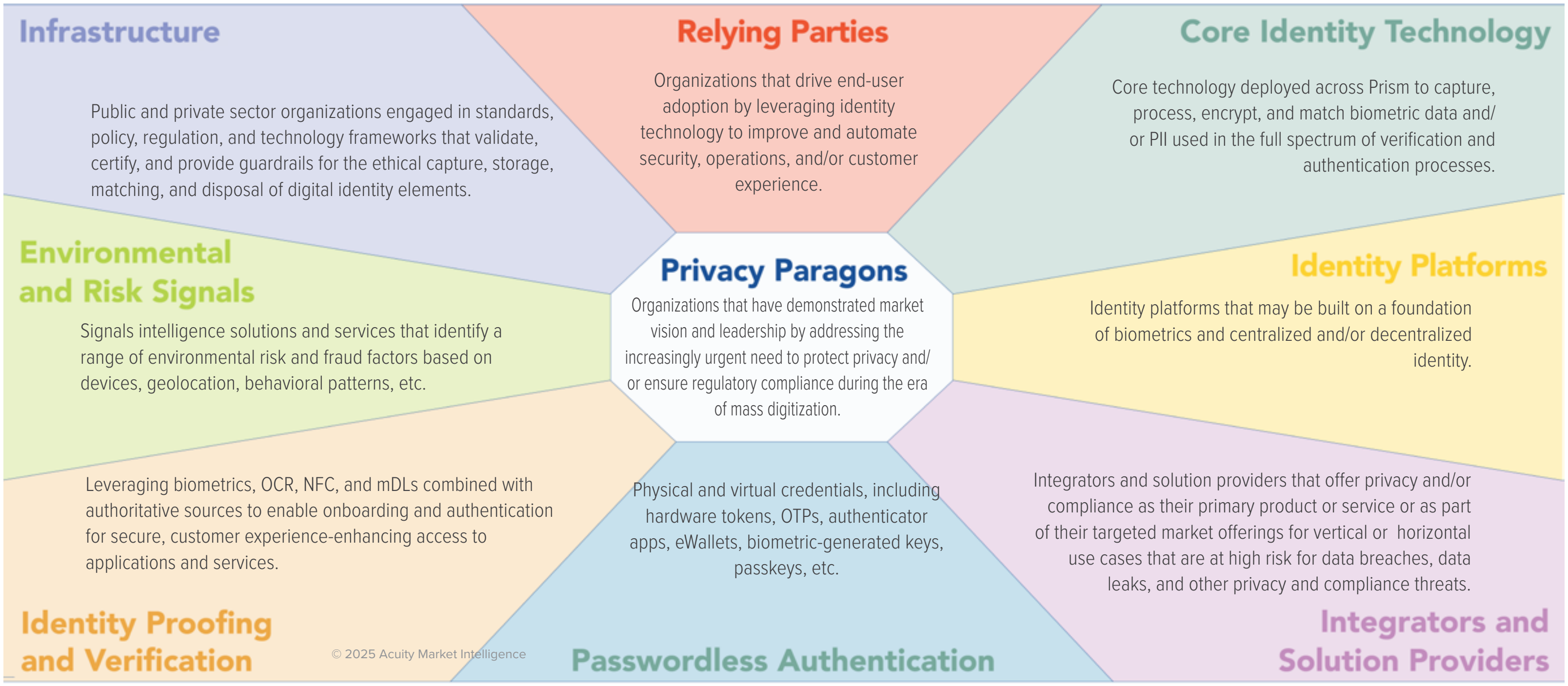
.

Prism Ver. 1.0 © 2025 The Prism Project

The Biometric Digital Identity Prism

Just as a beam of light contains all colors, the biometric digital identity ecosystem is comprised of many organizations contributing to the grand idea of digital identity. The Prism Project conceptualizes 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.

Biometric Digital Identity Privacy and Compliance Prism



Infrastructure

Public and private sector organizations engaged in standards, policy, regulation, and technology frameworks that validate, certify, and provide guardrails for the ethical capture, storage, matching, and disposal of digital identity elements.

Relying Parties

Organizations that drive end-user adoption by leveraging identity technology to improve and automate security, operations, and/or customer experience.

Core Identity Technology

Core technology deployed across Prism to capture, process, encrypt, and match biometric data and/or PII used in the full spectrum of verification and authentication processes.

Environmental and Risk Signals

Signals intelligence solutions and services that identify a range of environmental risk and fraud factors based on devices, geolocation, behavioral patterns, etc.

Privacy Paragons

Organizations that have demonstrated market vision and leadership by addressing the increasingly urgent need to protect privacy and/or ensure regulatory compliance during the era of mass digitization.

Identity Platforms

Identity platforms that may be built on a foundation of biometrics and centralized and/or decentralized identity.

Identity Proofing and Verification

Leveraging biometrics, OCR, NFC, and mDLs combined with authoritative sources to enable onboarding and authentication for secure, customer experience-enhancing access to applications and services.

Passwordless Authentication

Physical and virtual credentials, including hardware tokens, OTPs, authenticator apps, eWallets, biometric-generated keys, passkeys, etc.

Integrators and Solution Providers

Integrators and solution providers that offer privacy and/or compliance as their primary product or service or as part of their targeted market offerings for vertical or horizontal use cases that are at high risk for data breaches, data leaks, and other privacy and compliance threats.

© 2025 Acuity Market Intelligence

Organizations are positioned in one of nine Prism Beams. Each beam representing a critical component of the biometric digital identity landscape. For some organizations, it can be challenging to select one beam that represents their singular position in the marketplace. Many appear to span multiple beams. In these cases, we have selected the beam that most accurately reflects the breadth and depth of their product and service offerings and is most closely aligned with their unique differentiators. Organizations with profiles will see their penetration across multiple beams represented in our Luminosity Graphs (see more below).

How to Read the Prism

Within each beam, there are three evaluation categories: Pulsars, Catalysts, and Luminaries.

Pulsar

Pulsars are the bright upstarts and pivoting legacy vendors prioritizing the crucial elements of biometric digital identity. Startups with promising technology or established names with a proven aptitude for adapting to the new identity ecosystem, Pulsars have strong potential to influence the Prism landscape.

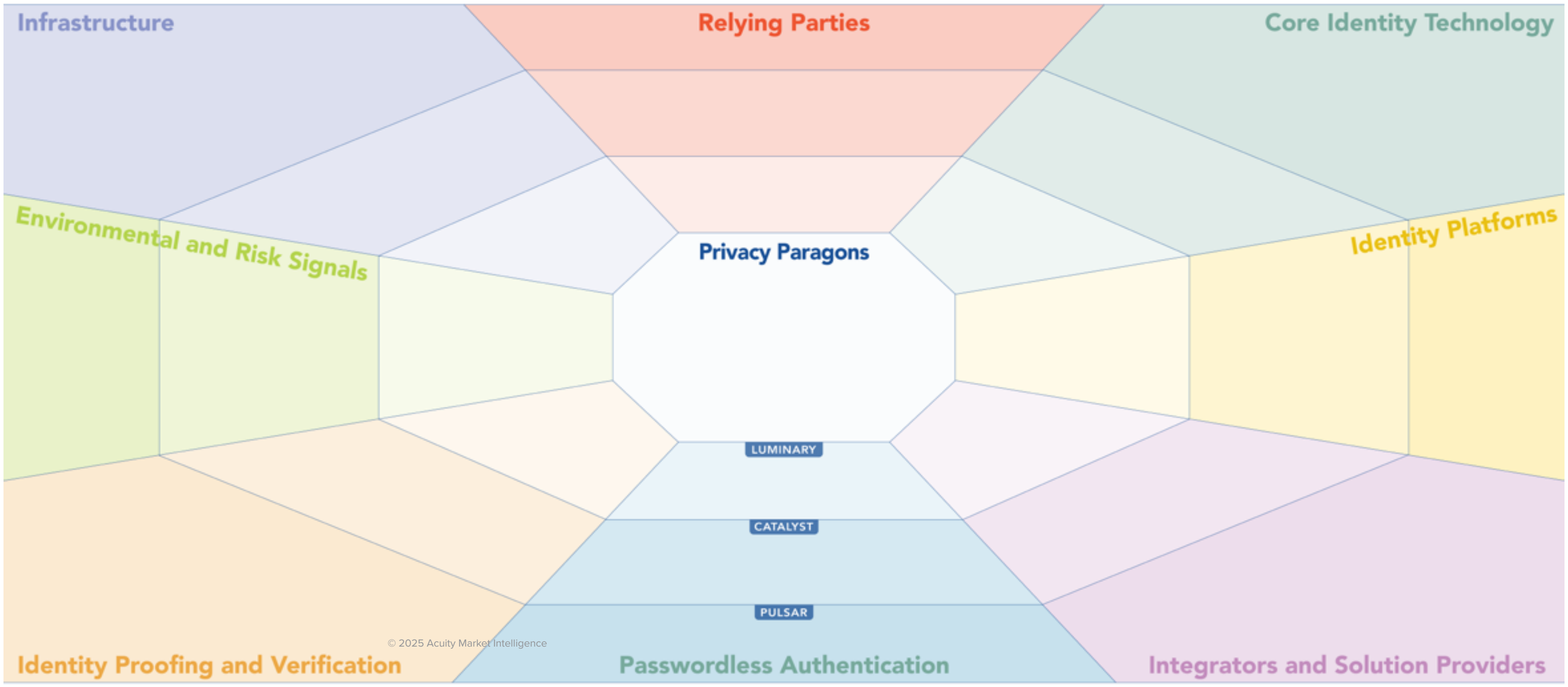
Catalyst

Catalysts are established disruptors, innovators, and agents of acceleration. With high proficiency in certain areas of assessment, Catalysts are often one step away from ascending to Luminary status, whether it's through an acquisition, a technological innovation, or an injection of resources.

Luminary

Luminaries 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.

Biometric Digital Identity Privacy and Compliance Prism



Infrastructure
Relying Parties
Core Identity Technology
Environmental and Risk Signals
Privacy Paragons
Identity Platforms
LUMINARY
CATALYST
PULSAR
© 2025 Acuity Market Intelligence
Identity Proofing and Verification
Passwordless Authentication
Integrators and Solution Providers

Refractors and Paragons

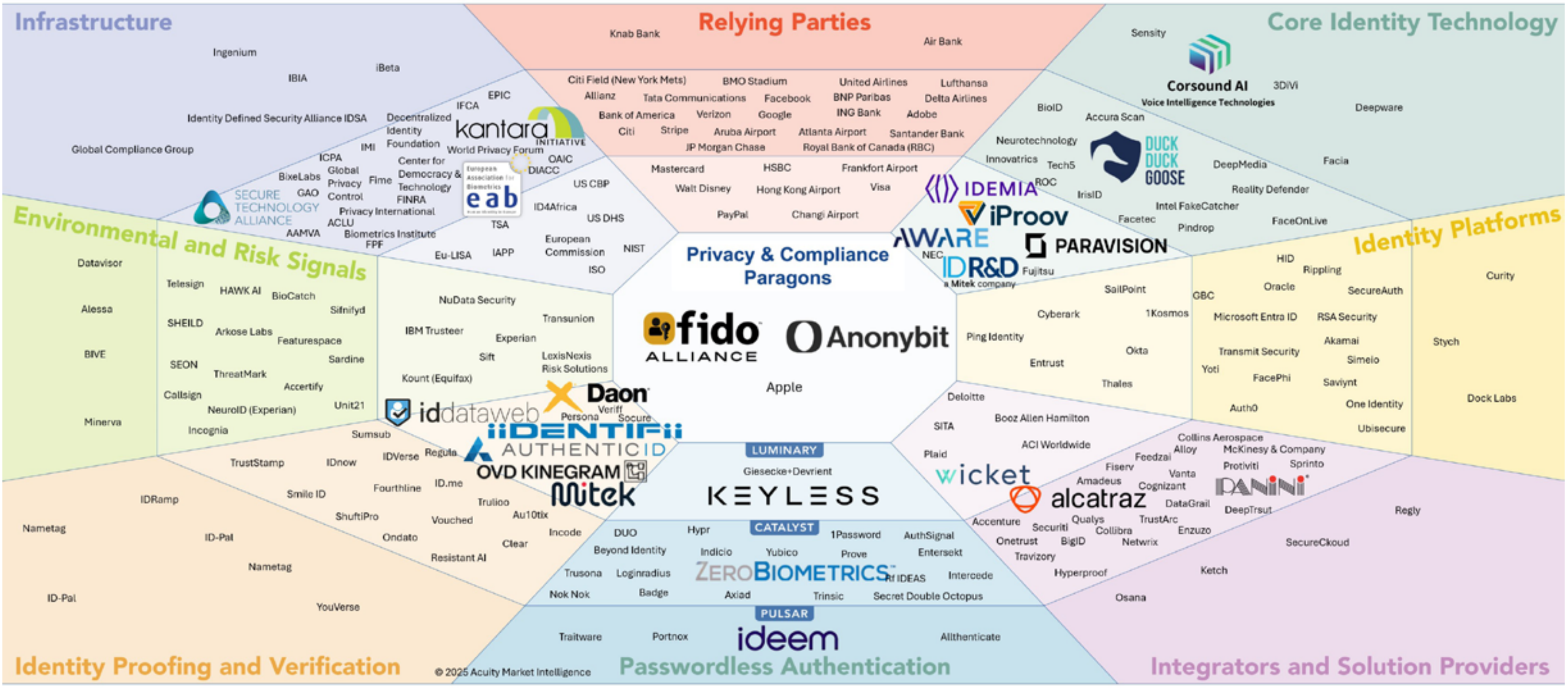
A special category anchors the center of the Prism—Refractors. In previous Prism reports, Refractor status was based on an organization's size, financial resources, global footprint, proven expertise, partner networks, and robust portfolio. These attributes gave them an outsized impact on the dynamics and evolution of the biometric digital identity market landscape. This role was defined as a Refractor, as it is through their initiatives that the industry is viewed.

For the Privacy and Compliance Prism, this definition has shifted somewhat. Regardless of size, revenue, global footprint, or other previous criteria, for this Prism landscape, the Refractor role has been assigned to Luminary class organizations whose vision and thought leadership—expressed through their ability to anticipate and take proactive steps to address the profound vulnerabilities and opportunities posed by privacy and compliance—distinguishes them as Privacy Paragons.

Prism Ver. 1.0 © 2025 The Prism Project

The 2025 Privacy and Compliance Prism Ecosystem

Privacy and Compliance Biometric Digital Identity Prism



© 2025 Acuity Market Intelligence

The Prism Project

Important Note on Prism Beams:

The Prism Beams and the classifications within represent important components of the emerging biometric digital identity landscape as it contends with deepfake and synthetic identity threats, and group organizations 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.

Prism Ver. 1.0 © 2025 The Prism Project

Evaluations & Profiles

In order to place organizations on the Biometric Digital Identity Prism, we assess the leading companies in each Prism Beam based on a proprietary evaluation scheme that includes six broad criteria.

- **Growth & Resources** – Current revenue, year-on-year growth, financial stability, and resources available to sustain and support ongoing growth.
- **Market Presence** – Overall geographic footprint and market sector penetration, as well as specific geographic regions and markets where a level of dominance has been achieved.
- **Proof Points** – Profile and size of overall and market sector customer base and key customers. Also includes 3rd party testing results and certifications and speed of implementation.
- **Unique Positioning** – Unique Value Proposition (UVP) along with differentiable technology and market innovation generally and within market sector.
- **Business Model & Strategy** – Overall marketing and sales positioning, messaging, and strategy as well as channel scope and quality and range of partnerships, channels, thought leadership, use of digital, social media presence, and engagement generally and within market sector.
- **Biometrics and Document Authentication** Capabilities– Depending on the market, solutions(s), specific beam, may be rated higher as proprietary or integrated technology.
- **Privacy & Compliance Leadership** – Demonstrated vision, action, and commitment to thought leadership concerning the urgent matter of privacy and compliance.

For the Infrastructure Beam, because of the special critical market supporting nature of these organizations, we replace Proof Points with Impact and Influence and we replace Biometric and Document Authentication Capabilities with Commitment to Biometrics.

- **Impact and Influence—**Effectiveness of an organization's ability to guide standards, regulations, policy, and industry best practices through its initiatives and thought leadership.
- **Commitment to Biometrics—**Evidence of long-term financial and cultural investment in biometrics as a core identity technology, not only within a product portfolio, but conceptually at an industry level.

Prism Ver. 1.0 © 2025 The Prism Project

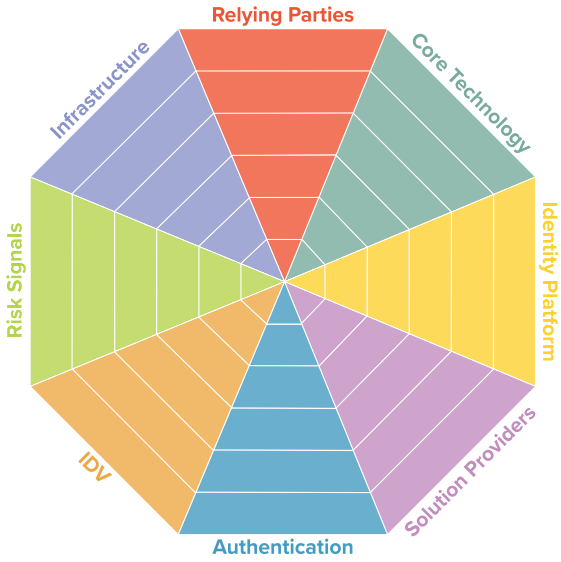
- We visualize this assessment as a Prism Evaluation Chart: an easy-to read graphic representation of an organization's current activity, resources, and abilities.

In 2025, the Prism Project has introduced a granular evaluation system represented with number grades on a scale of 0-6.

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Deepfakes & Synthetic Identity Leadership	Total	Average
VENDOR LOGO	5.50	5.33	5.17	5.50	5.33	3.00	6.00	35.83	5.12

Luminosity Graphs

New for 2025, Prism organization profiles include a Luminosity Graph—an illustration of the organization's penetration across all Prism Beams. The number of colored segments represents the proportional presence the organization has in the given segment of the overall biometric digital identity ecosystem (ie. the more teal colored segments a organization has, the more proof points it has in the Core Identity Technology Beam).



For reasons of spatial economy, we have abbreviated some of the corresponding beam titles as follows:

Relying Parties = Relying Parties

- Core Identity Technology = Core Technology
- Identity Platforms = Identity Platforms
- Integrators & Solution Providers = Solution Providers
- Passwordless Authentication = Authentication
- Identity Proofing & Verification = IDV
- Environmental Risk Signals = Risk Signals
- Infrastructure, Community, Culture = Infrastructure

Important Note on Evaluations and Prism Placement:

The evaluation metrics in this report are based on publicly available data, survey data, interviews, and confidential briefings. It is presented in good faith as a representation of the biometric digital identity ecosystem according to the values stated previously in this report. If you see your company here and have questions about your evaluation or placement within the Prism, please contact: info@the-prism-project.com.

Privacy Paragons

Organizations that have demonstrated market vision and leadership by addressing the increasingly urgent need to protect privacy and/or ensure regulatory compliance during the era of mass digitization.

Evaluations

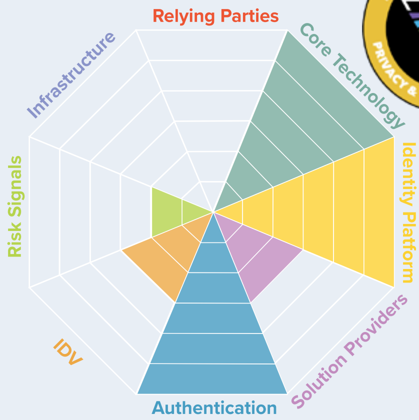
	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
Apple	5.67	5.83	5.17	5.83	5.67	4.67	6.00	38.83	5.55	Refractor
Anonybit	3.83	4.00	5.50	6.00	5.67	5.67	6.00	36.67	5.24	Refractor
fido ALLIANCE	5.75	5.50	5.83	5.67	5.50	5.83	6.00	40.08	5.73	Refractor

Anonybit

anonybit.io

BEAM: **Privacy Paragons** CLASSIFICATION: **Refractor**

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average
3.83	4.00	5.50	6.00	5.67	5.67	6.00	36.67	5.24



The position of Privacy Paragon in the Privacy and Compliance Prism is reserved for organizations that lead the industry through incisive thought leadership and bold innovation. No organization in the biometric-centric digital identity ecosystem personifies this achievement more than Anonybit. The company was established in 2018 by biometric industry stalwart Frances Zelazny, whose driving vision is based on 30 years of dedication to the foundational principle that the only reliable means of identifying humans in the digital world is via biometrics. Critical to bringing that vision into reality is eliminating the risk associated with centralized biometric data storage. From its targeted vision of privacy at the core, under Zelazny's zealous and indefatigable leadership, Anonybit has rapidly evolved into the industry's exemplar of a privacy-first biometric-centric digital identity platform.

Breaking New Ground By Breaking Up Identity Elements

Anonybit devised a genuinely novel approach to data storage: breaking up identity elements like biometrics into encrypted fragments (unsurprisingly called "Anonybits") and distributing them across a network. This patented method secures foundational identity while providing seamless life cycle compliance and reverence to the privacy contract between vendors, relying parties, and end-users across the entire identity hierarchy. Anonybits are never reconstructed when referenced, and because they are biometric in nature, clients never have to fall back to weaker authentication methods like PINs and OTPs for high-risk operations such as account recovery, closing what Zelazny refers to as the "Circle of Trust." The company's hybrid centralized/decentralized solution not only breaks down the identity elements but has also broken new ground in the industry by unassailably modeling how privacy can be built into biometric digital identity technology solutions at their core and at scale.

Fulfilling Your Identity Wishes

While its namesake refers to its unique approach to data storage, Anonybit's flagship product Genie solidifies foundational identity, securing the full user identity lifecycle from the onboarding process through every subsequent authentication and account recovery. Easy to deploy thanks to built-in integrations with enterprise platforms, Anonybit's technology supports all biometric modalities and clocks impressive speeds, performing 1:1 matching in under 200 milliseconds and 10 million 1:N searches in a split second. Supported by the Prism Refractor's decentralized biometric cloud and decentralized data vault, user data is immune to exposure through each of these transactions, making it seamlessly compliant with even the most stringent privacy regulations. After all, relying parties using Anonybit solutions aren't processing comprehensible identity elements—they're handling encrypted fragments.

Securing Banks and Enshrining Privacy

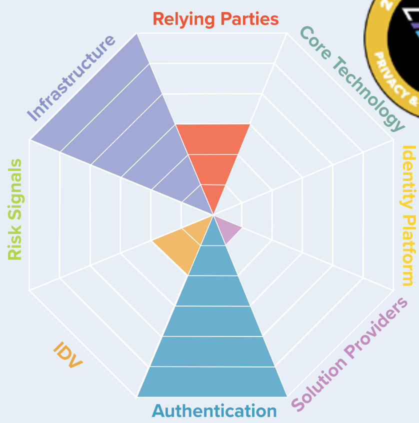
Based in Latin America, ADO Technologies is an identity solutions provider serving Tier 1 banks. As data breaches became increasingly common, and as countries in the region began adapting their privacy laws to harmonize with post-GDPR trends, the company saw a need to bolster their security. But ADO Technologies powers millions of transactions every day, so their solution needed to be frictionless, secure, and privacy-enhancing. The identity provider partnered with Anonybit, enabling a rapid and seamless integration on their terms—ADO could use its own biometric algorithms while deploying Anoybit's decentralized biometric cloud architecture. This gave ADO the ability to perform deduplication and synthetic identity defense at scale using Anonybit's powerful 1:N search and its customers benefitted from the privacy and security of the most innovative decentralized identity technology on the market. ADO saw a 99% reduction in fraud and improved regulatory compliance, all while enhancing customer experience and building trust. This application of privacy-enhancing security at every level of the identity hierarchy demonstrates Anonybit's dedication to protecting user data now while it pioneers a safer digital tomorrow.

Contact Anonybit: info@anonybit.io

fidoalliance.org

BEAM: **Privacy Paragons** CLASSIFICATION: **Refractor**

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacu & Compliance Leadership	Total	Average
5.75	5.50	5.83	5.67	5.50	5.83	6.00	40.08	5.73



The FIDO Alliance has been a stalwart defender of user privacy, campaigning for the importance of decentralized security methods since its inception in 2013. An early advocate for storing and processing identity elements on edge devices, the Alliance was founded on a radical vision of mobile-first identity, pre-empting the mobile biometrics revolution sparked by Apple's Touch ID by a matter of months. An acronym for Fast Identity Online, FIDO advocated a privacy-first paradigm of public key cryptography-based authentication, evangelizing a call for the "death of passwords" that would allow users to move beyond knowledge-based authentication (KBA). Flash forward to 2025, and FIDO is the world's preeminent voice in the evolution away from passwords as the world actually takes tangible steps to reduce its dependence on protecting data with secrets.

Passwords: The Opposite of Privacy

While regulations police relying parties' handling of identity elements, there is really no greater threat to user privacy than the data breach. In 2025, that threat still comes down to one digital pain point: the password. According to Verizon, over two-thirds of all hacking-related breaches involve stolen credentials and, thanks to the rise of generative AI, the phishing scams used to harvest knowledge-based authenticators like passwords are flooding inboxes around the globe. A database is only as secure as its weakest link, so the sheer scalability of these attacks constitute a crisis for any organization that safeguards user PII with KBA. FIDO was founded to protect against this exact threat, and its most recent innovation is making a tangible mark.

The Key to Privacy

Passkeys are a practical and deployable alternative to traditional access controls. Already available to use in many enterprise and consumer use cases, there's a good chance you log into at least some of your accounts—at work or at home—with a passkey that allows users to sign in with device unlock features, including biometrics. And while this technology has entered the mainstream, adoption of phishing-proof security needs to approach ubiquity to stem the flow of vulnerable identity elements. That's why FIDO introduced the 2025 Passkey Pledge—a voluntary commitment for vendors and service providers to demonstrate measurable actions enabling the deployment, adoption, and use of passkeys. Signatories include tech giants like Google and Apple, universities and public agencies, household names like Ikea, and other Prism Luminaries. By bringing organizations together to hold each other accountable, the pledge is a tangible community effort to strengthen the foundation of strong authentication and uphold the privacy contract with users everywhere.

Adaptation in the Face of Evolution

The FIDO Alliance has been grounded in reality through more than a decade of strong authentication advocacy, providing protocols and frameworks for practical applications that reflect the current state of the industry. Throughout this time, it has consistently placed privacy at the forefront of its operations. Through its standards, initiatives, certifications, and commitment to a simply stated mission FIDO moves deliberately, adapting to the evolving needs of the identity industry, regulations, and the needs of everyone living in our digital world.

For a complete list of FIDO Alliance members, visit https://fidoalliance.org/members/

Contact FIDO Alliance: fidoalliance.org/contact

Relying Parties

Organizations that drive end-user adoption by leveraging identity technology to improve and automate security, operations, and/or customer experience.

Evaluations

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
Adobe	5.50	5.33	5.17	5.50	5.33	3.00	3.17	27.50	4.58	Catalyst
Air Bank	2.17	1.83	2.67	2.67	2.67	3.67	5.00	20.67	2.95	Pulsar
Allianz	4.83	5.00	4.33	4.33	3.83	2.33	4.17	24.00	4.00	Catalyst
Amazon	5.83	5.67	4.67	5.83	6.00	5.33	2.17	29.67	4.94	Catalyst
Aruba Airport	4.33	3.33	4.67	4.67	5.50	4.50	6.00	28.67	4.78	Catalyst
Atlanta Airport	5.67	5.67	5.50	5.50	5.17	3.33	3.67	28.83	4.81	Catalyst
Bank of America	5.83	5.67	4.50	5.50	4.67	1.83	3.67	25.83	4.31	Catalyst

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
BMO Stadium	4.67	4.17	4.00	3.50	3.67	2.33	2.50	20.17	3.36	Catalyst
BNP Paribas	5.33	5.67	4.17	4.50	3.83	2.50	4.83	25.50	4.25	Catalyst
Changi Airport	5.00	5.00	5.33	5.50	5.50	5.17	5.50	32.00	5.33	Luminary
Citi	5.83	5.83	4.50	5.17	4.67	3.00	4.50	27.67	4.61	Catalyst
Citi Field	4.67	4.17	4.00	3.50	3.67	2.33	1.00	18.67	3.11	Catalyst
Delta Airlines	3.83	4.50	3.67	4.67	5.00	2.67	5.17	25.67	4.28	Catalyst
Facebook	5.67	6.00	3.50	5.33	5.33	2.33	2.33	24.83	4.14	Catalyst
Frankfurt Airport	5.17	5.33	5.17	5.33	5.17	3.83	5.50	30.33	5.06	Luminary
Google	5.67	6.00	4.83	5.67	6.00	3.33	1.50	27.33	4.56	Catalyst
Hong Kong Airport	5.50	6.00	5.33	5.50	6.00	4.33	3.83	31.00	5.17	Luminary
HSBC	5.83	6.00	4.67	5.17	4.67	4.67	4.83	30.00	5.00	Luminary

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
ING Bank	4.83	5.00	4.17	4.50	3.83	5.00	4.83	27.33	4.56	Catalyst
JP Morgan Chase (Chase)	5.83	5.83	4.67	5.17	5.67	2.33	5.33	29.00	4.83	Catalyst
Knab Bank	2.17	2.00	2.50	2.67	2.67	3.50	5.00	20.50	2.93	Pulsar
Lufthansa	3.83	4.50	3.83	4.00	3.83	2.17	5.33	23.67	3.94	Catalyst
Mastercard	5.83	6.00	4.83	5.50	5.83	3.00	4.83	30.00	5.00	Luminary
PayPal	5.83	5.67	5.17	5.83	5.83	5.00	4.50	32.00	5.33	Luminary
Royal Bank of Canada	4.83	5.00	4.67	4.83	4.67	5.50	5.00	29.67	4.94	Catalyst
Santander Bank	5.33	5.00	5.00	5.50	4.67	3.67	5.00	28.83	4.81	Catalyst
Stripe	4.17	4.50	4.67	4.33	4.83	5.00	4.67	28.00	4.67	Catalyst
Tata Communications	4.50	4.83	4.17	4.67	3.00	3.83	4.00	24.50	4.08	Catalyst
United Airlines	4.50	4.50	3.33	4.00	3.83	2.17	4.00	21.83	3.64	Catalyst

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
Verizon	4.83	5.00	4.00	4.67	4.00	3.67	4.83	26.17	4.36	Catalyst
Visa	5.83	6.00	4.67	5.33	5.67	4.67	5.17	31.50	5.25	Luminary
Walt Disney	5.67	6.00	5.67	6.00	5.00	2.83	4.83	30.33	5.06	Luminary

Core Identity Technology

Core technology deployed across Prism to capture, process, encrypt, and match biometric data and/or PII used in the full spectrum of verification and authentication processes.

Evaluations

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
3DiVi	1.33	1.33	2.17	1.17	1.33	2.83	3.33	13.50	1.93	Pulsar
Accura Scan	1.67	2.67	3.33	2.17	2.33	4.17	4.83	21.17	3.02	Catalyst
AWARE	4.00	4.33	5.50	5.17	5.50	6.00	6.00	36.50	5.21	Luminary
BioID	1.50	2.67	2.50	1.83	3.33	4.50	5.83	22.17	3.17	Catalyst
Corsound AI Voice Intelligence Technologies	1.67	1.17	3.33	4.50	2.67	3.00	2.50	18.83	2.69	Pulsar
DeepMedia	2.50	2.50	3.33	3.17	2.17	2.67	5.50	21.83	3.12	Catalyst
Deepware	1.17	1.00	1.67	2.00	1.50	0.33	5.50	13.17	1.88	Pulsar

Prism Ver. 1.0 © 2025 The Prism Project

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
DUCK DUCK GOOSE	2.17	1.67	3.83	4.50	4.17	3.83	4.33	24.50	3.50	Catalyst
FaceOnLive	1.67	1.83	3.33	2.67	3.33	4.83	4.83	22.50	3.21	Catalyst
Facetec	5.17	4.33	5.17	3.83	4.67	5.67	6.00	34.83	4.98	Catalyst
Facia	1.83	1.67	3.83	2.83	2.33	3.67	3.83	20.00	2.86	Pulsar
Fujitsu	5.17	5.00	5.50	4.17	5.00	4.50	5.83	35.17	5.02	Luminary
ID R&D a Mitek company	5.17	4.67	5.50	4.83	4.67	5.67	6.00	36.50	5.21	Luminary
IDEMIA	5.17	5.67	5.33	3.67	5.00	5.67	5.00	35.50	5.07	Luminary
Innovatrics	3.50	4.67	5.50	4.17	4.50	5.67	5.83	33.83	4.83	Catalyst
Intel FakeCatcher	5.00	3.00	4.17	4.00	3.00	2.33	5.83	27.33	3.90	Catalyst
iProov	4.50	4.50	5.00	5.67	5.33	5.00	6.00	36.00	5.14	Luminary
IrisID	4.50	4.33	5.17	4.50	4.83	5.67	5.67	34.67	4.95	Catalyst

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
NEC	4.67	5.00	5.67	4.33	5.17	6.00	6.00	36.83	5.26	Luminary
Neurotechnology	3.00	3.83	4.17	4.33	4.50	5.83	4.33	27.00	4.50	Catalyst
PARAVISION	3.50	4.50	5.33	5.33	5.17	5.17	6.00	35.00	5.00	Luminary
Pindrop	4.00	2.83	4.67	3.83	4.17	3.17	6.00	28.67	4.10	Catalyst
Reality Defender	2.50	1.67	3.50	3.00	2.83	2.83	6.00	22.33	3.19	Catalyst
ROC	4.17	3.67	5.17	5.67	4.67	5.50	5.83	34.67	4.95	Catalyst
sensity	1.17	1.83	2.67	2.83	1.67	2.67	6.00	18.83	2.69	Pulsar
Tech5	3.17	3.67	5.00	3.67	4.33	6.00	6.00	31.83	4.55	Catalyst

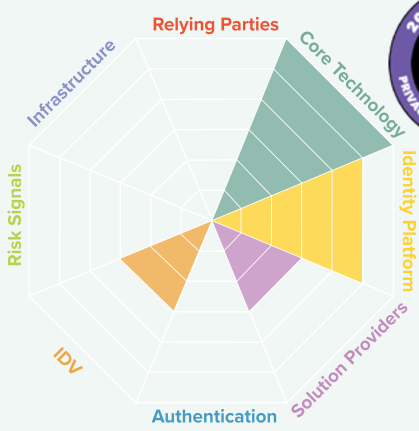
AWARE

aware.com

2025 LUMINARY PRIVACY & COMPLIANCE PRISM

BEAM: Core Identity Technology / CLASSIFICATION: Luminary

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average
4.00	4.33	5.50	5.17	5.50	6.00	6.00	36.50	5.21



Aware is synonymous with biometrics; a foundational technology pioneer whose innovations and advancements have guided the identity industry from its law enforcement roots, through the consumer-facing applications of the past decade, to the current moment of privacy-empowering identity solutions. Bolstered by new executive leadership, the company recently refocused its strategy on its greatest historical contributions to the biometrics industry: innovating core identity technology. Having played an integral role in the FBI's first large-scale fingerprint digitization effort over 30 years ago, Aware has been innovating identity in critical sectors for decades. With a science-forward design philosophy and a full portfolio of multimodal biometrics solutions bolstered by machine learning and liveness detection, achieving compliance and protecting privacy comes naturally with Aware—a quality fully realized by its Awareness platform. Configurable, flexible, and comprehensive, Awareness delivers biometric data management through every level of the identity hierarchy at scale.

As the regulatory landscape continues to evolve along with the steady march of digitization, countries on every continent are seeking to harmonize data privacy. These initiatives are directly influenced by the European Union's GDPR laws, to which Aware's solutions are fully compliant. Self-described as customer-obsessed, the company protects user privacy at all costs and promises compliance with all known data protection regulations while freeing clients from the risks of vendor lock-in. This comprehensive coverage is made possible through the company's end-to-end encryption, full data anonymization and image watermarking, and an unwavering dedication to consent and transparency. Of course, privacy protection is only as strong as its weakest link. Aware provides ironclad identity element defense with its full-spectrum approach—verifying user identity at onboarding and authenticating every subsequent transaction—backed by decades of research and proven innovation.

Contact Aware: sales@aware.com

Identity Platforms

Identity platforms that may be built on a foundation of biometrics and centralized and/or decentralized identity.

Evaluations

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
1Kosmos	5.00	4.67	5.33	3.83	4.50	5.67	6.00	35.00	5.00	Luminary
Akamai	5.67	5.67	4.00	3.00	4.00	1.00	4.83	22.50	3.75	Catalyst
Auth0	5.17	5.17	4.67	4.17	4.83	4.17	5.00	33.17	4.74	Catalyst
Curity	2.00	2.17	2.67	2.67	2.33	1.00	3.50	16.33	2.33	Pulsar
Cyberark	5.33	5.17	5.33	4.83	5.00	4.83	5.83	36.33	5.19	Luminary
Dock Labs	2.17	2.17	3.00	2.83	3.50	3.17	3.83	20.67	2.95	Pulsar
Entrust	5.33	4.67	5.00	4.67	5.17	5.83	6.00	36.67	5.24	Luminary

Prism Ver. 1.0 © 2025 The Prism Project

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
Facephi	4.50	3.83	4.50	3.67	4.17	5.83	4.83	26.83	4.47	Catalyst
GBG	4.67	5.00	5.17	4.33	5.33	5.00	4.83	34.33	4.90	Catalyst
HID	4.17	5.00	3.83	3.00	2.67	4.83	4.83	28.33	4.05	Catalyst
Microsoft Entra ID	5.50	5.17	5.00	5.00	5.50	3.67	4.17	34.00	4.86	Catalyst
Okta	5.33	4.67	4.67	4.83	5.67	5.00	5.00	35.17	5.02	Luminary
One Identity	4.00	3.50	4.17	3.33	4.67	1.50	3.83	25.00	3.57	Catalyst
Oracle	5.67	5.50	5.00	3.67	5.00	1.33	4.83	31.00	4.43	Catalyst
Ping Identity	5.00	5.50	5.50	5.00	5.83	5.00	5.83	37.67	5.38	Luminary
Rippling	5.00	4.00	4.83	4.00	5.17	1.33	3.83	28.17	4.02	Catalyst
RSA Security	3.83	4.50	4.00	3.83	4.17	2.83	5.00	28.17	4.02	Catalyst
SailPoint	5.83	5.00	4.83	4.33	5.83	4.33	5.83	36.00	5.14	Luminary

Prism Ver. 1.0 © 2025 The Prism Project

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
Saviynt	4.00	2.50	4.00	2.83	2.00	4.33	6.00	25.67	3.67	Catalyst
SecureAuth	3.50	2.33	3.83	3.17	4.17	2.83	3.50	23.33	3.33	Catalyst
Simeio	3.33	1.67	4.00	3.17	4.17	3.83	3.83	24.00	3.43	Catalyst
Stych	2.83	2.33	3.83	2.83	2.83	1.83	1.00	17.50	2.50	Pulsar
Thales	4.83	5.50	4.83	4.17	5.00	5.17	6.00	35.50	5.07	Luminary
Transmit Security	4.67	4.33	5.00	5.00	4.17	5.50	5.00	33.67	4.81	Catalyst
Ubisecure	2.67	2.50	3.17	2.50	2.83	3.67	5.83	23.17	3.31	Catalyst
Yoti	4.83	4.33	4.83	4.83	4.83	4.33	6.00	34.00	4.86	Catalyst

Prism Ver. 1.0 © 2025 The Prism Project

Integrators and Solution Providers

Integrators and solution providers that offer privacy and/or compliance as their primary product or service or as part of their targeted market offerings for vertical or horizontal use cases that are at high risk for data breaches, data leaks, and other privacy and compliance threats.

Evaluations

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
Accenture	5.17	5.50	4.67	4.00	5.00	4.67	5.83	34.83	4.98	Catalyst
ACI Worldwide	5.50	5.17	4.83	5.00	5.17	4.83	4.83	35.33	5.05	Luminary
alcatraz	3.83	3.83	5.33	5.17	5.33	5.17	5.33	34.00	4.86	Catalyst
Alloy	4.33	4.83	4.83	5.00	5.50	5.33	3.00	32.83	4.69	Catalyst
Amadeus	4.83	5.50	4.83	4.50	5.50	4.50	5.00	34.67	4.95	Catalyst
BigID	3.17	5.00	4.00	3.00	4.67	0.33	5.00	22.00	3.67	Catalyst
Booz Allen Hamilton	5.17	5.00	4.83	4.83	5.67	5.17	4.83	35.50	5.07	Luminary

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
Cognizant	5.67	5.67	4.50	3.00	5.17	1.33	3.83	23.50	3.92	Catalyst
Collibra	4.00	5.00	4.33	3.00	4.83	0.33	4.67	22.17	3.69	Catalyst
Collins Aerospace	5.00	4.83	4.67	3.67	4.50	4.83	3.83	31.33	4.48	Catalyst
DataGrail	4.00	5.00	4.00	3.00	5.00	0.33	4.00	21.33	3.56	Catalyst
DeepTrust	2.17	1.83	4.17	3.50	2.33	3.17	4.50	21.67	3.10	Catalyst
Deloitte	5.67	6.00	5.50	5.83	5.83	5.50	5.67	40.00	5.71	Luminary
Didomi	2.33	5.00	4.00	3.00	5.00	0.33	3.33	20.67	3.44	Catalyst
Enzuzo	1.17	5.00	4.00	3.00	5.00	0.17	2.00	19.17	3.19	Catalyst
Feedzai	4.17	4.83	4.67	5.33	5.50	4.83	5.00	34.33	4.90	Catalyst
Fiserv	5.33	5.33	4.50	5.00	5.00	4.50	4.83	34.50	4.93	Catalyst
Hyperproof	3.17	5.00	3.67	3.00	3.83	0.33	4.00	19.83	3.31	Catalyst

Prism Ver. 1.0 © 2025 The Prism Project

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
Ketch	2.33	3.50	2.67	3.00	3.00	0.33	4.00	16.50	2.75	Pulsar
McKinesy & Company	5.33	5.67	4.17	3.00	5.67	0.17	3.83	22.50	3.75	Catalyst
Netwrixx	3.67	5.00	3.67	3.00	4.00	0.33	3.83	19.83	3.31	Catalyst
Onetrust	5.17	5.67	5.33	3.00	6.00	0.83	6.00	26.83	4.47	Catalyst
Osana	2.33	5.00	2.50	3.00	3.00	0.33	3.00	16.83	2.81	Pulsar
PANiNi	3.50	3.67	4.17	3.67	3.33	4.00	2.00	24.33	3.48	Catalyst
Plaid	4.83	5.00	5.17	5.00	5.50	5.33	5.00	35.83	5.12	Luminary
Protiviti	4.83	5.00	4.50	3.00	5.67	0.33	4.00	22.50	3.75	Catalyst
Qualys	5.67	5.00	5.00	3.00	5.00	1.33	4.83	24.17	4.03	Catalyst
Regly	0.67	5.00	1.17	3.00	2.00	0.17	1.00	12.33	2.06	Pulsar
SecureCloud	2.33	5.00	2.50	3.00	3.00	0.33	2.00	15.83	2.64	Pulsar

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
Securiti	4.17	5.00	4.17	3.00	4.83	2.33	5.17	24.50	4.08	Catalyst
SITA	5.50	5.83	5.33	5.17	5.50	5.00	6.00	38.33	5.48	Luminary
Sprinto	2.50	5.00	2.67	3.00	5.00	0.33	4.83	20.83	3.47	Catalyst
Travizory	2.83	3.17	4.67	4.33	3.83	4.17	3.00	26.00	3.71	Catalyst
TrustArc	4.00	5.00	3.67	3.00	5.00	0.50	4.17	21.33	3.56	Catalyst
Vanta	3.67	5.00	5.00	3.00	5.00	0.50	4.83	23.33	3.89	Catalyst
wicket	4.50	5.00	5.33	5.17	5.67	4.50	5.00	35.17	5.02	Luminary

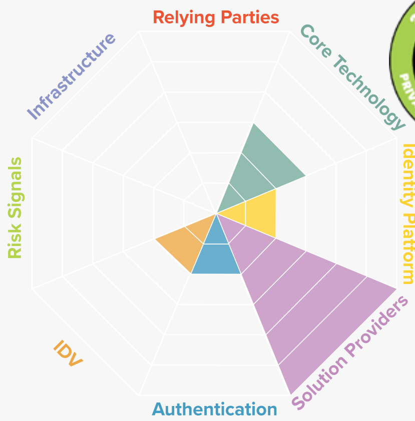
alcatraz

alcatraz.ai

2025 CATALYST PRIVACY & COMPLIANCE PRISM

BEAM: Integrators & Solution Providers / CLASSIFICATION: Catalyst

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average
3.83	3.83	5.33	5.17	5.33	5.17	5.33	34.00	4.86



Named for the famously impenetrable island, Prism Catalyst Alcatraz is locking up identity elements to protect privacy and secure compliance, demonstrating biometric excellence in the realm of physical access control. As physical and virtual worlds converge through digital transformation, sensitive data isn't just an online concern; it's also a brick-and-mortar challenge. Alcatraz's flagship product, the Rock, enables frictionless and secure physical access using non-identifying facial recognition technology. Rather than connecting biometrics to PII—a common practice in computer vision-based video security—the Rock only collects and processes badge IDs with its face templates. That means users' faces are only associated with the most basic information: whether they are allowed access to a facility. If a face scanned by the Rock matches the template associated with a badge ID, the door unlocks. If not, the door stays shut. This simple and effective approach to user-centric privacy ensures Alcatraz's customers comply with the most stringent regulations, including CCPA, GDPR, and BIPA, all while achieving the trifecta of access control: better security, less friction, and happier users.

Top-rated by NIST (National Institute of Standards and Technology) for one-to-many (1:N) identification, Alcatraz's Rock solution is compatible with existing access control and Video Management Systems (VMS). It's further reinforced by liveness detection to protect against presentation attacks in both enrollment and authentication scenarios, defending against crafty intruders and insider threats. And in addition to prioritizing privacy and compliance in its technology, Alcatraz literally protects the data centers that house high-value information in the real world. When Scott Data needed to replace the legacy security system it relied on for access to both its data center facility and three-storey office building in Omaha, Nebraska, it turned to Alcatraz. Scott Data's high-friction fingerprint access control system was nearing obsolescence—it encouraged tailgating, and the system-required badges were on backorder and becoming increasingly difficult to obtain. The Rock was deployed quickly, enabling the enrollment of hundreds of authorized users—including customers and contractors—in a matter of weeks, with each onboarding taking less than a minute. The results were immediate: a contactless, privacy-first biometric access control solution that streamlined security and eliminated tailgating while centering user privacy.

Contact Aclatraz: alcatraz.ai/contact

Passwordless Authenticators

Physical and virtual credentials, including hardware tokens, OTPs, authenticator apps, eWallets, biometric-generated keys, passkeys, etc.

Evaluations

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
1Password	4.50	4.67	4.83	4.83	4.33	2.67	5.33	31.17	4.45	Catalyst
Allthenticate	1.33	1.17	2.83	2.83	1.00	1.33	3.67	14.17	2.02	Pulsar
AuthSignal	3.83	3.33	5.17	5.17	5.00	4.00	4.00	30.50	4.36	Catalyst
Axiad	2.83	2.50	2.83	3.17	2.67	2.50	5.67	22.17	3.17	Catalyst
Badge	3.50	2.67	3.67	2.83	3.00	3.00	3.67	22.33	3.19	Catalyst
Beyond Identity	4.00	3.50	3.83	4.33	3.83	3.83	6.00	29.33	4.19	Catalyst
DUO	5.00	4.83	4.67	4.67	4.83	3.17	5.83	33.00	4.71	Catalyst

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
Entersekt	4.00	3.33	4.50	3.17	3.33	2.67	5.83	26.83	3.83	Catalyst
Giesecke+Devrient	5.33	5.00	5.17	4.83	4.50	5.67	6.00	36.50	5.21	Luminary
Hypr	4.17	3.33	4.67	4.17	4.50	5.17	6.00	32.00	4.57	Catalyst
ideem	2.00	2.17	2.83	2.50	2.00	3.00	3.67	18.17	2.60	Pulsar
Indicio	3.00	3.00	4.00	3.00	4.00	5.00	5.83	24.83	4.14	Catalyst
intercede	2.50	3.00	3.17	3.00	2.83	3.33	5.67	23.50	3.36	Catalyst
KEYLESS	4.50	4.67	5.50	5.00	5.33	5.17	5.83	36.00	5.14	Luminary
Loginradius	3.67	3.67	3.50	3.00	3.33	2.50	5.50	25.17	3.60	Catalyst
Nok Nok	2.83	3.33	3.50	3.17	3.00	0.83	6.00	22.67	3.24	Catalyst
Portnox	3.50	2.33	3.33	2.67	2.83	1.00	4.67	20.33	2.90	Pulsar
Prove	4.33	3.67	4.50	4.17	4.00	2.17	5.83	28.67	4.10	Catalyst

Prism Ver. 1.0 © 2025 The Prism Project

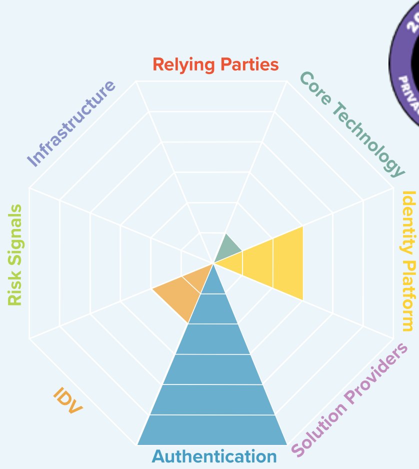
	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
rf IDEAS	4.17	3.17	3.83	3.00	3.33	3.17	4.00	24.67	3.52	Catalyst
Secret Double Octopus	2.50	2.33	3.50	2.67	2.50	2.00	5.67	21.17	3.02	Catalyst
Traitware	2.17	2.00	2.67	2.17	2.00	2.67	4.00	17.67	2.52	Pulsar
Trinsic	2.17	2.33	3.00	3.00	2.50	3.00	5.83	21.83	3.12	Catalyst
Trusona	2.83	3.17	3.50	3.33	3.00	3.67	6.00	25.50	3.64	Catalyst
Yubico	3.83	4.17	4.33	4.83	4.33	1.33	6.00	28.83	4.12	Catalyst
ZeroBiometrics™	2.33	2.33	3.00	3.33	2.50	3.83	5.83	23.17	3.31	Catalyst

KEYLESS keyless.io

BEAM: **Passwordless Authentication**

CLASSIFICATION: **Luminary**

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average
4.50	4.67	5.50	5.00	5.33	5.17	5.83	36.00	5.14



Thanks to its innovative use of biometric authentication, its proprietary approach to security, and its unwavering commitment to creating a safer and more private world, Keyless has achieved Luminary status as a Passwordless Authenticator on the Privacy and Compliance Prism. Combining facial biometrics with device possession, the company links a user and their device to those used at enrollment, enabling highly advanced multi-factor authentication.

Meanwhile, its patented Zero-Knowledge BiometricsTM technology transforms biometric data into a cryptographic representation that, when stored on the cloud, cannot be read by Keyless or the cloud service provider, and does not legally qualify as biometric data. When no Personally Identifiable Information (PII) is stored in centralized cloud repositories, there is nothing to be exposed in the event of a security incident.

Crypto is one of the most privacy-conscious markets in the world—so it's telling that Relai, an EU-based crypto wallet, chose Keyless as its solution to strict MFA requirements it needed to follow. Despite being a cloud-based system, Keyless was selected over methods that don't risk biometric data like FaceID or SMS OTPs because it provides the strongest security available without exposing PII. As an in-built multi-factor authentication solution that never stores biometric data—either on the cloud or the device—Keyless is able to provide the exclusive combination of security and privacy.

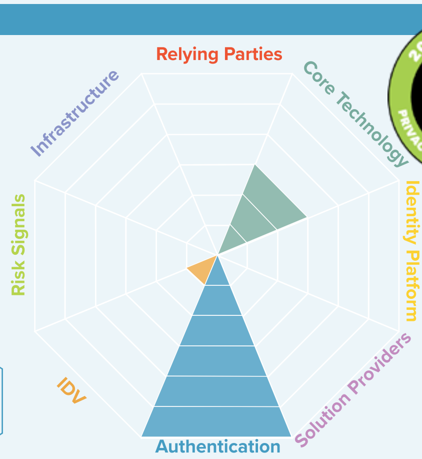
Contact Keyless: info.keyless.io

ZEROBIOMETRICS™ zerobiometrics.com

BEAM: **Passwordless Authentication**

CLASSIFICATION: **Catalyst**

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average
2.33	2.33	3.00	3.33	2.50	3.83	5.83	23.17	3.31



Singapore and Silicon Valley-based ZeroBiometrics has privacy encoded in its DNA. Pioneering a novel approach to biometrics and cryptography that asserts trusted identity without the need to store foundational, biographical, or contextual elements, ZeroBiometrics enshrines user privacy in the authentication process by eliminating the potential exposure of vulnerable identity elements. After all, a threat surface can't get smaller than zero. The company's patented technology relies on fast and accurate face biometrics to generate a unique on-demand IdentityKey™ for each individual at the time of authentication. This key only exists during a user's session—it is never stored and cannot be reverse-engineered—eliminating the possibility of a breach. And unlike other public key-based authentication solutions, ZeroBiometrics' digital identity technology is anchored in foundational identity, thanks to its ZeroFace™ solution that establishes proof of personhood.

In short, ZeroBiometrics eliminates the need to store and process identity elements and is the only solution that is ISO/IEC 30136 Compliant. This means that rather than comply with the increasingly stringent and constantly evolving data privacy regulations around the world, this Prism Catalyst is simply exempt from them. GDPR, CCPA, BIPA, and the next generation of emerging regulations they inspired don't apply when trusted biometric digital identity is never stored and remains effectively anonymous. So it's no surprise that this approach to identity is catching on. ZeroBiometrics' market launches in the US, Asia and Australia is bringing its vision of privacy-first biometrics into the world. And its new solution to add biometric trust anchors to Agentic AI agents demonstrates that its commitment to privacy-forward innovation is just beginning.

Contact ZeroBiometrics: zerobiometrics.com/contact-us/

Identity Proofing & Verification

Leveraging biometrics, OCR, NFC, and mDLs combined with authoritative sources to enable onboarding and authentication for secure, customer experience-enhancing access to applications and services.

Evaluations

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
Au10tix	3.67	3.33	4.33	3.83	4.33	5.67	5.67	30.83	4.40	Catalyst
AUTHENTICID	4.67	4.50	5.00	4.50	5.50	5.67	5.67	35.50	5.07	Luminary
Clear	3.67	3.67	4.50	3.67	4.50	4.83	3.83	28.67	4.10	Catalyst
Daon	4.50	4.83	5.50	4.67	5.33	5.83	5.67	36.33	5.19	Luminary
Fourthline	4.33	4.33	4.00	4.00	3.83	3.33	5.50	29.33	4.19	Catalyst
iddataweb	4.50	4.67	5.50	4.83	4.83	4.67	6.00	35.00	5.00	Luminary
ID.me	5.17	5.00	4.83	5.00	5.17	5.00	3.33	33.50	4.79	Catalyst

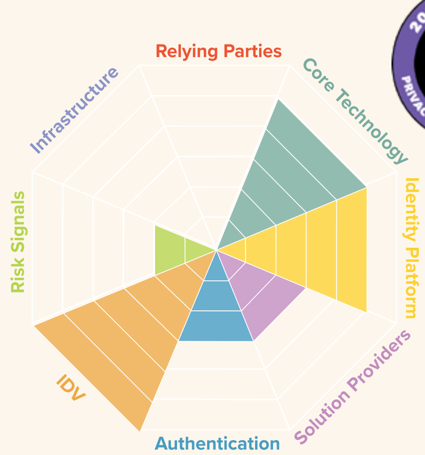
	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
IDnow	4.33	4.17	4.83	3.67	3.67	3.00	5.67	29.33	4.19	Catalyst
ID-Pal	1.33	2.00	3.00	2.33	2.33	4.50	4.50	20.00	2.86	Pulsar
IDRamp	1.00	1.33	2.67	3.17	2.33	5.00	4.00	19.50	2.79	Pulsar
IDVerse (LexisNexis)	4.33	3.83	4.83	4.50	5.50	5.50	6.00	34.50	4.93	Catalyst
iiDENTIFii	4.33	4.67	5.00	5.00	5.50	5.33	5.67	35.50	5.07	Luminary
incode	3.83	4.00	4.33	3.67	4.17	5.33	5.33	30.67	4.38	Catalyst
Mitek	4.50	5.17	5.00	4.33	5.00	5.67	5.67	35.33	5.05	Luminary
Nametag	1.67	1.33	3.00	1.50	1.33	5.00	3.83	17.67	2.52	Pulsar
Ondato	3.67	2.67	4.17	3.00	3.00	4.17	4.50	21.50	3.58	Catalyst
OVD KINEGRAM a KURZ company	5.17	4.50	4.83	4.50	5.00	5.33	5.67	35.00	5.00	Luminary
Persona	5.33	4.67	5.00	4.33	5.00	5.50	5.67	35.50	5.07	Luminary

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
Regula	5.17	5.00	4.83	4.50	4.50	5.33	5.83	35.17	5.02	Luminary
Resistant AI	3.00	1.67	3.33	3.17	2.67	3.00	4.83	21.67	3.10	Catalyst
ShuftiPro	3.17	3.00	3.50	3.00	2.83	4.67	5.00	25.17	3.60	Catalyst
Smile ID	3.00	3.83	4.00	3.67	2.83	4.67	4.83	26.83	3.83	Catalyst
Socure	5.67	5.17	5.33	5.67	6.00	5.00	6.00	38.83	5.55	Luminary
Sumsub	5.17	4.83	4.50	4.17	5.00	5.33	5.67	34.67	4.95	Catalyst
Trulioo	5.17	5.00	4.83	3.50	3.00	5.00	5.83	32.33	4.62	Catalyst
TrustStamp	3.00	3.00	4.00	3.00	4.00	5.17	4.67	23.83	3.97	Catalyst
Veriff	5.17	4.67	4.83	4.83	4.83	5.67	5.67	35.67	5.10	Luminary
Vouched	3.33	3.33	4.50	4.67	4.33	5.17	3.83	29.17	4.17	Catalyst
YouVerse	1.67	1.67	3.33	2.33	1.67	5.00	3.50	19.17	2.74	Pulsar

daon.com

BEAM: **Identity Proofing & Verification** / CLASSIFICATION: **Luminary**

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average
4.50	4.83	5.50	4.67	5.33	5.83	5.67	36.33	5.19



Securing 2 billion identities over six continents, Prism Luminary Daon is clocking more than 250 million daily authentications. Boasting over 285 global patents, which account for the processes and algorithms that power its platforms and applications, the Irish founded tech company has been securing identity since the dawn of the millennium. Those are impressive stats, but they also imply the collection and management of an immense amount of user data, which is a responsibility Daon takes seriously. With software-based biometric technology and an approach that uses public key cryptography, Daon's solutions improve user experience and engagement, reduce operational burdens and costs, and treat user privacy as paramount across sectors as varied as financial services, crypto, retail, telecom, healthcare, government, and travel and hospitality.

Say Goodbye to Silos

Identity silos—situations in which a variety of discrete implementations result in identity elements duplicated across databases—are a serious vulnerability when it comes to privacy and compliance. In addition to increasing the likelihood of this data being compromised in a breach, personal data scattered across multiple touch points becomes increasingly difficult to keep up to date in accordance with regulations. Daon has addressed these challenges with its concept of Identity Continuity, a type of user provenance based on a central identity that is woven through every transaction a customer has with a relying party: enrollment, subsequent authentications across all channels, and account recovery. By locking in one identity that's carried through an entire customer relationship, data is easier to manage and privacy remains protected.

Luxury-Class Facial Recognition For Privacy Protection

That continuous identity is facilitated by a full suite of biometric solutions, including luxury-class facial recognition. In September of 2025, Daon was ranked first in the National Institute of Standards and Technology's (NIST) Face Analysis Technology Evaluation (FATE) Quality test. Matched up against 56 other face biometrics technologies, Daon's algorithm—which filters out poor face images that typically cause errors to reduce false rejections and improve accuracy—came out on top in the 5% removal test. From a privacy and compliance standpoint, biometric accuracy plays a crucial role in both establishing digital identities on a foundational level and protecting biographical and contextual data with strong authentication supported by liveness detection.

Assurance, Consent, and Control On the Server

Daon's lauded facial recognition is featured in three of its core products: xAuth, a comprehensive multi-factor authentication portfolio; xProof, which matches biometrics against ID documents for identity verification and the establishment of foundational identity; and xFace, its highly secure face authentication technology. Deployed through an on-server method that prioritizes user consent, Daon's solutions store only the essential identity elements required for authentication. This gives relying parties control over their databases, allowing them to remain compliant with the increasing number of GDPR-inspired regulations emerging worldwide, while also truly respecting the privacy contract they have with their end-user community.

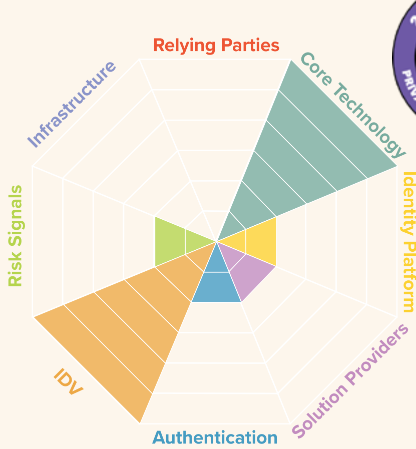
Contact Daon: daon.com/contact-us

miteksystems.com

2025 LUMINARY PRIVACY & COMPLIANCE PRISM

BEAM: **Identity Proofing & Verification** / CLASSIFICATION: **Luminary**

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average
4.50	5.17	5.00	4.33	5.00	5.67	5.67	35.33	5.05



Dedicated to innovation, collaboration, and customer experience, Prism Luminary Mitek empowers identity mainstays like Experian, Equifax, and Ping Identity to deliver privacy-enhancing and compliance-enabling solutions that fight fraud across the financial services, gaming, telecom, and marketplace sectors. Mitek was already an established industry standout in the document verification and fraud prevention space when it gave itself a biometric core technology and deepfake detection upgrade in 2021 with its acquisition of ID R&D. It further bolstered its technology and solutions portfolio by purchasing HooYu a year later, adding 3rd party signal orchestration and turn-key user verification journeys, allowing them to quickly become a leading market force in protecting identity elements with biometrics at the core.

Consolidated Identity Intelligence for User Risk Profiling

At the heart of Mitek's vision for digital transformation is the concept of layered identity verification, which it has realized through its flagship MiVIP solution. MiVIP—short for Mitek Verified Identity Platform—is a highly customizable solution that can facilitate KYC journeys, user onboarding, and anti-fraud protection with the use of AI, biometrics, and automated document validation. MiVIP streamlines the collection process of foundational, historical, and contextual identity elements, coalescing them into a single, trust-based view of personhood for online verification. This gives businesses the ability to dynamically adjust and control their verification journeys based on their own risk tolerances.

Collaborating on the Future of Compliance

As new mandates take hold in the EU and the UK—like Europe's EUDI regulation—Mitek is well-positioned to help businesses transition to the acceptance of eIDs and digital wallets. Mitek balances security and friction during an identity verification and that goes a long way toward helping businesses adapt to future regulatory requirements. Instead of juggling multiple vendors or patching together point solutions, MiVIP brings everything together under one roof—document validation, biometrics, liveness detection, and fraud intelligence—so organizations can keep the process frictionless for low-risk users and escalate protections only when they detect red flags. And with flexible integration options—from no-code to full API—companies can go live quickly and scale globally, prioritizing compliance without compromise.

Digital-First Customer Experience

On a fundamental level, online identity verification is tied to trust and security. And in an ever-changing regulatory ecosystem like financial services, that can be a high-stakes proposition that burdens the customer experience with undue friction. In 2019, when UK banking giant NatWest replaced its legacy identity verification system—a multistep process that took days to complete and involved visiting physical branches—with a real-time digital account opening process, it needed an agile compliance solution. Through its partnership with Mitek, the bank was able to deploy a wide range of identity verification technologies that enabled them to weed out fraud and protect consumers, all the while helping make good on its mission to improve customer experience. Secure, flexible, and compliant, Mitek offers a powerful trifecta in the digital age.

Contact Mitek Systems: miteksystems.com/contact

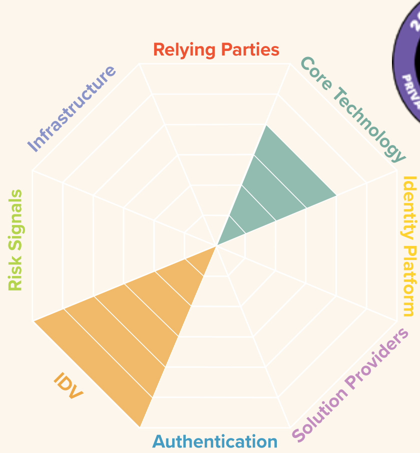
OVD KINEGRAM

a KURZ company

kinegram.com

BEAM: **Identity Proofing & Verification** / CLASSIFICATION: **Luminary**

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average
5.17	4.50	4.83	4.50	5.00	5.33	5.67	35.00	5.00



Nothing exemplifies physical embedded security innovation more than the evolution of the visual appearance of government issued documents and credentials like passports, national IDs, visas, driver's licenses, and money. This is the arena where OVD Kinegram minted its 40-year reputation for innovation influencing the design of everything from banknotes to travel credentials, most notably with its proprietary eponymous kinegram that provides a distinct visual layer of anti-fraud technology to genuine physical documents. This Switzerland-based Prism Luminary carries this tradition, its unique capabilities, and its reputation for excellence, forward into the digital transformation era, with software development kits (SDKs) that enable identity verification and authentication across a range of use cases spanning all layers of the Identity Hierarchy.

Identity in the Chip

True to its history as a document security specialist, OVD Kinegram's distinguishing innovation in the realm of digital identity is its ability to take full advantage of the security features embedded in passports, smart cards, and electronic machine-readable travel documents (eMRTD). Its MOBILE CHIP SDK solution enables an edge device like a smartphone to connect to the chip of a smart document and access the identity elements securely stored inside. This includes biometrics, foundational identity data, and biographical information. Combined with the company's MOBILE SCAN SDK and biometric matching, this allows for the highest level of remote identity proofing and verification.

Data Privacy on Customer Terms

Because OVD Kinegram's solution accesses identity elements securely stored on ID documents for the reference comparison step, it relies on a decentralized alternative to a traditional government system of record. This method supports the privacy contract between users and relying parties in two ways: by minimizing the exposure of valuable data and by promoting the highest level of document security for identity transactions, further normalizing its privacy-first design philosophy. Additionally, OVD Kinegram doesn't store data on an edge device, which merely acts as a connector between the document and the company's verification server. That server runs on a customer's premises and only processes data using RAM. That means the identity elements remain on the identity document they come from, ensuring compliance with stringent regulations.

Powering Privacy-first Partnerships

To see the broad scope of OVD Kinegram's application in the world of digital identity, just look to its neighbors. Swiss identity verification provider PXL Vision provides seamless, AI-powered IDV for financial services, healthcare, education, mobility, insurance, gaming, and more. As the privacy landscape evolved in its primary market, the EU, the company started facing increasing regulatory challenges that varied across verticals, some of which required NFC document data to be used in the identity proofing process. OVD Kinegram installed its solutions in an on-premises model, ensuring no user data was shared with third parties, allowing compliance while enshrining user privacy. Thanks to this privacy-enhancing partnership, PXL Vision will be using OVD Kinegram's technology to help onboard Swiss citizens to the country's upcoming eID program.

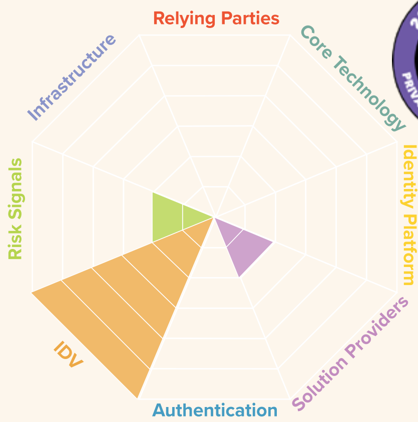
Contact OVD Kinegram: kinegram.com/contact

iddataweb

iddataweb.com

BEAM: **Identity Proofing & Verification** / CLASSIFICATION: **Luminary**

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average
4.50	4.67	5.50	4.83	4.83	4.67	6.00	35.00	5.00



Quick to deploy and integrate with existing identity verification workflows, this Prism Luminary brings together technology from over 70 attribute providers—many of which themselves are Prism Luminaries and Catalysts—to facilitate and defend the entire identity lifecycle. In an increasingly complex digital world beset by data breach threats and constantly evolving regulations, ID Dataweb excels by simplifying identity protection through its versatile orchestration toolkit and by enhancing user experiences, increasing operational efficiency, and boosting privacy. With provisions for contextual, biometric, and document-based identity elements—supporting IDs from more than 200 countries worldwide—ID Dataweb provides a comprehensive identity suite for highly regulated industries, including financial services, e-commerce, gaming, healthcare, aviation, insurance, and government applications.

KYC regulations are ubiquitous in the era of digital transformation. The first interaction between a customer and a relying party dictates the authenticity of every subsequent transaction, so due diligence is required. After all, acceptance of fraudulent identity elements on enrollment can have dire regulatory consequences. With ID Dataweb's advanced biometric verification—which compares an individual's face to their identity document and performs liveness detection—and its aforementioned real-time document authentication, its clients can transform what used to be a weeks-long onboarding process into one that takes only minutes. Add in real-time risk assessment of contextual identity elements and no-code deployments that take less than a day to implement, and ID Dataweb delivers immediate compliance you can trust, bolstered by exceptional security and user experience.

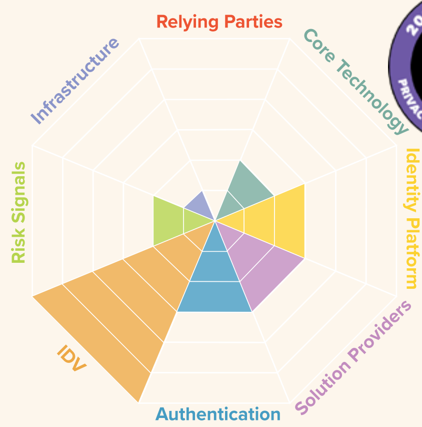
Contact ID Dataweb: sales@iddataweb.com

iiDENTIFii

iidentifii.com

BEAM: **Identity Proofing & Verification** / CLASSIFICATION: **Luminary**

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average
4.33	4.67	5.00	5.00	5.50	5.33	5.67	35.50	5.07



Founded in 2018 and headquartered in South Africa, Prism Luminary iiDENTIFi has rapidly embedded itself in the fabric of the region's identity infrastructure. Originally engaged by Standard Bank, the largest bank on the African continent, to address rising internal fraud challenges, iiDENTIFii has rapidly expanded its footprint across the African continent. Today, over 65% of South Africa's largest Tier 1 banks and one third of Africa's top 10 Tier 1 banks, along with leading African telcos, insurance companies, one of the world's largest resource companies, and key government departments serving the majority of South African citizens, all rely on iiDENTIFii's platform to safeguard their identity ecosystems.

Not only is this full-spectrum, Identity Hierarchy IDV player uniquely suited to address the infrastructure challenges common to many African markets — its built-in redundancies enable verification even in offline environments — it's fully automating KYC and AML processes reduce onboarding time and mitigate fraud at scale while enhancing compliance. iiDENTIFii meets rigorous global identity, security, and privacy standards, while its certifications ensure compliance, resilience, and trust across regulated sectors and African markets alike. As digital transformation cascades across the fastest population growth region in the world, this home-grown identity trailblazer has cemented its market-defining role in securing trust in the digital age by securing trust in African identities.

Contact iiDENTIFii: info@iidentifii.com

Environmental Risk Signals

Signals intelligence solutions and services that identify a range of environmental risk and fraud factors based on devices, geolocation, behavioral patterns, etc.

Evaluations

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
Accertify	5.50	4.17	4.33	4.50	4.17	2.67	4.67	30.00	4.29	Catalyst
Alessa	1.17	1.50	2.83	2.33	1.67	4.17	5.50	19.17	2.74	Pulsar
Arkose Labs	4.67	4.00	4.83	3.67	4.50	2.67	5.00	29.33	4.19	Catalyst
BioCatch	4.67	5.17	4.67	3.83	4.83	2.67	6.00	31.83	4.55	Catalyst
BIVE	2.50	2.83	2.83	2.83	2.83	3.17	1.33	18.33	2.62	Pulsar
Callsign	3.17	2.33	3.00	3.17	2.00	2.17	5.67	21.50	3.07	Catalyst
Datavisor	3.17	2.33	3.50	2.50	2.50	2.17	4.50	20.67	2.95	Pulsar

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
Experian	5.17	4.83	5.33	4.67	5.67	5.67	5.83	37.17	5.31	Luminary
Featurespace	4.67	4.00	4.83	3.67	4.50	2.67	6.00	30.33	4.33	Catalyst
HAWK AI	3.50	4.00	4.00	4.00	4.00	4.00	5.83	29.33	4.19	Catalyst
IBM Trusteer	4.33	5.00	5.00	5.00	5.00	5.00	5.67	35.00	5.00	Luminary
Incognia	4.17	4.00	4.00	5.00	4.00	2.00	5.83	29.00	4.14	Catalyst
Kount (Equifax)	4.67	5.00	5.00	5.00	5.00	4.67	5.67	35.00	5.00	Luminary
LexisNexis Risk Solutions	5.33	6.00	6.00	6.00	5.83	3.33	6.00	38.50	5.50	Luminary
Minerva	2.50	2.17	2.67	2.50	3.00	1.33	1.33	15.50	2.21	Pulsar
NeuroID (Experian)	3.33	4.00	4.00	4.00	4.00	4.00	5.83	29.17	4.17	Catalyst
NuData Security	4.67	5.00	5.00	5.00	5.00	5.00	6.00	35.67	5.10	Luminary
Sardine	4.83	4.00	4.50	3.33	4.50	5.33	5.83	32.33	4.62	Catalyst

Prism Ver. 1.0 © 2025 The Prism Project

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Privacy & Compliance Leadership	Total	Average	Beam Position
SEON	3.00	2.33	3.67	2.83	3.17	2.00	5.67	22.67	3.24	Catalyst
SHEILD	4.67	4.17	4.50	3.50	4.17	2.17	4.00	27.17	3.88	Catalyst
Sifnifyd	3.67	5.00	5.00	5.00	5.00	5.00	4.67	33.33	4.76	Catalyst
Sift	4.50	5.00	5.00	5.00	5.00	5.00	6.00	35.50	5.07	Luminary
Telesign	4.67	3.83	4.33	2.83	3.83	4.17	4.83	28.50	4.07	Catalyst
ThreatMark	3.50	4.00	4.00	4.00	4.00	4.00	5.67	29.17	4.17	Catalyst
Transunion	5.33	6.00	6.00	6.00	5.83	3.33	6.00	38.50	5.50	Luminary
Unit21	4.67	3.00	4.00	4.17	5.17	5.17	5.83	32.00	4.57	Catalyst

Infrastructure

Public and private sector organizations engaged in standards, policy, regulation, and technology frameworks that validate, certify, and provide guardrails for the ethical capture, storage, matching, and disposal of digital identity elements.

Evaluations

	Growth & Resources	Market Presence	Impact & Influence	Unique Positioning	Business Model & Strategy	Biometric Commitment	Privacy & Compliance Leadership	Total	Average	Beam Position
AAMVA	3.75	5.00	3.17	5.83	5.00	4.33	4.00	31.08	4.44	Catalyst
ACLU	4.75	5.17	4.67	4.00	5.83	1.83	5.67	31.92	4.56	Catalyst
Biometrics Institute	3.25	4.50	4.00	4.33	5.67	6.00	5.67	33.42	4.77	Catalyst
BixeLabs	1.50	2.83	0.83	4.50	1.33	5.17	4.83	21.00	3.00	Catalyst
Center for Democracy & Technology	4.00	4.00	3.67	5.00	5.33	1.83	5.67	29.50	4.21	Catalyst
Decentralized Identity Foundation	3.75	4.17	3.00	4.83	5.00	2.67	3.33	26.75	3.82	Catalyst
DIACC	3.25	4.33	3.83	5.50	5.67	4.33	5.50	32.42	4.63	Catalyst

	Growth & Resources	Market Presence	Impact & Influence	Unique Positioning	Business Model & Strategy	Biometric Commitment	Privacy & Compliance Leadership	Total	Average	Beam Position
European Association for Biometrics eab Human Identity in Europe	4.00	4.83	3.33	4.67	5.17	6.00	5.67	33.67	4.81	Catalyst
EPIC	3.00	3.83	3.00	4.83	5.17	2.00	5.83	27.67	3.95	Catalyst
eu-LISA	4.25	5.83	5.17	5.17	5.33	5.83	5.33	36.92	5.27	Luminary
European Commission	5.25	6.00	5.67	5.67	6.00	5.67	6.00	40.25	5.75	Luminary
Fime	4.50	4.67	5.00	5.00	5.00	0.33	4.50	29.00	4.14	Catalyst
FINRA	4.50	5.50	5.00	5.33	5.33	2.17	4.33	32.17	4.60	Catalyst
FPF	4.00	5.17	3.83	5.00	5.67	3.33	5.67	32.67	4.67	Catalyst
GAO	4.50	5.33	4.17	2.00	5.00	3.50	3.33	27.83	3.98	Catalyst
Global Compliance Group	1.75	1.17	1.17	5.33	1.67	1.00	1.83	13.92	1.99	Pulsar
Global Privacy Control	3.25	4.17	3.00	5.67	5.33	1.67	4.83	27.92	3.99	Catalyst
IAPP	5.25	6.00	5.67	5.67	6.00	4.50	6.00	39.08	5.58	Luminary

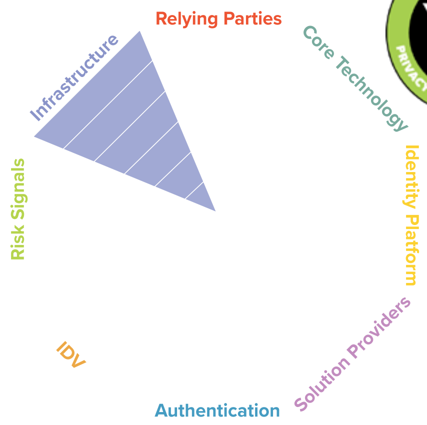
Prism Ver. 1.0 © 2025 The Prism Project

	Growth & Resources	Market Presence	Impact & Influence	Unique Positioning	Business Model & Strategy	Biometric Commitment	Privacy & Compliance Leadership	Total	Average	Beam Position
iBeta	1.50	3.60	2.83	2.83	2.17	4.67	3.17	20.77	2.97	Pulsar
IBIA	1.75	2.00	4.00	2.33	1.17	4.33	3.17	18.75	2.68	Pulsar
ICPA	3.25	3.67	2.33	4.00	3.50	1.17	5.33	23.25	3.32	Catalyst
ID4Africa	4.00	5.50	4.33	6.00	5.83	6.00	6.00	37.67	5.38	Luminary
IDSA	2.75	3.33	2.50	2.83	3.83	3.00	2.67	20.92	2.99	Pulsar
IFCA	4.00	4.83	3.50	4.00	4.67	2.00	4.50	27.50	3.93	Catalyst
IMI	3.25	3.67	2.17	4.00	3.50	3.83	3.67	24.08	3.44	Catalyst
Ingenium	2.00	1.00	0.83	2.00	1.33	3.83	2.50	13.50	1.93	Pulsar
ISO	5.00	6.00	6.00	5.83	6.00	5.83	5.83	40.50	5.79	Luminary
kantara INITIATIVE	3.75	3.67	3.50	4.17	4.00	5.33	6.00	30.42	4.35	Catalyst
NIST	5.00	5.83	5.67	6.00	6.00	6.00	6.00	40.50	5.79	Luminary

	Growth & Resources	Market Presence	Impact & Influence	Unique Positioning	Business Model & Strategy	Biometric Commitment	Privacy & Compliance Leadership	Total	Average	Beam Position
OAIC	5.00	5.83	5.67	6.00	6.00	6.00	6.00	40.50	5.79	Catalyst
Privacy International	3.25	4.50	3.50	5.67	6.00	3.33	5.83	32.08	4.58	Catalyst
SECURE TECHNOLOGY ALLIANCE	3.00	2.67	2.00	3.17	2.67	4.00	4.00	21.50	3.07	Catalyst
TSA	5.75	5.50	4.50	5.50	5.33	6.00	4.83	37.42	5.35	Luminary
US CBP	4.25	5.67	5.33	5.83	6.00	6.00	5.67	38.75	5.54	Luminary
US DHS	5.25	5.67	5.67	6.00	6.00	6.00	5.67	40.25	5.75	Luminary
World Privacy Forum	5.25	2.83	2.50	4.33	3.67	5.33	5.50	29.42	4.20	Catalyst

eab.org

BEAM: **Infrastructure** / CLASSIFICATION: **Catalyst**



Growth & Resources	Market Presence	Impact & Influence	Unique Positioning	Business Model & Strategy	Biometric Commitment	Privacy & Compliance Leadership	Total	Average
4.00	4.83	3.33	4.67	5.17	6.00	5.67	33.67	4.81

The European Association for Biometrics (EAB) is a non-profit, nonpartisan organization dedicated to addressing Europe's complex identity-related challenges. At a time when privacy and compliance present crucial challenges in digital identity, and digital and physical transactions are rapidly converging worldwide, regional leadership attuned to the nuances of culture and regulation is paramount. Given that the European Union is the birthplace of modern data privacy legislation, thanks to its pioneering GDPR law, that's a tall order when it comes to protecting and managing identity elements like biometrics, biographical information, and contextual metadata. Europe is a continent characterized by its cultural diversity and seamless trade and travel. In the era of digital transformation, this means identity elements are being traded regularly in physical and logical contexts, within countries and across borders. The EAB is positioned to guide relying parties, identity vendors, and European citizens to a privacy-forward and compliant future with biometrics at the core.

Mission-based Identity Leadership

Fairness, accessibility, security, and privacy are the digital identity goals promoted by the EAB, which fosters the responsible use of digital identity technologies through various tactics, including lectures, workshops, and working groups. Bringing together stakeholders in government, NGOs, special interest groups, academia, and the private sector—with members representing every beam and classification in the Biometric Digital Identity Prism—this Infrastructure Catalyst facilitates discussion, debate, networking, and other initiatives designed to advance modern digital identity for the good of Europe and its people. From deepfake defense to privacy protection, the Association is ensuring the right parties are ahead of the most crucial issues in identity.

The Platform For Discussion

EAB's holistic approach to forwarding privacy-enhancing biometric digital identity technologies is best served through multidisciplinary networking and discussion. It supports its membership and pursues its goals through the development of a coherent industry vision, the promotion of biometric deployments throughout the region, advocacy for the use of biometrics, and communicating with legislators and regulators. This all helps build a community within the EU united around the use of biometrics. That community comes together at the largest industry event on research funded by the European Union on the topic of biometrics and identity management, which the EAB organizes. The EAB Research Projects Conference exists to promote new research in the field, facilitate connections between its attendees from diverse backgrounds, and identify partners for possible future initiatives.

The World Capital of Data Privacy

Thanks to the global impact of GDPR, Europe is considered the world capital of data privacy, with its citizens being among the first people in the world to have fully articulated data privacy rights, including advanced provisions such as the right to be forgotten. And the laws are not static—as digital life continues to adapt to new media, technologies, and societal expectations, so do the regulations protecting identity elements belonging to EU residents. The most reliable way to stay on the right side of the law is to respect the privacy contract with end users. The EAB understands that this is best achieved with biometrics at the core, and is leading by example.

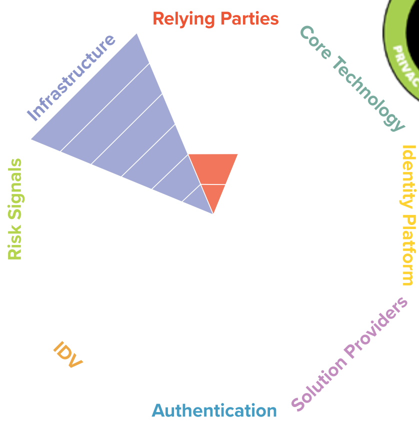
Contact EAB: secretariat@eab.org

kantara INITIATIVE

kantarainitiative.org

BEAM: **Infrastructure** / CLASSIFICATION: **Catalyst**

Growth & Resources	Market Presence	Impact & Influence	Unique Positioning	Business Model & Strategy	Biometric Commitment	Privacy & Compliance Leadership	Total	Average
3.75	3.67	3.50	4.17	4.00	5.33	6.00	30.42	4.35



2025 CATALYST PRIVACY & COMPLIANCE PRISM

The Kantara Initiative serves as a focal point for identity technology thought leadership and collaboration. Founded in 2009, Kantara is the only organization in the world able to assess identity solutions and services against NIST's 800-63 guidance for identity privacy and technology. Driven by its mission to improve the trustworthy use of identity and personal data, Kantara hosts discussion and work groups that bring together the brightest minds from within and beyond its organization to tackle the most pressing challenges in identity, from accessibility to AI-powered fraud threats to issues of privacy and mobility.

The Importance of Intent

While much of the privacy conversation around digital identity centers on preventing user data from falling into the hands of malicious actors, there are widespread concerns about otherwise trusted relying parties succumbing to the negligent and gross misuse of identity elements. Mission creep, convenience, carelessness, lack of policy—there are any number of reasons why organizations that process and store identity data may use it beyond the confines of their expressed and user-approved intention. And while some privacy guidelines and regulations are beginning to address this challenge, many existing standards lack the assurance that an individual's identity elements will be used solely for the fulfillment of the transactions to which they consented. That's why Kantara started the Privacy Enhancing Mobile Credentials (PEMC) working group—to create a set of requirements to help protect the privacy of mobile ID users—as well as the Biometric Data Discussion Group—to develop a set of recommendations and best practices for biometric data management that serve as practical guidance for use alongside existing standards.

Prism Beam Embodiment

The Infrastructure Beam plays an outsized role in the Biometric Digital Identity Prism ecosystem. That's thanks to the ubiquity of user privacy concerns, the involvement of numerous stakeholders, and the existential importance of privacy in ensuring the viability of converged physical/digital transactions. Catalysts like Kantara actively develop, deploy, and distribute thought leadership to its members and the broader identity community. They play an integral role in ensuring key industry players prioritize compliance, minimize data exposure, and empower users with technology that enhances their privacy. Beyond advising and informing the world on the evolving best practices for managing identity elements and achieving compliance, the organization puts its findings into practice, ensuring its own assessment program continues to guide relying parties and their customers on the path to privacy.

Noatable Members:

experian. facetec GakuNin GSA HINDLE CONSULTING ACUITY MARKET INTELLIGENCE

ID.me IDEMIA PUBLIC SECURITY IDENTOS IDmachines incode

Interac INTERNET2 JakobsenID deliver for stability / design for change Proof Patient Centric Solutions

iDPrivateid® Secours.ai SLANDALA Socure UNITED STATES POSTAL SERVICE

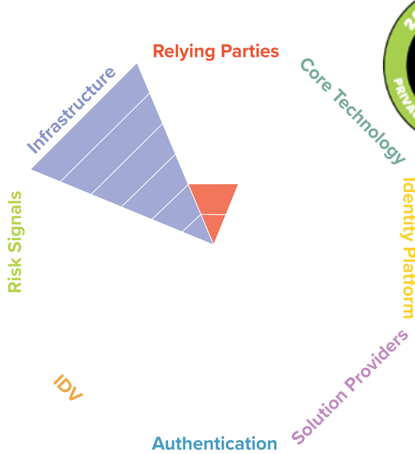
Contact The Kantara Initiative: hello@kantarainitiative.org

SECURE TECHNOLOGY ALLIANCE

securetechalliance.org

BEAM: **Infrastructure** / CLASSIFICATION: **Catalyst**

Growth & Resources	Market Presence	Impact & Influence	Unique Positioning	Business Model & Strategy	Biometric Commitment	Privacy & Compliance Leadership	Total	Average
3.00	2.67	2.00	3.17	2.67	4.00	4.00	21.50	3.07



2025 CATALYST
PRIVACY & COMPLIANCE PRISM

As the steady march of digitization uncovers new threats to user privacy, the Security Technology Alliance (STA) provides thought-leading advocacy for payment and secure identity technologies that keep users safe. A pioneer in the smart card revolution, STA was founded in 1993, facilitating adoption of the technology across industry sectors. Now, as it expands and develops its mission to educate and empower technology providers and ecosystem adopters to prioritize security, STA has become a major advocate for mobile driver's license (mDL) technology—a game-changing tool in the fight to put individuals in control of their digital identities.

The Anti-Surveillance Killer App

In many respects, the mDL is the full embodiment of the identity hierarchy, which is especially true from a privacy perspective. Rooted in foundational identity and government systems of record, the mobile driver's license ecosystem as advocated for by STA, puts users in control of their identity elements. Consent-first and pseudonymous by design, mDLs allow users to manage what data they share, with whom, and the terms of its use. While this powerful and novel technology has unfortunately been subject to misconceptions, true to its mission, STA has reliably demystified the myths and educated stakeholders on the functionality of mDL technology while remaining steadfast in its anti-surveillance posture.

Cross-Industry Infrastructure

Identity is for everyone, and that's why it is crucial for vendors and organizations tasked with the management and protection of identity elements to achieve industry-level velocity and collaborate. STA stands out as an Infrastructure Catalyst thanks to its inter-industry membership, enabling the kind of connections and collaborations required to ensure the companies with solutions are working together with parties on the front lines of protecting user privacy. Central to this cross-industry approach is the evolution of the Alliance itself, expanding beyond its initial flagship US Payments Forum to welcome its younger cousin, the Identity and Access Forum (IAF), which hosts the Jumpstart Committee, bringing together the stakeholders responsible for making privacy-enhancing and compliance-enabling mDLs a reality.

Identity & Access Forum Steering Committee Members:

AMERICAN EXPRESS · consult hyperion · cpi · CRYPTOMAThiC · Decipher.id · DISCOVER Global Network · fime

fiserv. · GET GROUP · HID · IDEMIA PUBLIC SECURITY · ID TECHNOLOGY · infineon · intercede

JCB · NextgenID · ST · THALES · VISA · XTec

For a complete list of STA members, visit https://www.securetechalliance.org/alliance-members/

Contact STA: info@securetechalliance.org

The Prismatic Future of Identity

Widespread digitization has opened the door to a secure and convenient future powered by biometric digital identity, but the resulting proliferation of identity elements runs the risk of eroding trust and violating the privacy rights of individual users. As data protection regulations around the globe strive for a type of worldwide harmony, it is imperative that relying parties prioritize the privacy of customers and employees. Through the adoption of technologies grounded in the foundational level of the Prism Identity Hierarchy, relying parties in all industries stand to significantly benefit from the biometric digital identity solutions explored in this report, keeping themselves on the right side of data privacy laws and doing their part inf ushering in the coming era of privacy-first identity.

The future of biometric digital identity demands:

- Easy and accessible onboarding that can bind human biometric identity to a system of record, establishing foundational identity, rejecting synthetic identities, and complying with shifting regulations.
- Strong authentication, bolstered with liveness and deepfake detection, that carries the trust from that foundational identity forward through every transaction including account recovery.
- A convenient end user experience meeting the evolving demands of citizens that doesn't come at the expense of trusted authentic identity.
- A hybrid centralized/decentralized paradigm of digital identity that puts users in control of their data, prioritizes consent, and functions in online and offline contexts.

Enterprise stakeholders have a multitude of biometric digital identity options to choose from. Those highlighted in this report are ready to deploy and contribute to the holistic ecosystem of trust required to prioritize privacy and compliance as digital and physical worlds converge. By choosing identity solutions designed with biometrics at the core, organizations the world over have the opportunity to contribute to a safer and more trustworthy tomorrow.

Prism Partners

The Prism Project is proud to collaborate with the following publication partners:

ID TECH

ID Tech is a leading online publication dedicated to the digital identity and biometrics industry. The platform provides daily news, in-depth articles, and expert thought leadership covering the latest trends, technologies, and regulatory updates in digital identity. Its content spans a broad range of topics, including government initiatives, private sector innovations, and the evolving landscape of biometric authentication and identity verification solutions. The site is recognized for its timely reporting and comprehensive coverage, making it a go-to resource for professionals, policymakers, and technology enthusiasts seeking to stay informed about advancements in identity management.

In addition to news updates, ID Tech features interviews with industry leaders, podcasts, and featured articles that offer insights into the practical applications and challenges of digital identity technologies. The platform also maintains a company directory, providing visibility to key players in the field. With a focus on thought leadership and expert commentary, ID Tech plays a crucial role in fostering dialogue and knowledge exchange within the identity technology ecosystem.

IDENTITYWEEK

GLOBAL • TRUSTED • VISIONARY

IdentityWeek is a leading online publication and news platform serving the global identity and security ecosystem. As the digital arm and sister publication to the renowned Identity Week series of events, it delivers breaking news, expert analysis, and in-depth features on the latest developments in digital identity, biometrics, secure credentials, verification, authentication, decentralized identity, and identity management. The platform

Prism Ver. 1.0 © 2025 The Prism Project

curates content for government, enterprise, and industry professionals, highlighting innovations, regulatory shifts, and emerging threats such as deepfakes and fraud. Its coverage is closely aligned with the work of the broader identity sector, reporting on how organizations authenticate and protect identities across physical, digital, and mobile domains.

IdentityWeek also acts as a community hub, supported by a bi-weekly newsletter and regular multimedia content, including interviews and short-form video insights from key stakeholders and industry experts. The publication's audience includes over 10,000 readers, reflecting its role as a trusted source of information and trend analysis for decision-makers and practitioners worldwide. In addition to news, IdentityWeek.net promotes and reports on its flagship global events-such as Identity Week Europe and Identity Week America-which offer networking, education, and business development opportunities for companies and professionals involved in identity verification, fraud prevention, and digital trust.

PEAK iDV

PEAK IDV is a media and enablement provider specializing in digital identity and identity verification (IDV). Founded in 2022 and led by industry veteran Steve Craig, the company offers media and expert advisory services to enterprise buyers, solution providers, and investors navigating the rapidly evolving digital trust landscape. PEAK IDV's media offerings include tailored enablement programs through their PEAK IDV ACADEMY. Additionally, its PEAK IDV LIVE virtual events create engaging and timely livestream content for the broader community featuring experts and in-depth coverage of topics such as artificial intelligence, authentication, biometrics, fraud prevention, and more.

PEAK IDV is also recognized for its thought leadership within the industry. The company produces the EXECUTIVE SERIES video podcast and newsletter, featuring interviews with innovators and CEOs, and covers merging topics like deepfakes and synthetic identity fraud. By combining deep market intelligence with community-driven learning, PEAK IDV positions itself as a trusted partner for organizations and investors seeking to navigate the complexities of digital identity, compliance, and fraud prevention in today's digital-first world.

KYC AML Guide is a specialized intelligence platform and consultancy focused on helping businesses navigate the complex landscape of Know Your Customer (KYC) and Anti-Money Laundering (AML) technology solutions. Headquartered in London with additional presence in Dubai and Milwaukee, the company operates at the intersection of compliance journalism, technology evaluation, and B2B matchmaking. KYC AML Guide assists financial institutions and new economy businesses in selecting the most suitable KYC solutions to streamline customer onboarding and identity verification processes. Their platform offers objective, data-driven vendor analysis—leveraging over 165 testing metrics and more than 100 deployment consultations—to ensure clients make informed decisions based on transparent and quantitative criteria.

Beyond consultancy, KYC AML Guide acts as a marketplace for compliance expertise, connecting organizations with seasoned KYC/AML professionals for short-term projects across industries and regions. Their services encompass a comprehensive suite of KYC and AML offerings, including biometric verification, document and age verification, eID, video KYC, PEP and sanctions screening, adverse media checks, and payment fraud prevention. The company is recognized for its rigorous and transparent methodology, as well as exclusive vendor performance ratings, positioning itself as a trusted partner for compliance-driven organizations seeking to reduce onboarding friction, enhance regulatory adherence, and stay ahead in the rapidly evolving RegTech space.

Prism Ver. 1.0 © 2025 The Prism Project

The Prism Project

Showing Identity in a New Light

The Prism Project arose organically out of a collaborative survey-based research project launched by Acuity Market Intelligence and FindBiometrics in late 2022. The intent of the Project is to use the proprietary Prism framework as the lens through which we continue to analyze and evaluate the rapidly evolving biometric digital identity industry as we help influencers and decision makers understand, innovate, and implement digital identity technologies.

Reports and Collaborations

In 2024, The Prism Project published four reports, primarily focused on biometric digital identity adoption in key vertical markets:

- The Financial Services Prism Report
- The Travel and Hospitality Prism Report
- The Government Services Prism Report
- The 2024 Flagship Prism Report

The Prism Project will publish, promote, and distribute three new reports in 2025, focusing on key applications of biometric digital identity, such as:

- Deepfake and Synthetic Identity Prism Report
- Privacy and Compliance Prism Report
- The 2025 Flagship Prism Report

Visit www.the-prism-project.com/prism-reports for more information.

Ongoing Collaboration and Sponsorship Opportunities.

The Prism Project is conducting on-going research and continuing to explore how biometric digital identity is being used today, where the roadblocks to adoption lie, what obstacles must be overcome to successfully deploy these technology solutions,

Prism Ver. 1.0 © 2025 The Prism Project

and where they are being used and by whom. We welcome collaborators and are open to discussing how your organization might benefit from and/or leverage the opportunities The Prism Project presents. To reach out, visit www.the-prism-project.com or email us at info@the-prism-project.com.

About the Author

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.

Strategic innovator, market visionary, and forecasting guru Maxine Most is the founding Principal of Acuity Market Intelligence (www.acuity-mi.com), a strategic research and analysis consultancy recognized as the definitive authority on global biometrics market development. Throughout her decades long career, Maxine has evangelized emerging technology on five continents. Since 2001, she has applied her unique ability to bring clarity to the unpredictable and volatile world of emerging technology to the rapidly evolving biometric and digital identity marketplace.

As an executive strategist, Maxine has earned a stellar reputation for innovative thought leadership by consistently providing unique, unvarnished, and reliable market insight while accurately anticipating biometric and digital identity market trends. Under her leadership, Acuity has provided strategic guidance to Global 1000s, established technology market leaders, start-ups, 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, is an active contributor to the Kantara Initiative, and presents

Prism Ver. 1.0 © 2025 The Prism Project the-prism-project.com

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.

Let The Prism Project be Your Guiding Light!

The Prism Project (www.the-prism-project.com)
The Prism Project is an innovative framework for understanding and evaluating the rapidly evolving biometric digital identity marketplace is **the only market model that is truly biometric-centric** based on the foundational conviction that in the age of digital transformation the only true, reliable link between humans and their digital data is biometrics.

Maxine Most
Principal, Acuity Market Intelligence
cmaxmost@acuity-mi.com
Founder, The Prism Project
cmaxmost@the-prism-project

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.

Prism Ver. 1.0 © 2025 The Prism Project