BIOMETRIC DIGITAL IDENTITY GOVERNMENT SERVICES PRISM REPORT

2024

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 Biometric Digital Identity Government Services Prism Report is made possible thanks to participation from our sponsors and partners. The biometric digital identity ecosystem depends on collaboration, and we are grateful to work with the following organizations.

SPONSORS

PARTNERS

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

Table of Contents

Introduction

Welcome to the **2024 Biometric Digital Identity Government Services Prism Report**—the third vertical market-focused publication from The Prism Project. Expanding on the findings in the 2023 Biometric Digital Identity Prism, this report collates the various identity industry forces at work in the government services space. The aim is to illuminate the complex and shifting ecosystem that keeps us transacting safely, privately, and conveniently in both the physical and virtual realms.

The Biometric Digital Identity Prism launched in 2023. Using original market research and easy-to-understand language, it serves to inform, educate, and motivate influencers and decision makers seeking identity solutions as they tackle the challenges of wide-scale digitization. A product of industry collaboration and ongoing research, The Prism Project uses a unique, proprietary framework to conceptualize biometric digital identity under the global conditions of digital transformation.

The initial deployment of the Prism framework revealed that the most viable vendors operating in the digital identity space had common traits and interacted in specific ways—cooperatively and competitively—with the brightest stars working together to enable highly orchestrated, secure, and convenient user experiences with baked-in privacy and ethics. The Prism Project distilled these characteristics into evaluation criteria based on a strategic philosophy:

- Digital identity belongs to the user it describes.
- True ID empowerment relies on government systems of record.
- Identity must be consistently and continuously orchestrated to remain secure.
- Biometrics must be at the core of any sustainable digital identity ecosystem.

On a fundamental level, government services fits perfectly within this Prismatic paradigm. The government sector plays a foundational role in establishing and validating citizen identities, making it both an integral piece of the biometric digital identity landscape and also a major market for vendors. Taking advantage of mobile biometrics, liveness detection, document validation, and trusted government records, digitized citizen identity has the potential

Government Services Relying Parties:

- Federal Governments
- State Governments
- Municipal Governments

Government Services Key Use Cases:

- Civil Identity
- Healthcare
- Social Services
- Elections
- Passports and Visas
- Border Control
- Immigration
- Internal Administration
- Emergency Services

to serve as the core identity form factor for users as they transact across all physical and digital spaces.

The government sector is defined by public participation and (somewhat obviously) politics. This is an area in which educating decision makers about the promise and reality of biometric digital identity is key to widescale adoption and use. Interoperability will also be crucial, as government issued digital IDs will need to be recognized and useable across jurisdictions by a wide range of devices.

The opportunity for biometric digital identity in government services is still largely untapped. A prismatic framework can help spur adoption.

In this report you will find:

- A holistic analysis of the government services industry framed around common pain points and the biometric solutions that can solve them.
- The Prism Identity Hierarchy: a visual representation of the 'biometrics at the core' concept, which is anchored by strong biometric digital identity at the government level.
- An original market forecast from Acuity Market Intelligence laying out the opportunity for biometric digital identity in government services.
- A government services version of the proprietary Biometric Digital Identity Prism.
- Evaluations of vendors operating at the intersection of biometric digital identity and government services.
- Case studies demonstrating biometric digital identity vendors solving real challenges for government services relying parties.

The result is a vision of government services that puts human beings first. By investing in biometric digital identity solutions like those identified in this document, government services stakeholders will find measurable benefits. But beyond the immediately tangible results, participating in the biometric digital identity ecosystem has a wider, global effect.

My collaborators and I are evangelists of strong identity and believe that the only way to safely move forward in our time of digital transformation is to take human identity seriously. By reading and sharing our vision of a secure, convenient, and privacy-first future of user-empowered identity, you are participating in the positive change required to level-up government

services, increase inclusion, and secure the future of identity all around the world.

Sincerely,

Maxine Most,
Founder
The Prism Project

Executive Summary

The Government Services Biometric Digital Identity Prism shifts the focus of the Prism Project's ongoing research to shine on the public sector. In doing so, it describes a powerful digital identity concept, **The Prism Identity Hierarchy**—a distillation and segmentation of the various relationships between human beings and their identity data, which depends on trusted issuing authorities like government agencies. The Prism Identity Hierarchy is key to realizing the transformative power of biometric digital identity as it relates to civic engagement and public services. And in order to understand this concept, we need to start with the effects of digital transformation on government organizations.

The market for biometric digital identity in government services is expected to grow at an overall CAGR of 39.2% from 2024-2028 generating just over $202.5 billion globally.

The Prism Project fielded surveys to government stakeholders from around the world to capture how digital transformation has impacted their operations, and how digital identity technology like biometrics factors into their respective digitization roadmaps. Cybersecurity concerns and legacy systems are cited as the most significant obstacles facing government services providers when it comes to their digital transformation, while customer demand, work from home, and financial factors like the threat of recession are spurring digitization efforts.

Two-thirds of survey respondents are actively seeking or deploying digital identity solutions, which they are confident can enable automation, protect against fraud, enhance user experience, and enable regulatory compliance. The highest uptake for biometric processes has so far been in customer and third-party authentication along with employee access control. Meanwhile, there seems to be resistance to digitizing the onboarding process for the citizen end user, with over 30% of respondents saying they are not considering customer onboarding on their digitization roadmaps.

Biometric digital identity is already being used for some identity related processes in government services, with agencies and organizations leveraging biometric technology for customer and third-party onboarding and authentication, as well as for employee time and attendance. That having been said, passwords and PINs are still used regularly throughout the entire identity lifecycle, along with non-biometric second factors like tokens, FOBs, cards, and SMS or mobile 2FA (two-factor authentication) codes.

Digital transformation is its own industry challenge for government services, thanks largely to the aforementioned legacy systems and cybersecurity worries. Inclusion is important too, with digitization promising higher levels of efficiency and reach but running the risk of leaving behind underserved populations who may not have access to the prerequisite technology like smartphones, computers, or internet connectivity. And inclusion is crucial—research from Eurofound, an EU agency for improving living and working conditions, shows that the level of political engagement is equal between rural and urban populations, but privileging one group over the other by means of access to easier experiences can erode trust in the government.

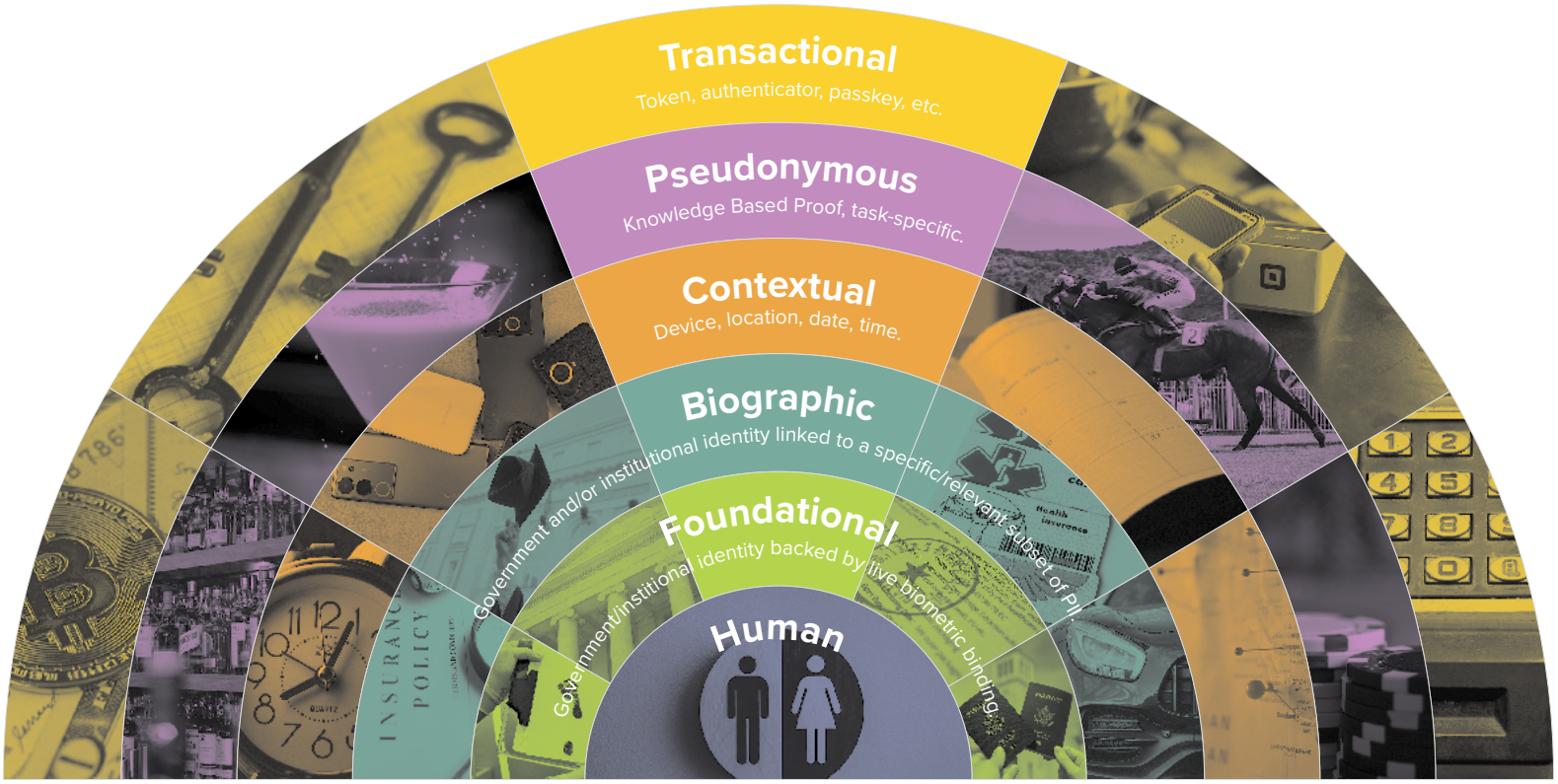
Two-thirds of surveyed government services stakeholders are actively seeking or deploying digital identity solutions.

Digitization has spawned data privacy and cybersecurity regulations across the globe. At the same time, it has opened up new possibilities both good (enhanced emergency services and better citizen end user experiences) and bad (fraud and data breaches). As such, government agencies are pulled in many different directions as they progress down their digital transformation paths. In one direction, they must comply with stringent regulations. In another direction, they must protect users from being victimized by hackers and fraudsters. And in yet another direction is the desire to achieve new levels of engagement and operational success with the rapid communications made possible through online channels.

Biometric digital identity is capable of addressing these challenges and seizing these opportunities. But it must be deployed in such a way that it provides the levels of assurance and trust required for both high and low-risk transactions while at the same time reassuring the user that they are not losing control of their identity. Thankfully, governments are in the ideal situation to succeed in this endeavor because of the role they play in the Identity Hierarchy.

The Prism Identity Hierarchy

The Prism Identity Hierarchy illustrates the six levels of identity: human, foundational, biographic, contextual, pseudonymous, and transactional.



The model shows each level radiating out from the human at the center of the hierarchy, representing how far removed a type of identity is from the carbon life form it represents. Crucially, while ascending the hierarchy, the human identity is carried forward from level to level. The same cannot be said from the top down. For each level to carry the assurance of a human being's true identity, that identity must stem from levels before it. For example: biographical identity can only be fully trusted as belonging to the human claiming it when it is built on the foundational identity underneath it, which is bound to the human through biometrics.

But what does that foundational biometric binding look like in practice? It only requires two elements: a human and a government issuing authority. The government is the arbiter of the most

authoritative and definitive identity data describing a document holder. But the credentials it issues, be they physical or digital, are still one step removed from the actual object of the identity (ie. the person it identifies). This becomes a serious problem when transacting over remote channels because the credentials and the information therein can be presented by impersonators by virtue of their transferability. By collecting and binding the credential holder's biometrics to the foundational identity credentials issued by the government, the cornerstone of identity is created.

That biometrically-bound foundational identity is the basis for the next two additive layers of the Hierarchy: biographical, based on what a person has done (where they have lived, what they have accomplished); and contextual, based on where they are and what they are doing now. These layers of the identity hierarchy build on the foundation of a government-vetted real human identity to give permissions like driving vehicles or accessing online portals, and to enhance assurance that the correct human is linked to this permission.

On the outer layers of the hierarchy, we see the privacy enhancing and practical aspects of identity. Unlike the layers underneath, the pseudonymous layer doesn't add data to build the identity up, but obscures what is there so that a person is only asserting the parts of their identity that they are required to complete a specific transaction. For age-restricted substances like alcohol or cannabis, or regulated services like gambling, pseudonymous identity represents the act of confirming you have permission to participate without having to share the actual information that proves it. Think of it as a government certified checkmark that says, "This person can buy wine, trust us."

The outermost layer, transactional identity, represents access. This is the identity of keys and locks, passwords and login pages, payments and purchases. In digital spaces, we are most familiar with transactional identity because, as the outer layer of the hierarchy, the actions it represents can be performed without the deeper layers of identity. That is to say: transactions can be performed without trust, security, or privacy. While that might be the case when using knowledge-based authentication or security tokens and passkeys that have no foundational element, when supported by the full identity hierarchy, transactional identity can be asserted with greater ease, benefit from stronger security, and be easily recovered.

With the full spectrum of the Prism Identity Hierarchy behind it, as enabled by government organizations and the infrastructure supporting them, biometric digital identity can meet the extremely wide ranging demands of this market.

Six Levels of the Prism Identity Hierarchy:

- Human
- Foundational
- Biographical
- Contextual
- Pseudonymous
- Transactional

Various form factors have emerged to bring the potential of the full spectrum of the identity hierarchy to fruition. The most common iteration is a government issued electronic or mobile ID, or a mobile drivers license (mDL), which places a biometrically bound, government attested digital identity on a user's smartphone. But recent innovations in biometric encoding technologies are giving rise to analog forms as well, like barcodes containing biometric templates, which can be printed on documents by issuers to add an element of biometric binding without requiring a mobile device. This type of innovation has powerful applications when it comes to including underserved populations in government services.

These biometric digital identity technologies require participation from identity platform players, biometric core tech vendors, solutions providers, integrators, identity proofing and verification players, as well as organizations that provide the infrastructure for their development, integrity, and adoption—all of which are set for worldwide growth in the coming years.

The Prism Project is powered by Acuity Market Intelligence (www.acuitymi.com), whose government services biometric digital identity market forecast shows a Total Addressable Market of approximately $295 billion between 2024 and 2028 globally, with Europe demonstrating the most potential. That's powered by a potential 6.4 trillion transactions in that same period, with Asia Pacific generating half of that potential traffic. About 57% of those transactions are expected to materialize in the 2023 and 2028 timeframe, generating an actual $202.5 billion in global revenue (representing 69% of the Total Addressable Market) spread relatively evenly between North America, Europe, and Asia Pacific.

Biometric digital Identity in government services is essential for the future of our digital civilization. Thanks to the role the government plays in creating a foundational identity, and the ability of digital identity technologies like the ones described in this report to bind that identity to the human it describes, this sector will define how other markets can leverage transactional and pseudonymous user identity for their own digitalized experiences. By coming into its role as an arbiter of identity, and working with the Solutions Titans, Luminaries, Catalysts, and Pulsars highlighted in this report, government agencies have the opportunity to protect their citizens from fraud and cyber threats while improving their own operations and invigorating the wider economy.

How to Read the Prism

The Government Services Biometric Digital Identity Prism Report is divided into six sections:

Digitization in Government Services

The first section collects and analyzes the results of a vertical market focused survey examining how government services stakeholders view biometric digital identity solutions in relation to their digital transformation journeys. **This high-level content is the starting point for the Biometric Digital Identity Government Services Prism.**

The Prism Lens (Challenges and Solutions)

The second section draws on aggregate government services industry research from leading analysts, government organizations, and NGOs, as well as trusted international news sources. It provides a holistic visualization of eight core government services challenges, then breaks them out individually to demonstrate how biometric digital identity can address them. The graphic visualization is supported by further written analysis. **The pain points highlighted in the Prism Lens serve as the basis for the practical applications of biometric digital identity technology profiled later in the report.**

Market Forcasts

The third section presents original proprietary market research from Acuity Market Intelligence, forecasting the global revenue and transaction volumes, broken down by region, for biometric digital identity in government services. **The charts provide insight into anticipated market growth based on existing and forecasted market adoption levels within the government services arena.**

The Prism

The fourth section is the proprietary biometric digital identity industry ecosystem framework: The Prism. This version of the Prism is specifically focused on the government services industry, depicting the various players that provide the solutions and initiative required to realize an identity-safe future of government. **The Prism is a living research**

program, subject to updates, showing a high-level view of how the biometric digital identity community is working together to fight fraud, improve UX, and empower people.

Evaluations and Case Studies

The fifth section lists the vendors depicted in the Prism framework next to their evaluations. Each vendor is evaluated in relation to the rest of the market and grouped according to its Prism Beam. After each set of evaluations, use cases are presented to demonstrate how the solutions offered by sponsors of this report can address the challenges identified in the Prism Lens section. **The evaluations and case studies demonstrate how biometric digital identity vendors currently operate in the government services sector.**

The Prismatic Future of Government

The sixth and final section contains strategic guidance and recommendations based on this report's research. It also contains author information, an overview of The Prism Project, and ways to get involved with future iterations of the Prism. **The conclusion will light your way to the next steps on your digital identity roadmap.**

Each section can be taken on its own, but together they offer a full picture of the current state of identity in government services and the massive potential for its biometrics-enabled future.

Digital Transformation and Identity in Government Services

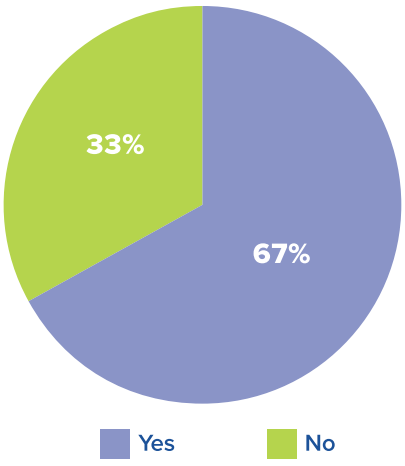
The Prism Project emerged from survey data comparing how biometric digital identity vendors' perception about identity's role in digital transformation lined up with the experience and views of of end users in vertical markets. Enhancing customer service, reducing fraud, and creating operational efficiency were identified as main adoption priorities in both segments, and data showed a prevailing support of converged physical and digital access. At large, we found biometric digital identity was moving from a paradigm of application-based point solutions to a holistic concept based on human users navigating digital spaces with a single ID.

For 2024, we directly surveyed government services professionals with digital identity expertise.

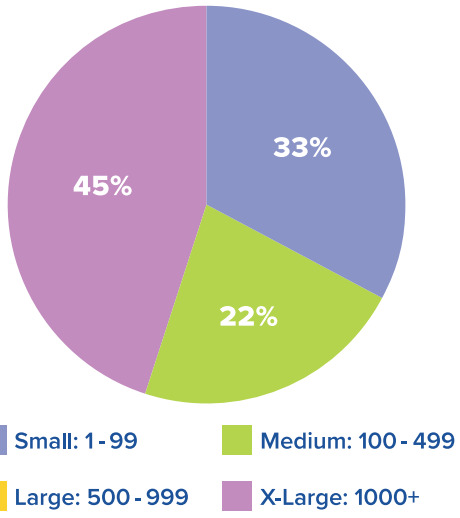
Survey Scope

The Government Services Prism Survey reached organizations of varying sizes, the majority composed of more than 1000 employees. Two-thirds of the respondents are actively seeking or deploying biometric solutions.

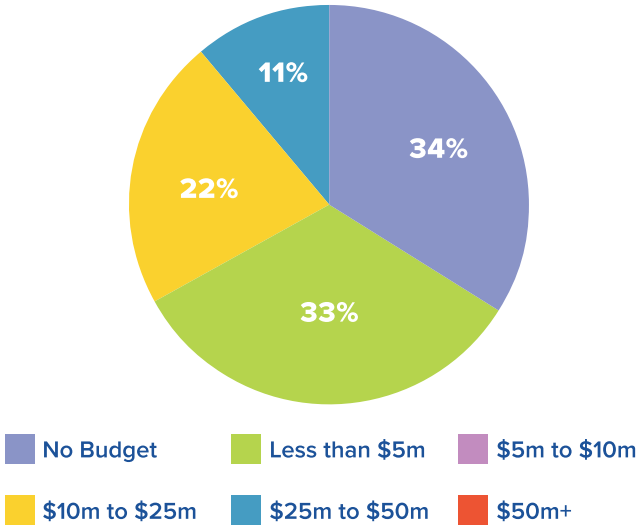
Are you actively seeking or deploying digital identity solutions?



How big is your organization?



What is your approximate budget (in USD) for digital transformation projects for 2024 and 2025?

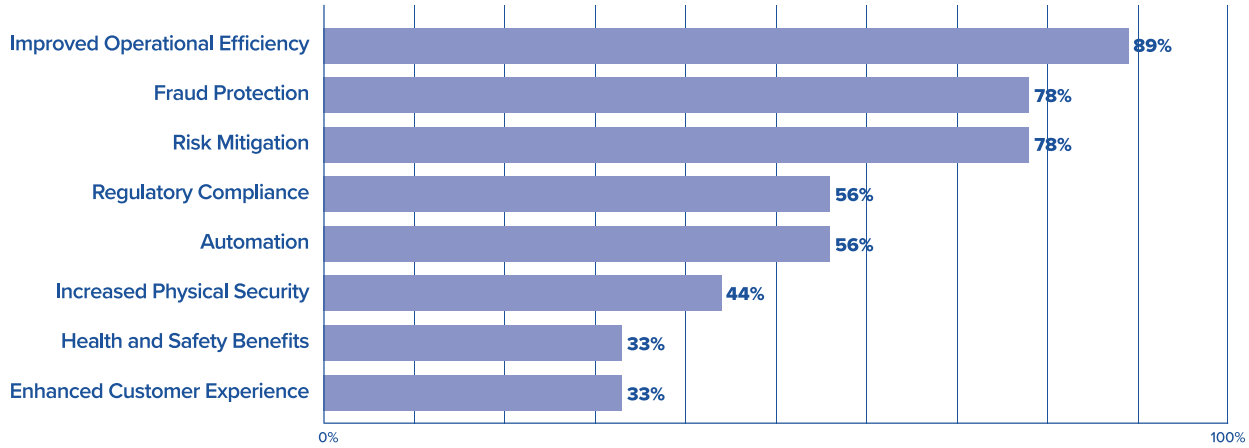


Their budgets for digital transformation projects varied, but only a third reported having more than $5 million for 2024 and 2025. No respondents reported a digital transformation budget over $25 million, and 34% have nothing allocated to digitization.

Motivation and Expectation

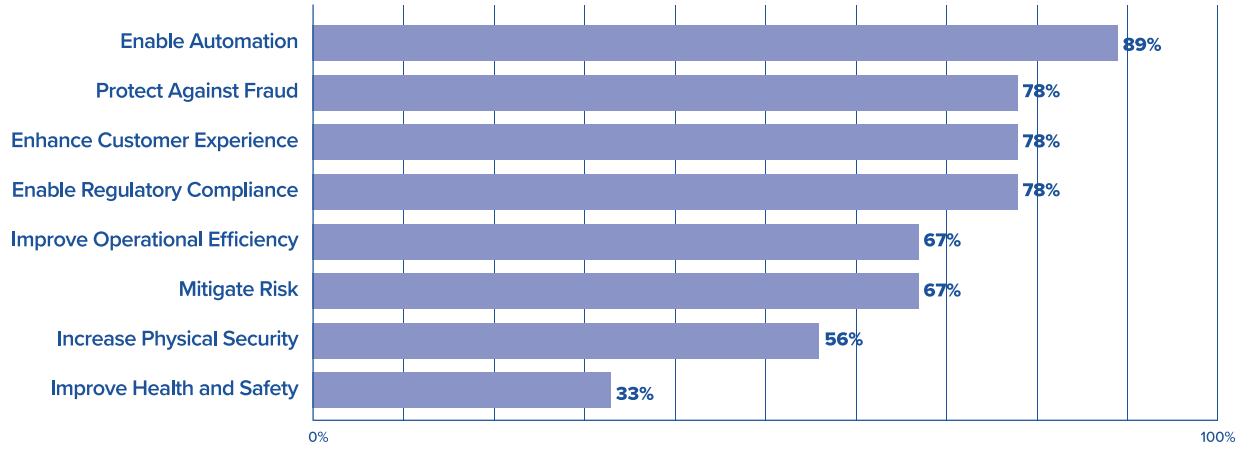
Respondents are primarily motivated to adopt digital transformation technolgies for reasons of improved operational efficiency, as well as fraud prevention and risk mitigation.

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



That motivation to adopt digital technology strongly aligns with respondents' confidence in digital identity solutions, which they understand to enable automation, protect against fraud, improve efficiency, and enhance customer experience.

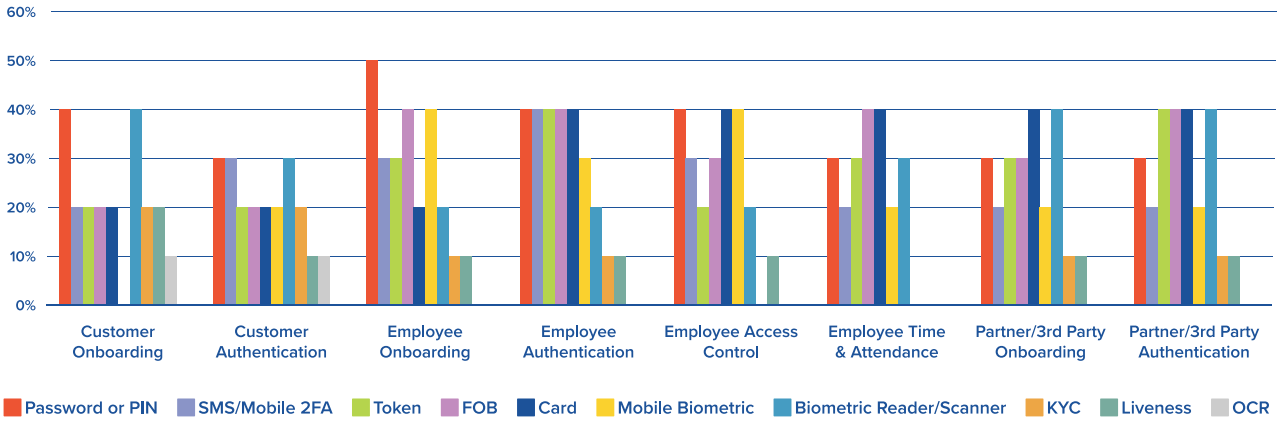
Mostly confident that digital identity solutions can:



Priorities and Obstacles

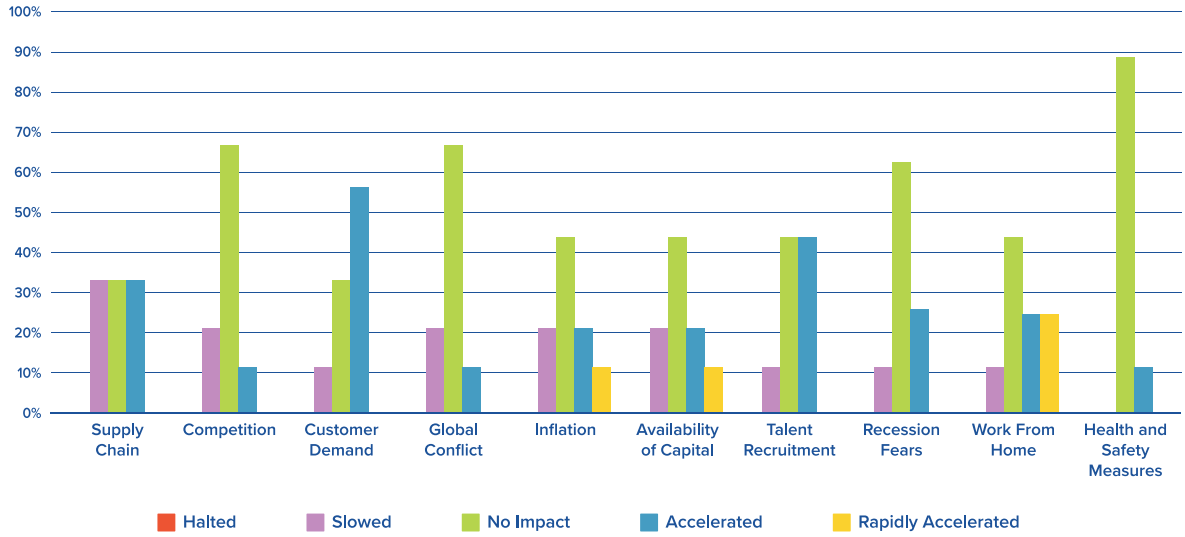
Agencies and organizations are already leveraging biometric technology for customer and third party onboarding and authentication, as well as for employee time and attendance. Knowledge-based authentication like passwords and PINs are still widely used throughout the entire user lifecycle, along with other non-biometric security.

What authentication/ID technology do you use for the following identity-related processes?



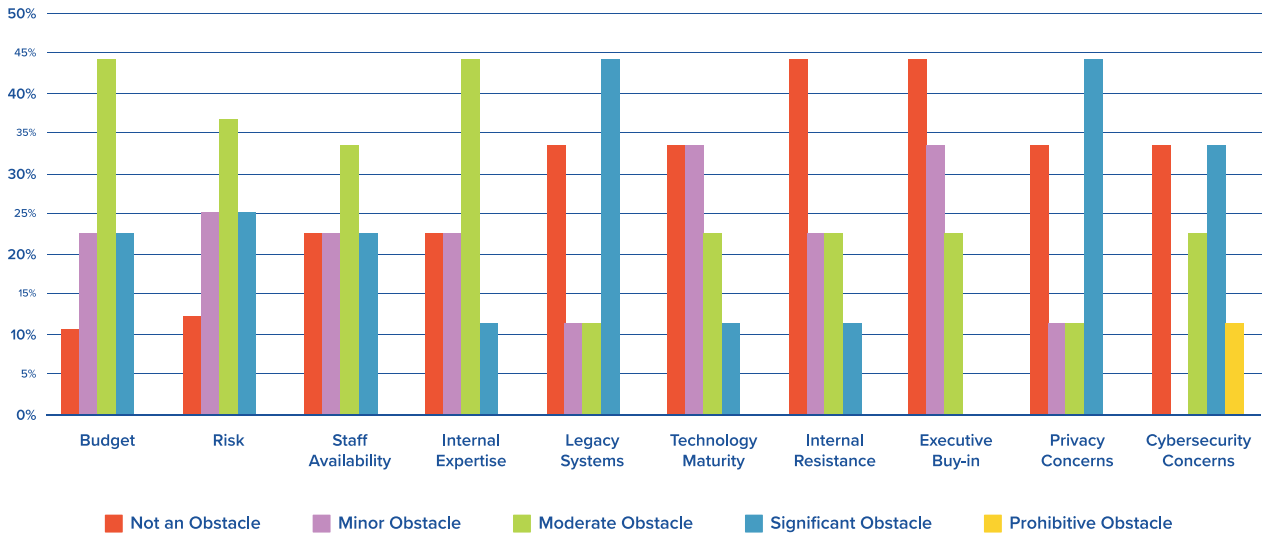
Meanwhile, global factors that impacted the wider industry in 2022 and 2023 are largely inert in 2024's government services landscape. Financial concerns like inflation and availability of capital seem to be accelerating digital transformation, along with work from home trends.

How are global factors impacting your digital transformation?



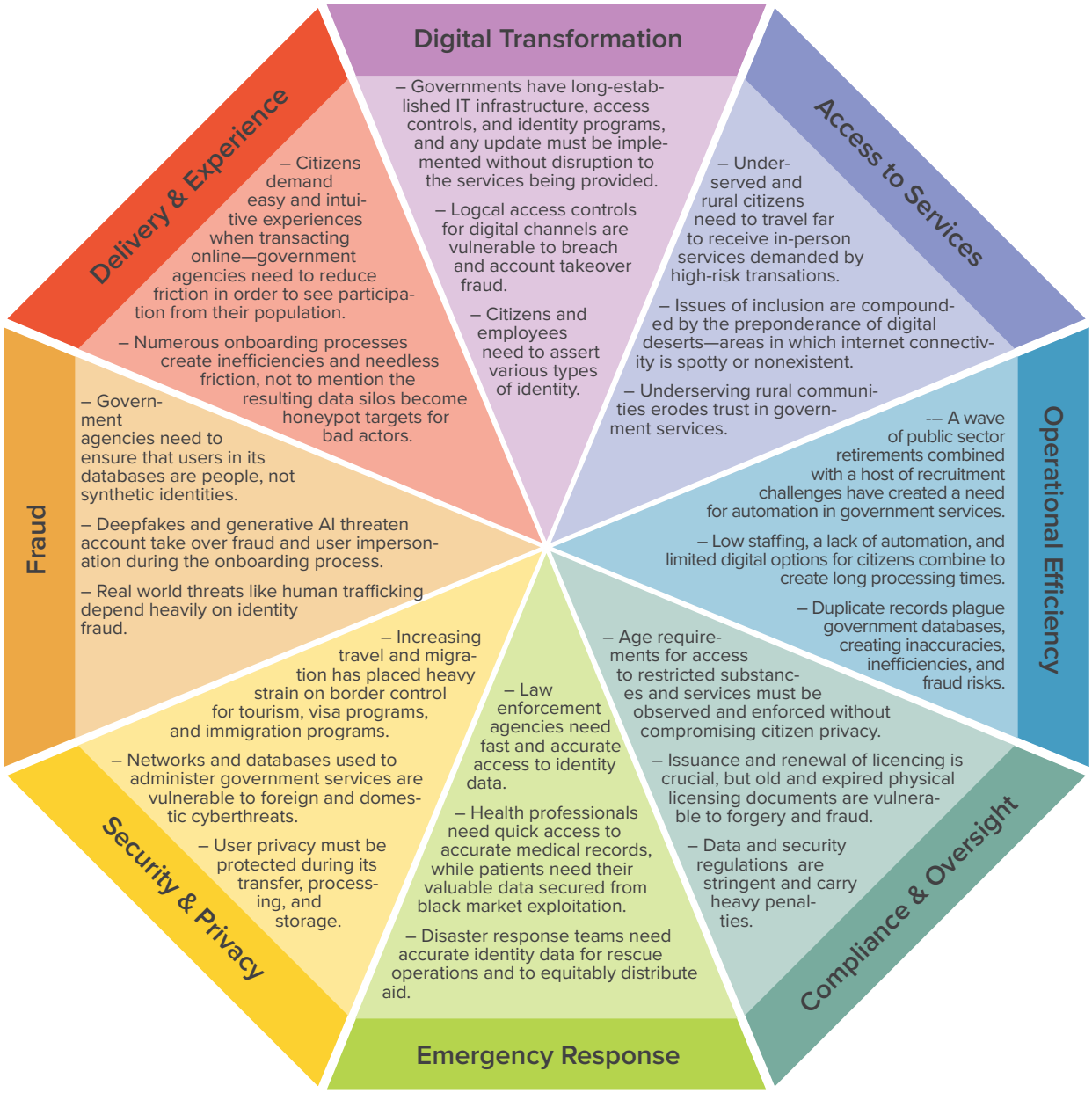
But the obstacles and adoption barriers to digital transformation are wide-ranging. Cybersecurity, privacy concerns, and legacy systems are presenting significant challenges to government services providers on their digital transformation roadmaps. And reports of internal resistance, staffing availability, budget, and risk as obstacles, taken together, paint a picture of a challenging and turbulent environment for the adoption of digital solutions.

How severe are the following obstacles to your digital transformation roadmap?



Viewing Challenges Through the Prism Lens

To understand how the broad benefits of biometric digital identity can be applied to government services we use the **Prism Lens**. Each segment of this octagon represents one significant challenge for the market as it feels the increasing pressure of digital transofrmation and user expectation, which are inextricable from the other issues. By understanding these challenges holistically through the Prism Lens, we can see common obstacles on the path to achieving the full spectrum represented in the Prism Identity Hierarchy.



Biometric Solutions

Biometric digital identity solutions can be applied to each segment of the **Prism Lens** to address the digital transformation challenges faced by government services stakeholders.

Digital Transformation

– Biometric digital identity can bind established foundational identity documentation to human citizens through simple onboarding processes without the need to start from scratch.

– Biometric digital identity works on a transactional level for secure and convenient access control, ensuring online channels for government services are only accessed by authorized citizens.

– Citizens and government employees can be in control of how much identity data they share in a given transaction.

Access to Services

– Biometric digital identity enables remote government services, allowing for transactions to be performed quickly and at scale in urban and rural regions.

– Built-in redundancies can enable offline functionality for digital identity technologies, while biometric barcode technology eliminates needs for specific types of device hardware.

– Biometrics at the core enables equal service and participation for all citizens, fostering trust through inclusion.

Operational Efficiency

— Biometric digital identity enables remote transactions, lightening the load for government offices.

– Digital identity solutions significantly mitigate onerous onboarding and identity proofing transactions.

— Binding identity data to a biometric means that all government records can be coalesced and linked to a single human being via a 1:N search and match process.

Compliance & Oversight

– Biometric digital identities can support pseudonymous and selective data sharing, allowing citizens to assert age of majority without sharing any other Personally Identifiable Information (PII).

– Biometric digital identity allows for remote renewal of licenses and doesn't leave a paper trail of expired documents.

– Identity Proofing & Verification Prism vendors provide compliance to the stringent regulations as a matter of course.

Emergency Response

– Biometric digital identity can be used for accurate and fast background checks, booking, and watchlist maintenance.

– Medical records bound to a user's biometrics can be recalled in emergencies when patients are non-verbal or unconscious, and they are invulnerable to medical fraud.

– Biometrics can be used in disaster response to identify survivors, distribute aid, and enable services in the absence of physical ID.

Security & Privacy

– Biometric digital identity solutions enable visitors to engage with border control remotely, enhancing the border crossing experience while maintaining its integrity.

– Biometric digital identity protects networks through strong authentication and unimpeachable audit controls, ensuring every moment of access can be traced to a specific, authorized human being.

– With biometrics at the core, transactional and pseudonymous activity still benefits from the highest levels of trust while protecting a user's PII.

Fraud

– Biometric onboarding ensures that the person enrolling in a government service is who they claim to be and not a synthetic identity.

– 1:N search functions can clear up databases that already contain synthetic accounts.

– Biometric liveness and deepfake detection can spot AI generated impersonations and reject them from logging into an account.

– Biometric digital identity cannot be counterfeited for use by smugglers or human traffickers.

Delivery & Experience

– Biometric digital identity removes friction, making transactions as smooth as looking into a camera, scanning a fingerprint, or tapping a phone.

– One enrollment can be used among numerous services at varying levels of privacy.

– Biometric digital identity, supported by a trusted system of record, has the potential to empower citizens in any scenario in which they need to prove they are who they claim to be.

Looking through the Prism Lens

Thanks to the vast purview of government services—which touch everything from elections and taxes, to financial benefits and healthcare, to travel and national security—organizations and agencies operating in the public sector are beset by myriad challenges. Biometric digital identity, when deployed in tune with the Prism Identity Hierarchy, can address many of these obstacles.

Digital Transformation

Digital transformation is a necessity for governments all over the world. But unlike private industries or unregulated markets that have sped ahead and created a demand for online channels, the public sector is burdened by restrictive budgets, bureaucratic processes for funding and approval, and legacy systems. That last item is particularly obstructive in advanced economies, and is indicative of a sad truth when it comes to modernization of public services: governments are often in their own way and need to avoid tripping over themselves. A digitized service needs to be vetted, approved, and implemented successfully without disrupting the current services being offered. And citizens are demanding it now.

Opening digital channels for government services requires logical access controls for government employees and citizens. And wherever there are digital credentials there is also a risk of account takeover (ATO) fraud. Phishing, hacking, password reset attacks are all common methods of exploiting digital channels to gain wrongful access to assets and accounts. In 2022, US federal agencies reported 30,659 information security incidents. According to the Government Accountability Office, 34% of those were due to usage violations, while 10% were directly related to phishing.

Biometric digital identity can bind established foundational identity documentation like passports and birth certificates to human citizens via intuitive and secure onboarding processes. The Identity verification and biometric identity platform solutions that facilitate this can integrate with legacy systems, enabling seamless deployment. Once that biometrically bound foundational identity is in place, the account takeover fraud, databreaches, and phishing emblematic of digital government services become a thing of the past.

10% of the 30,659 information security incidents reported by US Federal Agencies in 2022 were directly related to phishing, according to the Government Accountability Office.

Biometrics with sufficient liveness detection cannot be phished, lost, or stolen. When linked to a government source of record, the often exploited account recovery process is also secured. As for the usage violations, biometric digital identity can't be shared with coworkers or left out in the open, and it allows for audit trails that can be both comprehensive and privacy preserving when need be. All of this adds up to a genuine opportunity for government agencies struggling to safely move services online.

Access to Services

Government agencies need to reach all of their citizens. And while it is tempting to hyperbolize how connected our world is, many people remain underserved by organizations due to where they live, what they have, and who they are. Citizens in rural regions may have to travel long distances to gain access to government services, while those in digital deserts might not have the connectivity to use digital channels. In the EU and G20 countries fixed broadband speeds are nearly 50% slower in rural regions than in urban areas. This digital divide is crucial to address because rural and urban populations are equally engaged in politics, but underserved populations show an understandable lack of trust when they are neglected due to logistics that favor city dwellers.

Fixed broadband speeds in the EU and G20 nations are nearly 50% slower in rural regions, creating a significant digital divide.

Foundational identity bound to user biometrics can enable remote government services for high risk transactions far distances from physical government branches and even in areas of low or no bandwidth. Identity proofing can be performed on smartphones, tablets, laptops, and desktop computers. Once a citizen is onboarded and their biometrics are bound to a system of record, their mobile ID can be digitally signed, allowing for offline use. This and other redundancies are methods currently being used in Africa to ensure service and boost inclusion.

Meanwhile, new innovations in biometric barcode technology are bringing biometric digital identity into the analog world. Not every one has access to smart device technology, but innovations like those that allow for the embedding of a user's biometric template in a QR code that can be scanned when needed—means the benefits of strong biometrics can be printed on documents, passports, or licenses.

Operational Efficiency

The workforce is retiring, and the government sector needs automation. Countries facing an influx of immigration are seeing their populations grow while the number of employees on hand to administer and process government services is shrinking. Add the fact that digital transformation is requiring management of converging physical and digital channels, operations are contributing to slowdown, worker burnout, user frustration, and inevitably citizen disengagement. Making things even more challenging, decades of siloed data collection and human error have created a preponderance of duplicate records which, in addition to contributing to waste and disorganization, open the door to fraud.

Biometric digital identity lightens the operational load, allowing for high risk transactions through digital channels. Processing time required for identity proofing is shrunk by orders of magnitude, with operations that used to require lengthy transit and manual checks replaced by AI-supported biometric matching.

These speeds are possible thanks to biometric binding that links a human to their foundational identity. That core identity can be subjected to a 1:N search, enabling duplicate records to be coalesced, merged, or deleted as needed. With biometrics at the core, government agencies can count on clean records and reduced toil at a time when they need all the relief they can get.

1:N biometric searches enable duplicate records to be coalesced, merged, or deleted as needed, cleaning databases and reducing operational workloads.

Compliance & Oversight

Age requirements for restricted substances and services fall under the purview of the government, but they must be observed by relying parties providing the products, be they liquor or cannabis stores, casinos, adult websites, or even movie theaters. But fake IDs are prevalent, and digital services rely primarily on an honor system. Meanwhile, showing ID as a citizen qualified to consume an adult product generally involves providing more information than required, demanding a citizen reveal their name, photo, age, and address to the person verifying them.

Speaking of physical IDs—licenses, credentials, passports, and permits need to be renewed and up to date. The process of doing so is necessarily onerous, thanks to the identity proofing required. Expired physical IDs also contribute to the above challenge, feeding into the fake ID problem that drives underage access to a range of age restricted services and their often unfortunate subsequent consequences.

Compliance with data regulations is crucial too. Government agencies are beholden to the same data privacy laws they engineer, and regulations like GDPR, PSD2, CCPA have sharp teeth when it comes to taking reprisal on non-compliant organizations. For instance, in the European Union, individuals can claim compensation if they suffered a material or non-material loss as a result of a public body running afoul of GDPR.

Biometric digital identity has a long and growing history of enabling regulatory compliance. Implemented with biometrics that bind a human to their foundational identity, mobile IDs, eIDs, mDLs, and biometrically-bound national IDs like India's Aadhaar eliminate the need for weak authentication controls that risk running afoul of data laws. Those same digital credentials have strong enough continuous identity assurance that they can enable remote renewal for licenses and permits that would otherwise require snail mail or in-person transactions. And biometrics truly shine when used for pseudonymous age checks, able to give relying parties a simple yes or no signal that they can trust—no need to share anything else than a thumbs up. With biometrics, compliance isn't just easy, it's privacy enhancing.

Emergency Response

Identity is complex, and that is especially true in law enforcement. The sector is largely responsible for the foundational science behind biometrics, and the technology is much needed in both the office and the field for booking and threat identification. Meanwhile, when citizens require background checks, that also falls under the purview of law enforcement agencies.

Health professionals, who in many countries act as part of or in partnership with government services need quick access to medical records. Sometimes it's a matter of regulations and due diligence, and other times it can be a matter of life and death. Regardless of the situation, access to patient records must be quick, secure, and accurate. Incorrect identification of a patient can lead to mistreatment, allergic reactions, and other mortal consequences. Meanwhile, that same data that's crucial for keeping citizens healthy is the most sought after by criminals, estimated to be worth ten times as much as payment data on the black market.

And when disaster strikes—and it is striking with increasing frequency—response teams need access to accurate identity data in the immediate and long term aftermath in order to perform rescue operations and subsequently distribute equita-

ble aid.

Biometric digital identity can be used in law enforcement for fast and accurate background checks, like those required for public employees. In the healthcare space, medical records bound to a user via biometrics allow for fast and accurate recall, even in situations when the patient is non-verbal or unresponsive. The same is true in disaster response, where foundational identity biometrically bound to a user can ensure they have access to government services even if their physical credentials are lost, destroyed, or left behind in an evacuation.

Security & Privacy

The government sector faces threats from bad actors on all fronts, from the border, to the internet, to its own communities. Increases in travel and migration are straining border control for tourism, visa programs, and immigration. Agencies need to be able to welcome visitors while maintaining national security.

On a digital level, the networks and databases used to administer government services are vulnerable to cyberthreats from within and abroad. Cybercrime, whether its from domestic actors or foreign powers, is a real concern, and it exploits weaknesses in a nation's identity infrastructure to gain access to critical data. According to the Center for Strategic & International Studies (CSIS)—which records significant cyber attacks "on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars" across the globe, 45 of such cyber attacks occurred in the first nine months of 2024. And that's not mentioning the information in transit, as citizens interact with their governments online.

Biometric digital identity addresses each of these security concerns while actually improving the user experience for both citizens and public servants. Border control solutions like Digital Travel Credentials (DTC), which allow trusted travelers to perform pre-screening from their homes, use strong identity and verifiable credentials to lessen the burden and alleviate bottlenecks at the border. But that's secondary to the accurate identity checks that are made possible through the DTC, which is already maintaining security in regions as far apart as the Virgin Islands, Europe, and Asia Pacific.

On the digital front, biometric authentication supported by a strong foundation and unbroken trust chain makes breaking into databases significantly more challenging. And decentralized storage methods, exemplified by Prism Biometric Identity Platform BeamLuminary Anonybit, makes compromised data useless even if it is leaked. As for the citizens, biometric digital identity means

that only they have access to their government services.

Fraud

An extension of security and privacy is fraud. A major challenge for all sectors undergoing digital transformation, especially in the post-pandemic age of AI and synthetic identities. Governments need to ensure their databases are free of fraudulent accounts that can be used to collect benefits, scam services, and as a basis to open non-government accounts that can be used for more widespread fraud. Impersonations are also a problem exacerbated by AI, with easy-to-access deepfake technology able to render weak biometric security methods useless, making them vulnerable to account takeover. In 2024, this proved to be an increasing threat in Singapore, after a series of unreported data breaches led to the proliferation of know your customer documents and selfie data on the dark web.

Meanwhile, in North America, according to Thomson-Reuters' "2023 Government Fraud Waste and Abuse Report," U.S. government workers' confidence that they are equipped to address these issues has decreased 13% year over year. The report points to " overall fraud activity, more sophisticated fraud schemes, and lack of person-to-person interaction" as contributors to increased challenge.

In the physical world, fraud is used for human trafficking. Counterfeit identity credentials are used to facilitate the transport and sale of 10% of the world's estimated 50 million modern slavery victims. On a broader level, the same kind of fraud is used for illegal transit of all kinds. The challenge is ensuring false credentials are caught and taken out of circulation.

Fraud is a purposeful mismatch between a bad actor and someone else's foundational or biographical identity. When biometrics connect humans to those other aspects of their identity, they become inseparable. In databases, that means foundational and biographical data can't exist without a real human attached to them. And with increasingly reliable liveness and deepfake detection, threats from generative AI can be thwarted before they corrupt government databases.

In the real world, the same principle can prevent people from assuming false or wrongful identities. A biometric digital ID, whether it's a mobile ID, a traditional identity document encoded with biometrics, or a barcode embedded with a biometric template physically printed on a piece of paper, an impersonator cannot rightly claim to be the document holder when the biomet-

U.S. government workers' confidence that they are equipped to address issues of fraud, waste and abuse decreased 13% between 2022 and 2023.

-Thomson-Reuters' "2023 Government Fraud Waste and Abuse Report"

ric facial recognition fails.

Service Delivery & Experience

Citizens demand easy and intuitive experiences when transacting online, and government services must meet these demands. This means reducing friction without compromising security. A big part of that is minimizing the number of onboarding touchpoints. When a citizen needs to re-enroll for a new government service, not only does the process contribute to inefficiency and expand the fraud surface by adding another onboarding touchpoint, it introduces another obstacle between the person and their service. Citizens need to have one multi-purpose ID that they control, one that is secure, reusable, and privacy enhancing.

Biometric digital ID is the one ID to rule them all. A single enrollment can be used to bind a citizen to their foundational identity, and from there build up and out to encompass the entirety of modern identity, from biographical details to contextual circumstances and beyond. Putting biometrics at the core of citizen life means a person can confidently and easily assert their identity across a variety of use cases, in person or online, without needing to reintroduce themselves every time they encounter a new branch of government. In the city, the suburbs, rural communities, or even digital deserts, digital ID enabled with biometrics and supported by a system of record means that government services serve you no matter who or where you are.

"Prime Minister Prayut Chan-o-cha, who presided over the launch of the "ThaID" mobile application, said it was designed to make it more convenient for people to access state-run services. Gen Prayut expressed hopes that more state agencies and private agencies would make use of the digital ID system to streamline their services and urged media outlets to promote wider use."

-Traisuree Taisaranakul, Thai Deputy Government Spokeswoman speaking to Bankok Post

The Biometric Digital Identity Government Services Market Forecasts

Bolstered by the significant interest in digital identity technologies and the converging industry trends illustrated in the previous section, which lend themselves to biometrics adoption, the Biometric Digital Identity Government Services Market is on track for significant growth, globally.

The following data is based on original proprietary market research from Acuity Market Intelligence. These are bottom up market forecasts based on quantifiable 3rd party data such as regional population and digital adoption rates along with a series of assumptions about the current level of biometric adoption, average use, and projected growth of the user base and user adoption based on proprietary analysis.

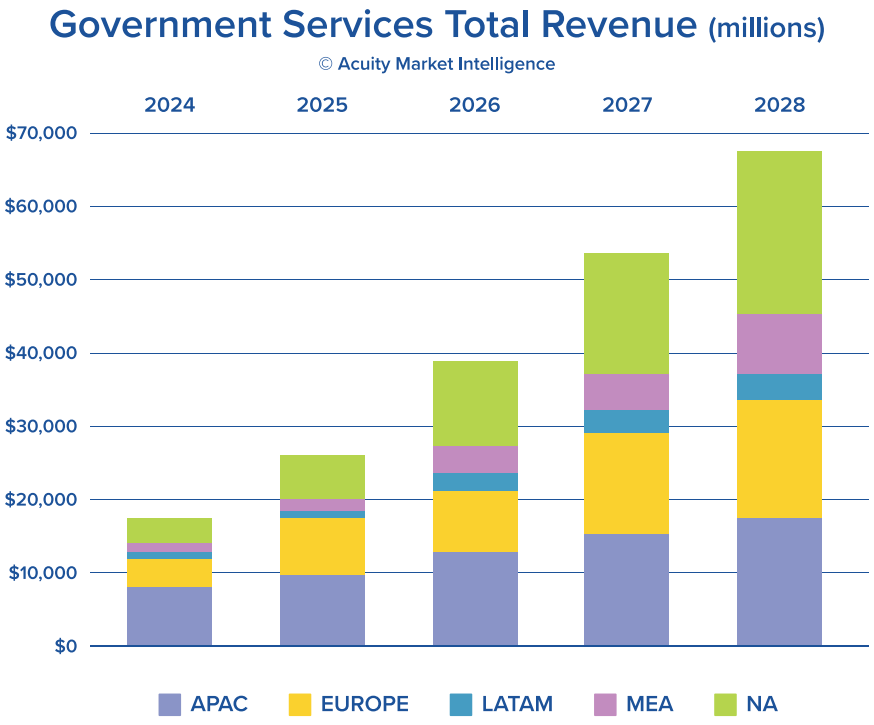
This proprietary analysis is based on ongoing market research, third party data, vendor reported data, and industry expert assessments.

Interactive spreadsheets of these forecasts with further visibility into the market are available for purchase.

Contact cmaxmost@acuity-mi.com for inquiries.

Global and Regional Forecasts

Total biometric digital identity government services revenue from 2024-2028 is expected to grow at an overall compound annual growth rate (CAGR) of 39.2%, generating just over $202.5 billion globally.

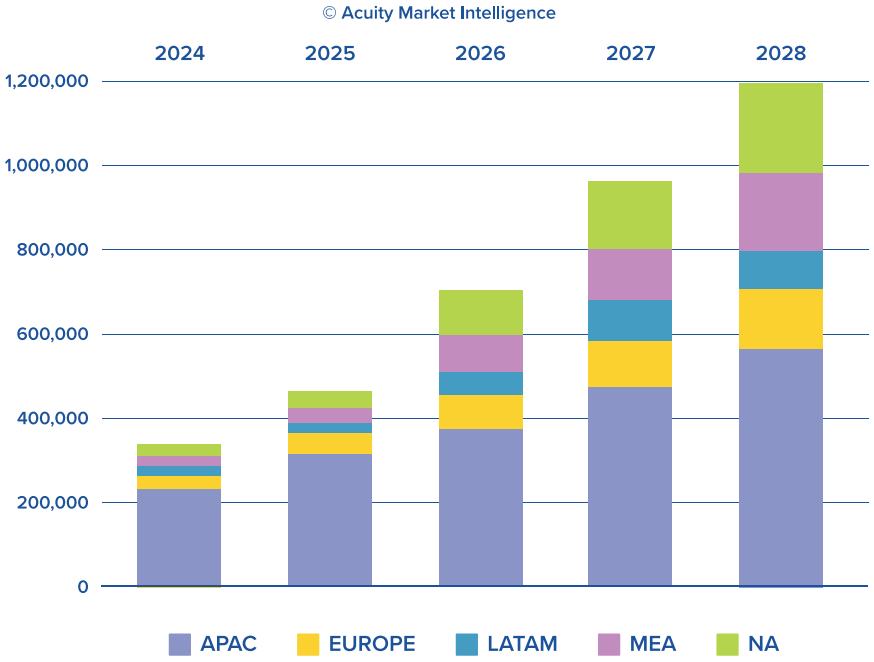


Total Revenue (millions)					
	2024	**2025**	**2026**	**2027**	**2028**
APAC	$7,788	$9,669	$12,107	$14,931	$17,508
EUROPE	$4,937	$6,857	$9,904	$13,387	$16,505
LATAM	$1,016	$1,413	$2,026	$2,746	$3,417
MEA	$1,148	$1,917	$3,352	$5,347	$7,301
NA	$3,221	$5,651	$10,330	$16,872	$23,177
Total	**$18,110**	**$25,506**	**$37,718**	**$53,282**	**$67,909**

Global and Regional Transaction Volumes

The total global transaction volume for biometric digital identity in government services is forecast to exceed 3.6 trillion during the 2024-2028 forecast period. As with any identity-related application, population ultimately determines transaction volume. So it is no surprise that the Asia Pacific region dominates transaction volumes in the government services arena. Especially when China and India have invested heavily in biometric-based national identity schemes for their citizenry of nearly 3 billion.

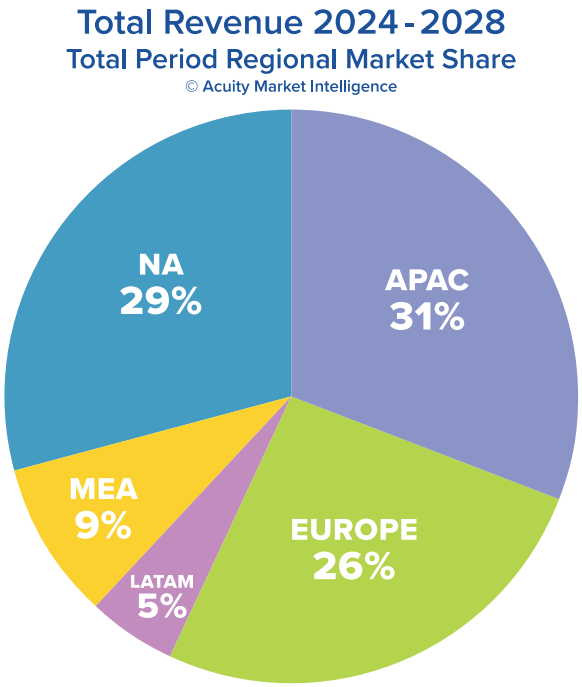
Government Services Total Transactions (millions)



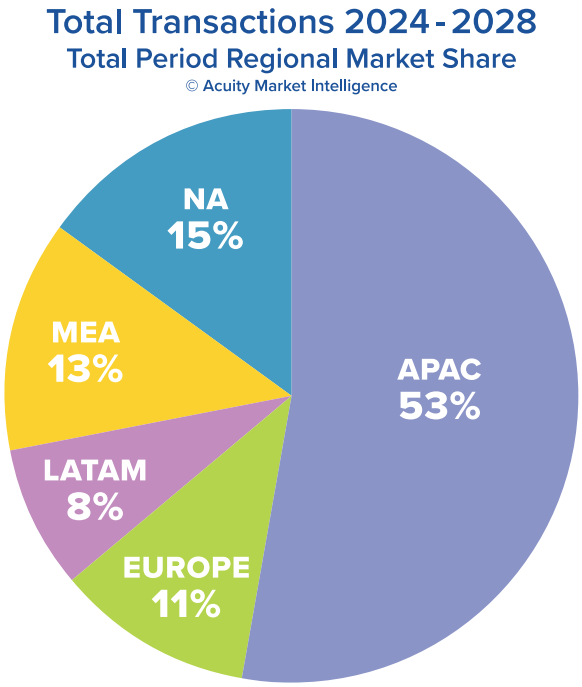
Total Transactions (millions)					
	2024	2025	2026	2027	2028
APAC	219,120	284,610	378,988	479,264	568,758
EUROPE	36,696	53,022	79,969	110,478	137,611
LATAM	25,806	36,821	54,449	74,825	93,526
MEA	26,928	45,477	80,400	128,994	176,337
NA	29,964	53,302	98,426	161,542	222,013
Total	**338,514**	**473,132**	**692,231**	**955,104**	**1,198,245**

Total Regional Share of Revenues and Transactions

APAC leads in revenues for the period, with North America and Europe close behind.

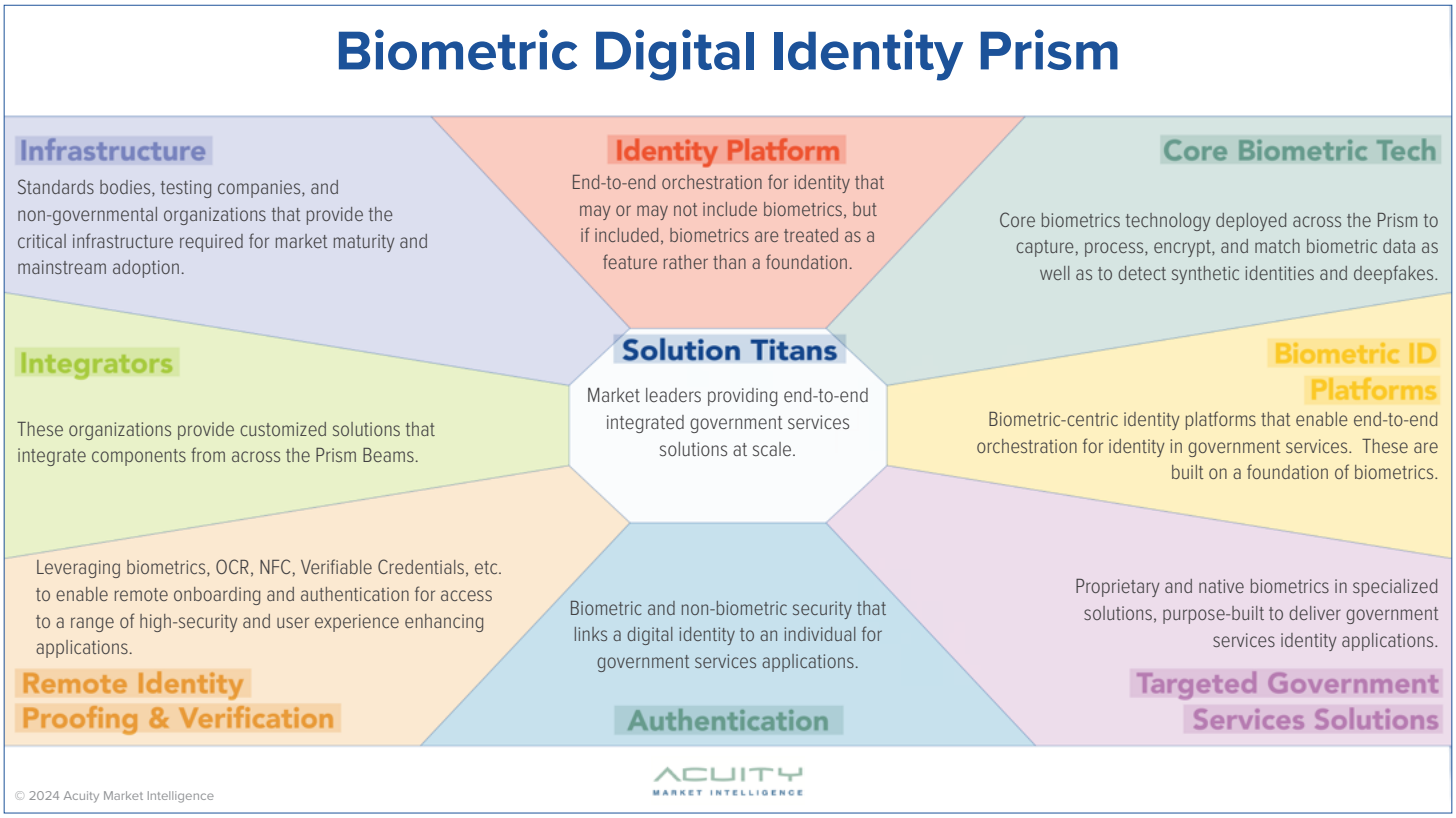


Meanwhile, APAC dominates in transaction volumes, with 53% of the market share from 2024-2028.



The Government Services Prism

Just as a beam of light contains all colors, the biometric digital identity ecosystem is comprised of many vendors, organizations, and relying parties 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.



Vendors are positioned in one of nine Prism Beams. Each Beam representing a critical component of the biometric digital identity landscape for government services. For some vendors, 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.

How to Read the Prism

Within each beam, there are three Vendor Categories: Pulsars, Catalysts, and Luminaries.

Pulsar

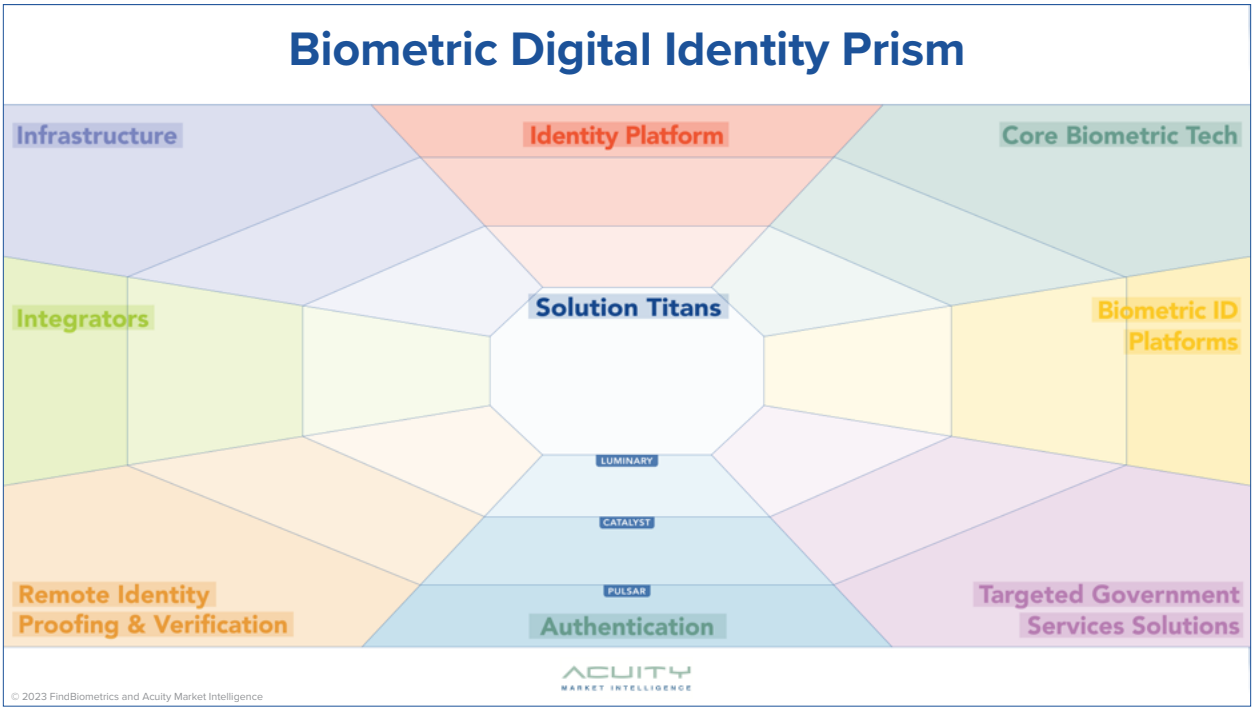
Pulsars are the bright upstarts and pivoting legacy vendors prioritizing the crucial elements of biometric digital identity. Startups with promising technology or established names with a proven aptitude for adapting to the new identity ecosystem, Pulsars have strong potential to influence the Prism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

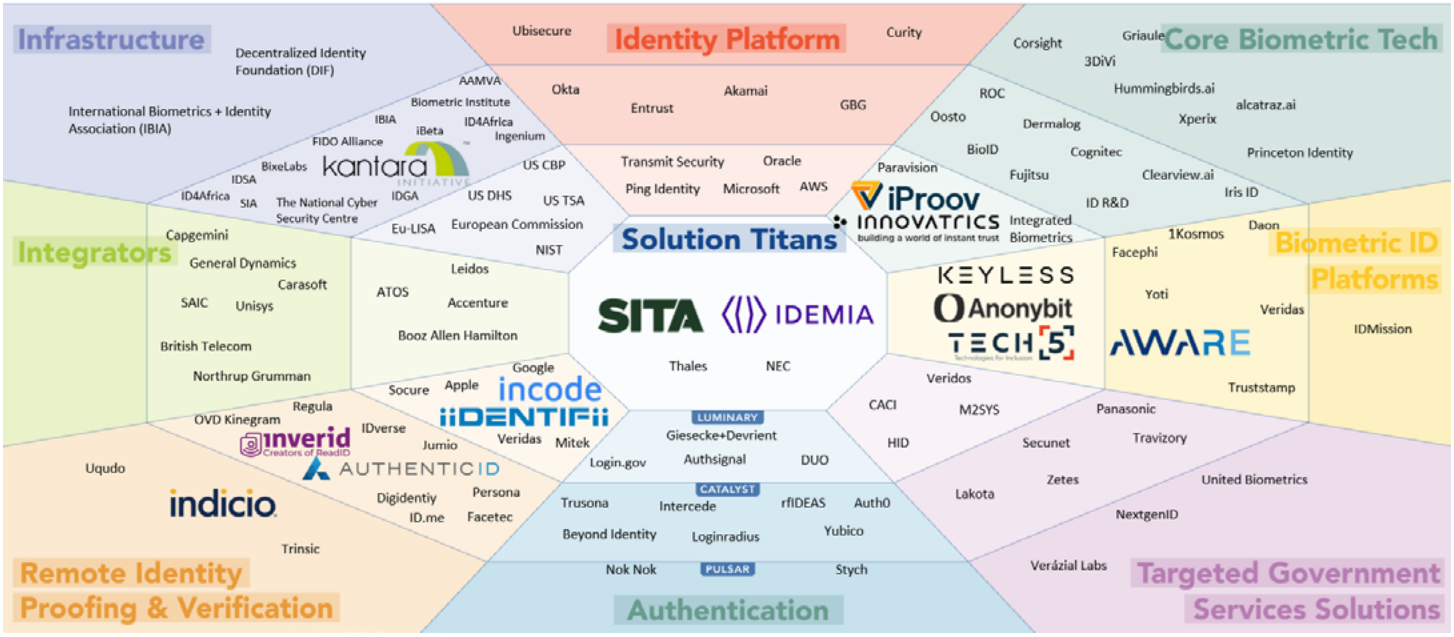


Refractors and the Solution Titans

The center of the Prism is anchored by a special category—the Solution Titans. These companies, due to their size, global footprint, proven expertise, partner networks, and robust portfolios, have a definitive role in the government services biometric digital identity landscape. This role is that of a Refractor: it is through their initiatives that the industry is viewed.

As the market evolves through acquisition, development, regulation, and innovation, the Refractor position may grow or diminish. Luminaries in the Identity Platform Beams are best positioned to ascend to Refractor status.

The Government Services Biometric Digital Identity Ecosystem



Important Note on Prism Beams:

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

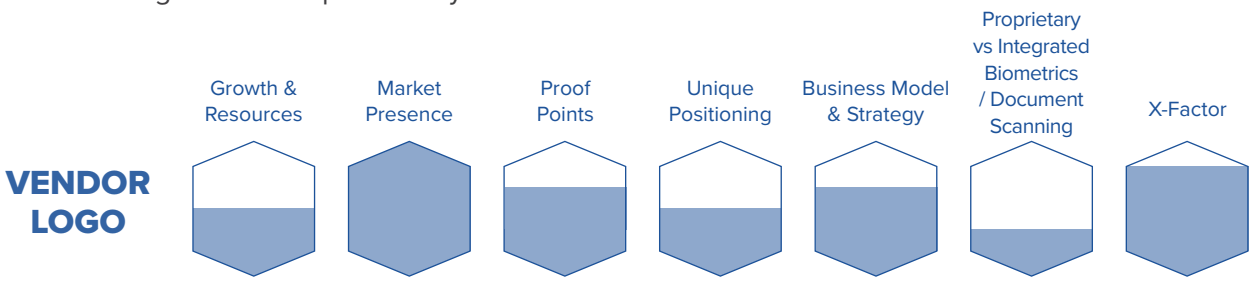
Evaluations & Use Cases

In order to place vendors on the Biometric Digital Identity Prism, we are assessing the leading companies based on several 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.
- **Proprietary Versus Integrated Biometrics and Document Authentication** – Depending on the market, solutions(s), specific beam, may be rated higher as proprietary or integrated technology.
- **Commitment to Digital Identity** – Evidence of longterm financial and cultural investment in digital identity, demonstrated through R&D, participation in standards, inter-industry collaboration, and thought leadership.
- **Commitment to Biometrics** – Evidence of longterm financial and cultural investment in biometrics as a core identity technology, not only within a product portfolio, but conceptually at an industry level.
- **Impact and Influence** – Effectiveness of an organization's ability to guide standards, regulation, policy, and industry best practices through its own initiatives and thought leadership.
- **X-Factor** – This is a unique beam and market sector specific metric.

Note on Evaluation Criteria:
Some Prism Beams are graded on unique rubrics that better represent how their constituents fit into the Biometric Digital Identity Government Services Ecosystem. Any changes in criteria are noted at the beginnging of an evaluation section.

We visualize this assessment as a Prism Evaluation Chart: an easy-to read graphic representation of a vendor's current activity, resources, and abilities. The more color filling a Prism hexagon, the higher level of proficiency.



Important Note of Evaluations and Prism Placement:

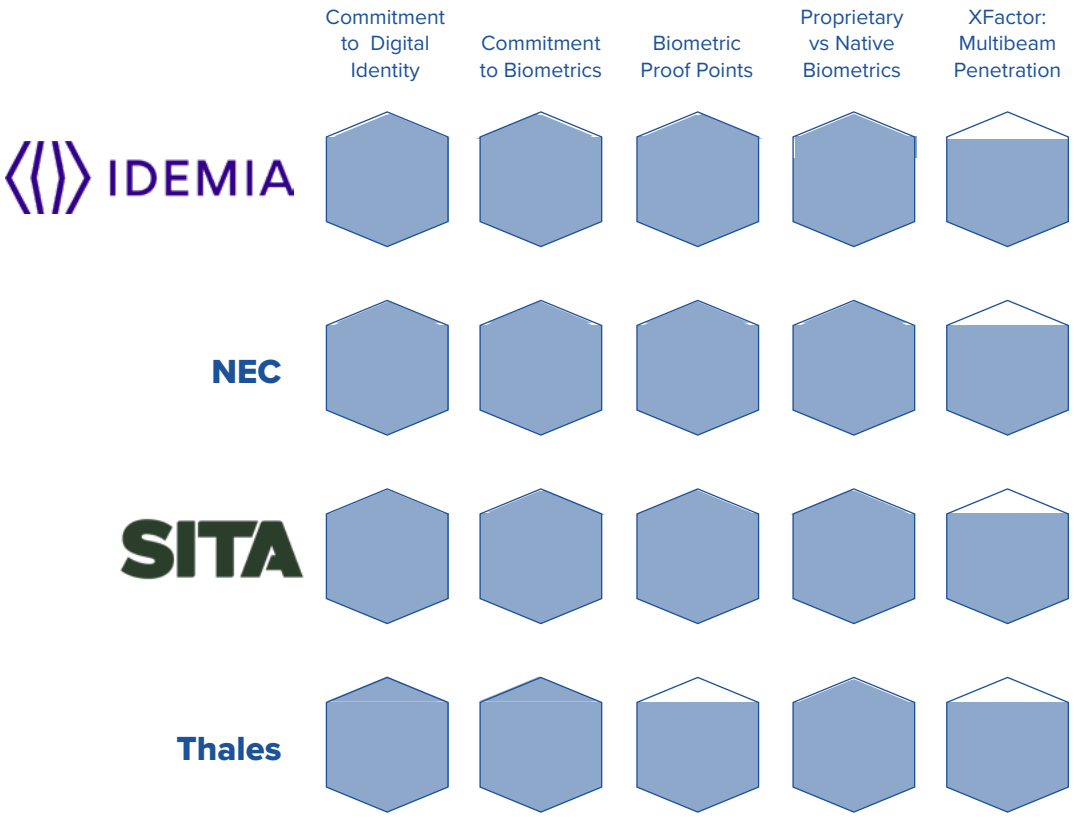
The vendor specific metrics in this report are based on publicly available data, survey data, interviews, and confidential briefings. It is presented in good faith as a representation of the biometric digital identity government services ecosystem according to the values stated previously in this report.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

Solutions Titans

These leading government services players are critical to global acceptance and adoption of biometric digital identity. To date, they have made various levels of investment in biometric tests, pilots, and deployments but they all understand the critical role biometrics will play as the foundation of an identity-first world.

Evaluation Note:
Solutions Titans are graded on five unique criteria including their presence in other Prism Beams, which is explored further on the next page.

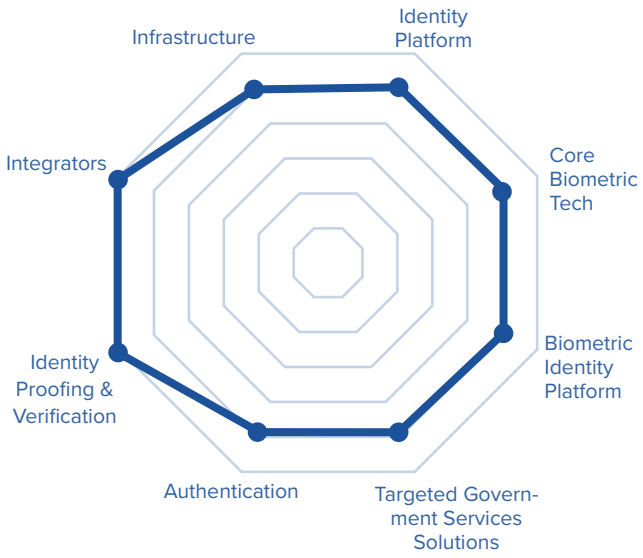
Evaluations



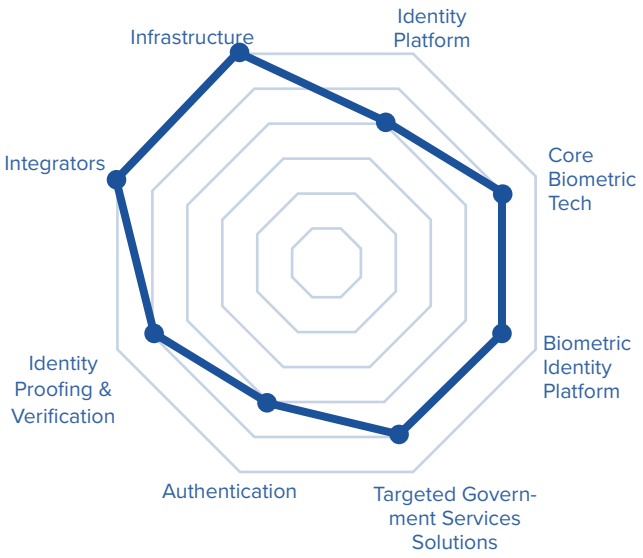
Refractor Beam Penetration

The Solutions Titans are positioned in the center of the Prism because of their demonstrated ability to define the biometric digital identity government services landscape through their participation in each other Prism Beam. The following Refractor Charts display each Titan's leadership within every aspect of the biometric digital identity ecosystem.

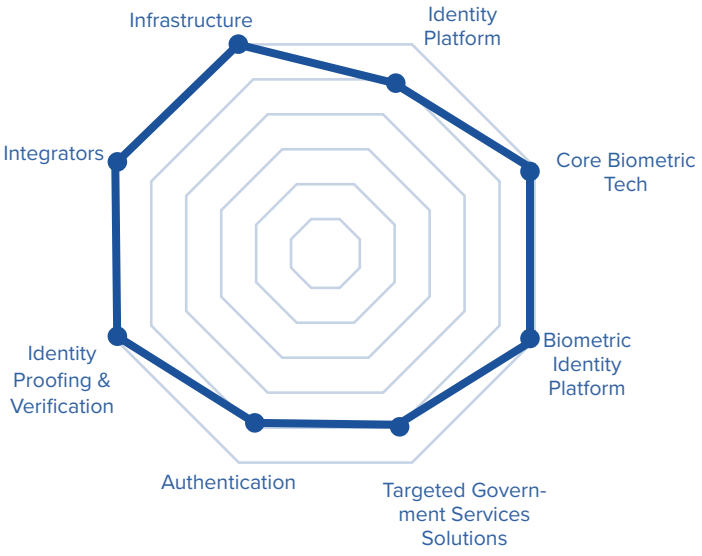
IDEMIA



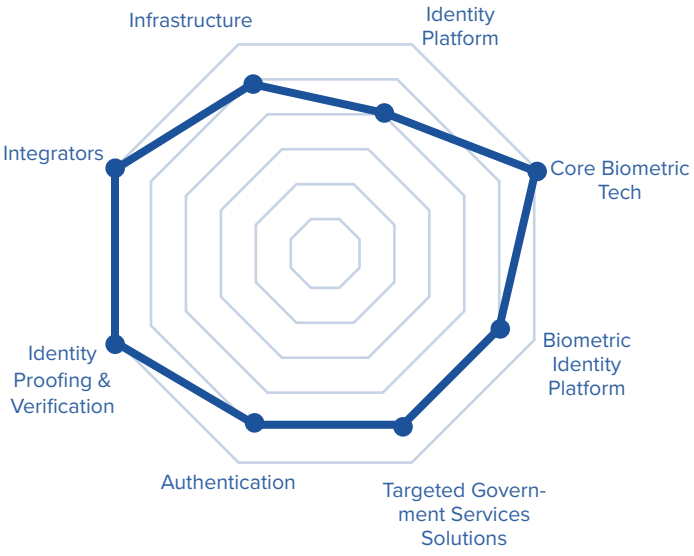
NEC



SITA



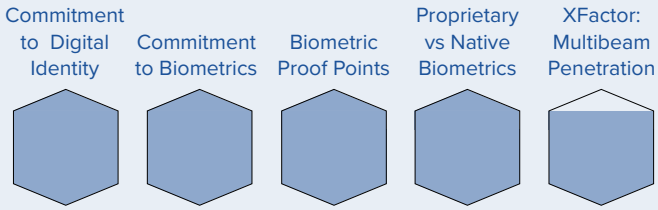
Thales

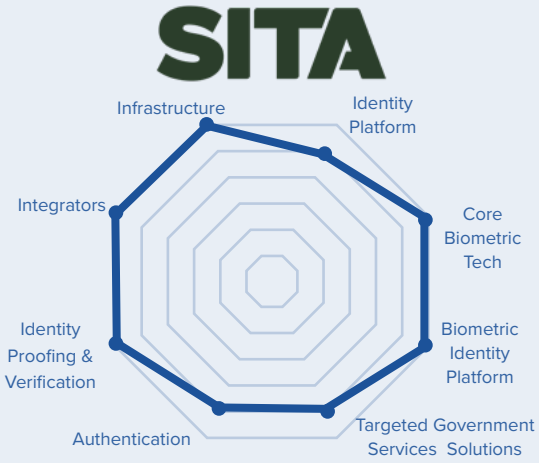


SITA

sita.aero

BEAM: **Solutions Titan** / CLASSIFICATION: **Refractor**





Founded in 1949 by a consortium of airlines seeking to improve air travel, SITA began its existence focused on providing network and communications services between airports and airlines. In the 75 years since its creation, the company has grown and evolved to become not just a titan of the travel industry—facilitating more than 2.2 billion travel journeys every year and operating with over 700 airlines across 200 countries—but also a trusted partner to governments across the globe. Border control is inextricably linked to travel, especially at the scale on which SITA operates, and over the past quarter-century, the firm has been delivering cutting-edge solutions to dozens of governments, including all G20 nations. Using AI, biometrics, and other identity management technologies like verifiable credentials, SITA is solving significant data challenges for governments before travelers even leave their homes.

The Government Side of Travel

When we take an international view of government services, our eyes necessarily turn to travel, and we must focus on the border. Governments benefit from visitors. Tourism, visa-based education, and work, legal immigration—each of these reasons for citizens from abroad to enter a country offers opportunities for national prosperity. At the same time, the channels used for legitimate entry can be exploited by bad actors. Terrorism, human trafficking, and other types of international transgressions exploit every effort to make the travel experience easy for legitimate travelers. Government agencies must, therefore, strike a balance between attracting visitors with seamless border experiences and keeping their nations safe with strong identity controls. It's a tall order, which can only be fulfilled by a Solutions Titan with a long legacy of expertise and proven biometric digital identity technology.

Blending Security with Optimal Experience

Thanks to its partner network that spans airlines and airports, seaports, and land borders and includes over 70 governments, SITA is in the ideal position to ensure each stakeholder—from the government agencies to the travel companies to the citizens in motion—gets what they want at a border crossing. With its Digital Travel Suite comprising over 5,000 biometrically enabled touchpoints worldwide, SITA is leveraging eGates, Automated Border Control Kiosks, and the Digital Travel Ecosystem to provide a trust network for sharing Verifiable Credentials, like its game-changing Digital Travel Credential (DTC). Empowered by technical standards recently released by the UN's International Civil Aviation Organization (ICAO), SITA's DTC has already transformed the island of Aruba for the better.

Prime Time for Digital Travel Credentials

The story of SITA's Digital Travel Credential solution exemplifies the company's ability to pivot into success when faced with dynamic market conditions. During the pandemic of 2020, the government of Aruba was seeking solutions to resolve fraudulent COVID certificates that were required for visiting the island. Now that those credentials are no longer needed, and Aruba is back to competing with other vacation destinations to safely facilitate visitors, the DTC allows travelers to receive pre-approval for border control before leaving home. A traveler scans their passport with their phone to create a DTC, shares it remotely with the Aruban government, and are then issued a Trusted Travel verifiable credential while the government creates an arrival gallery for their visit. The result: the average border crossing takes only eight seconds and visitor data errors have been nearly eliminated. Thanks to DTC, Aruba is meeting its visitors with a friendly face while protecting its borders. And with SITA's Passenger Trends data showing that 85% of respondents believe this technology would be useful on their travel journeys, we see just how powerful a good user experience can be when it comes to driving the adoption of biometric digital identity for government services.

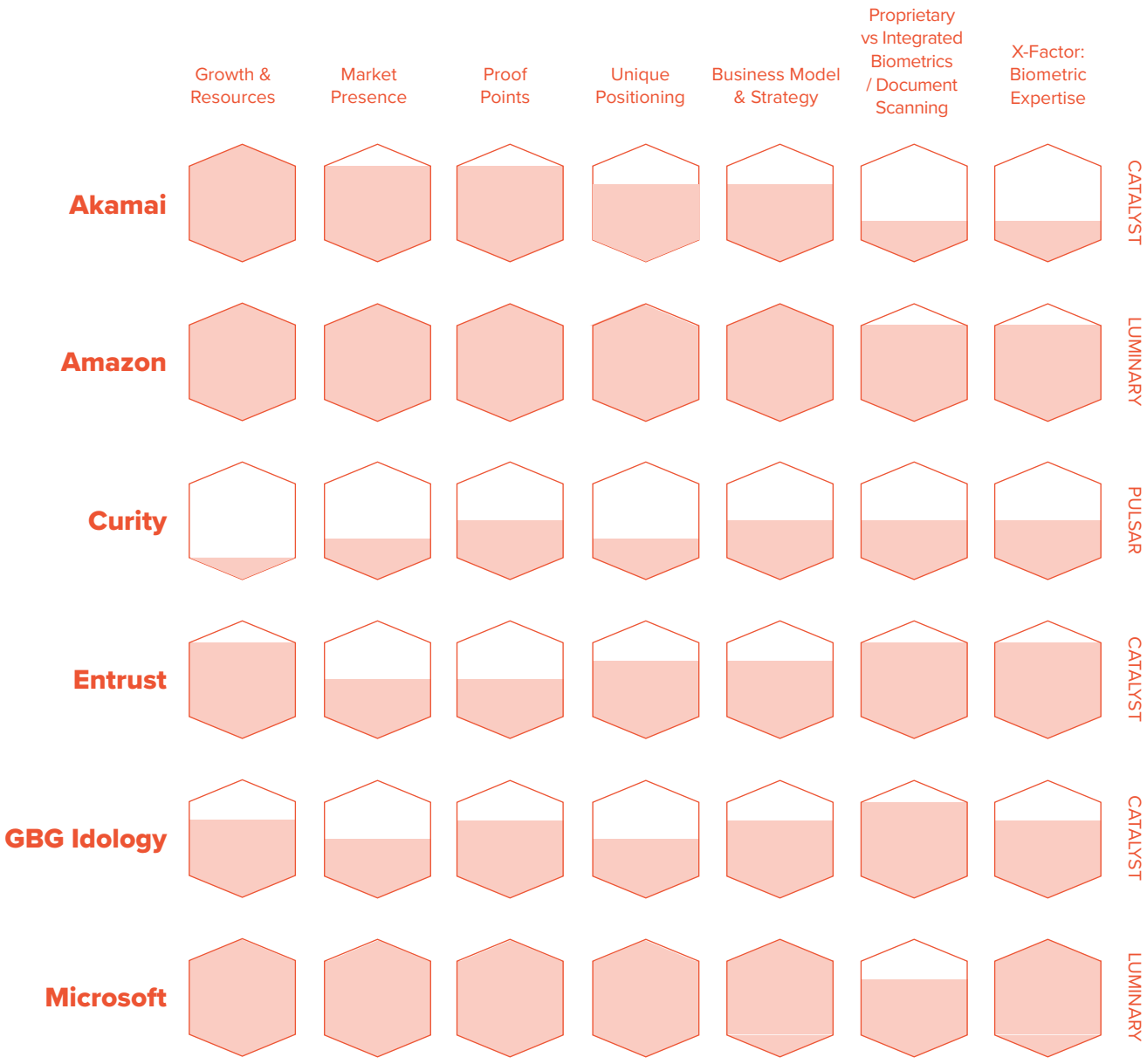
Contact SITA: Euro.iSales@sita.aero

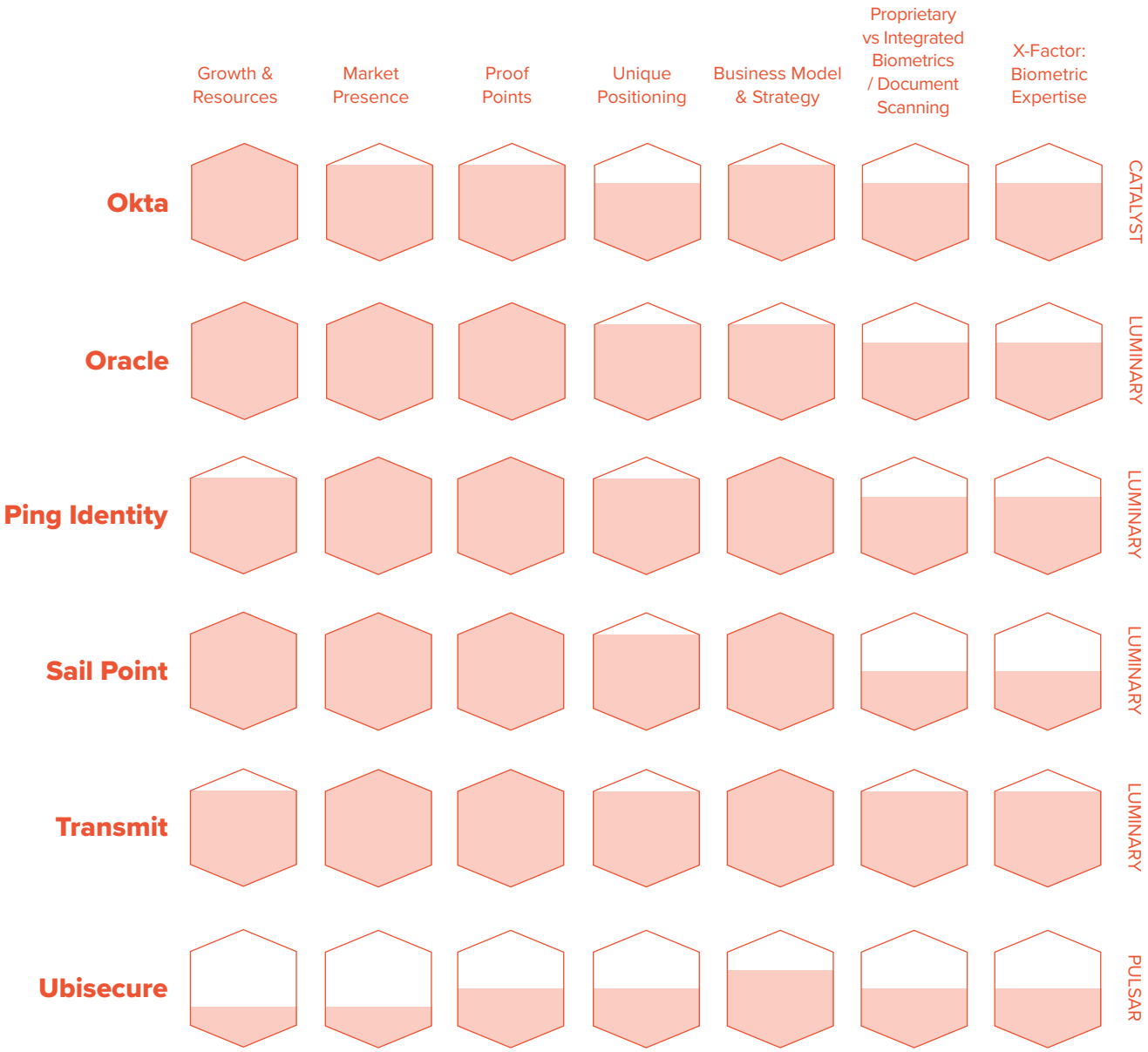
Identity Platforms

End-to-end orchestration for identity that may or may not include biometrics, but if included, biometrics are treated as a feature rather than a foundation.

Prism XFactor: Biometric Expertise

Evaluations



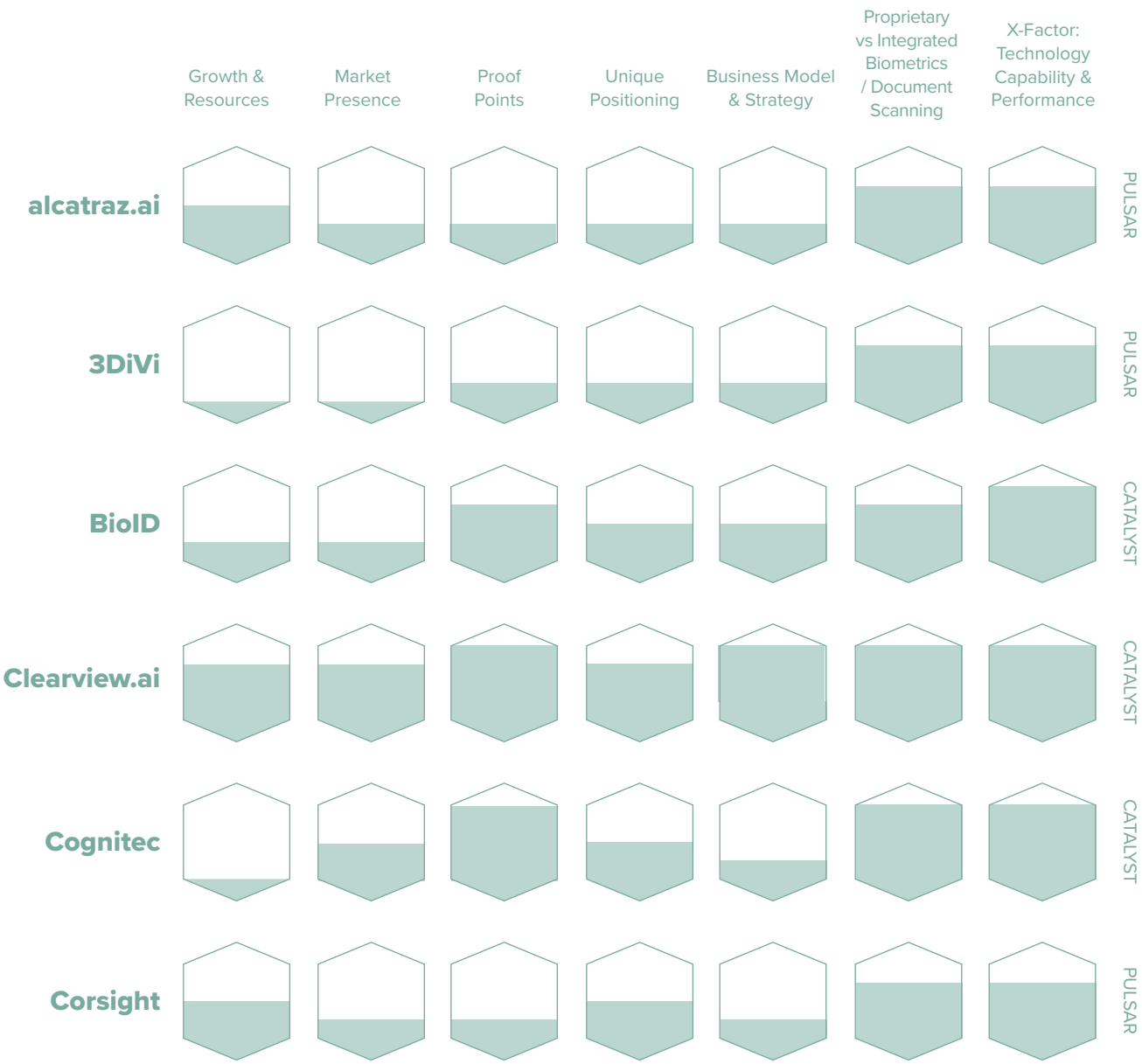


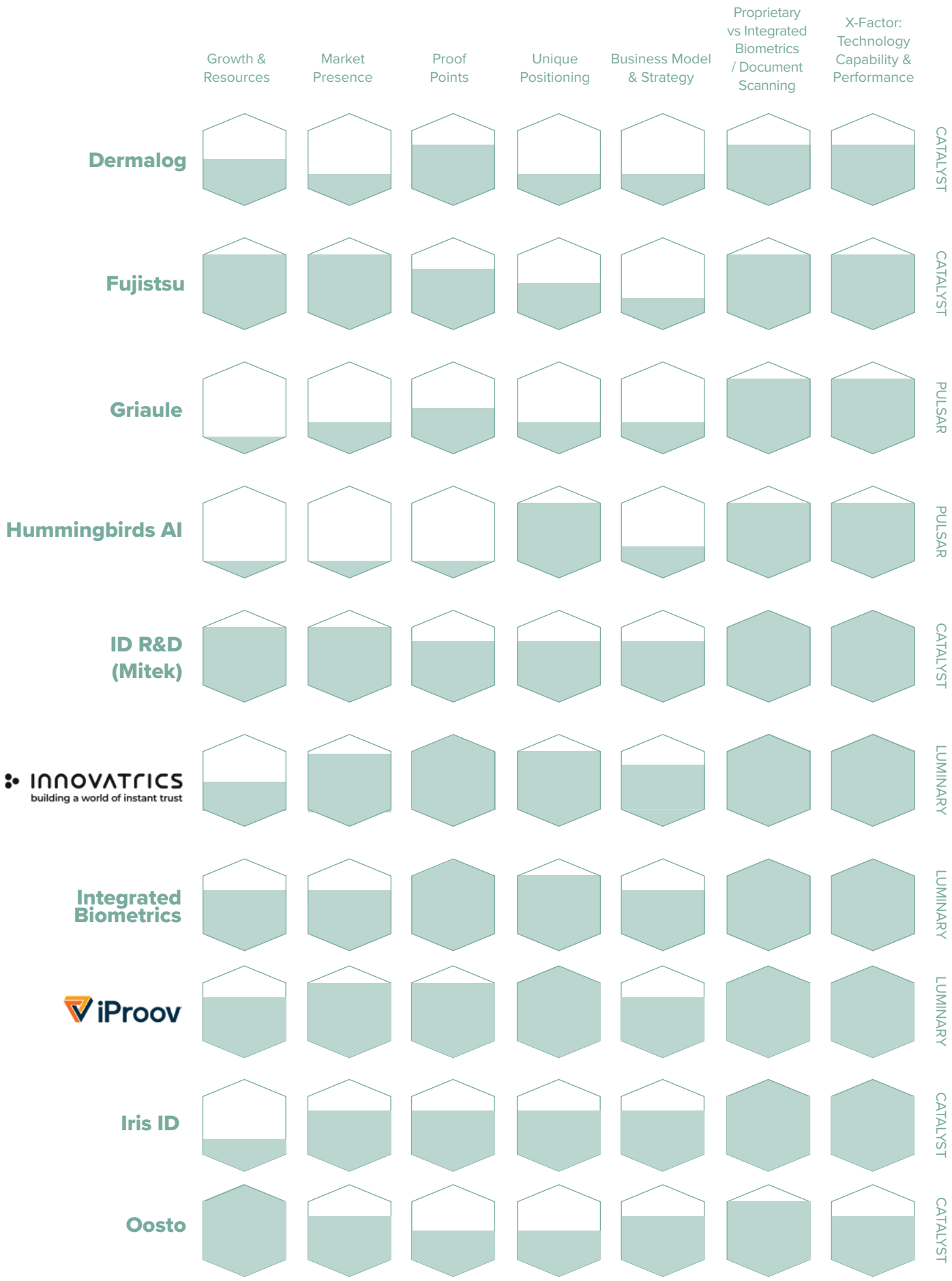
Biometric Core Technology

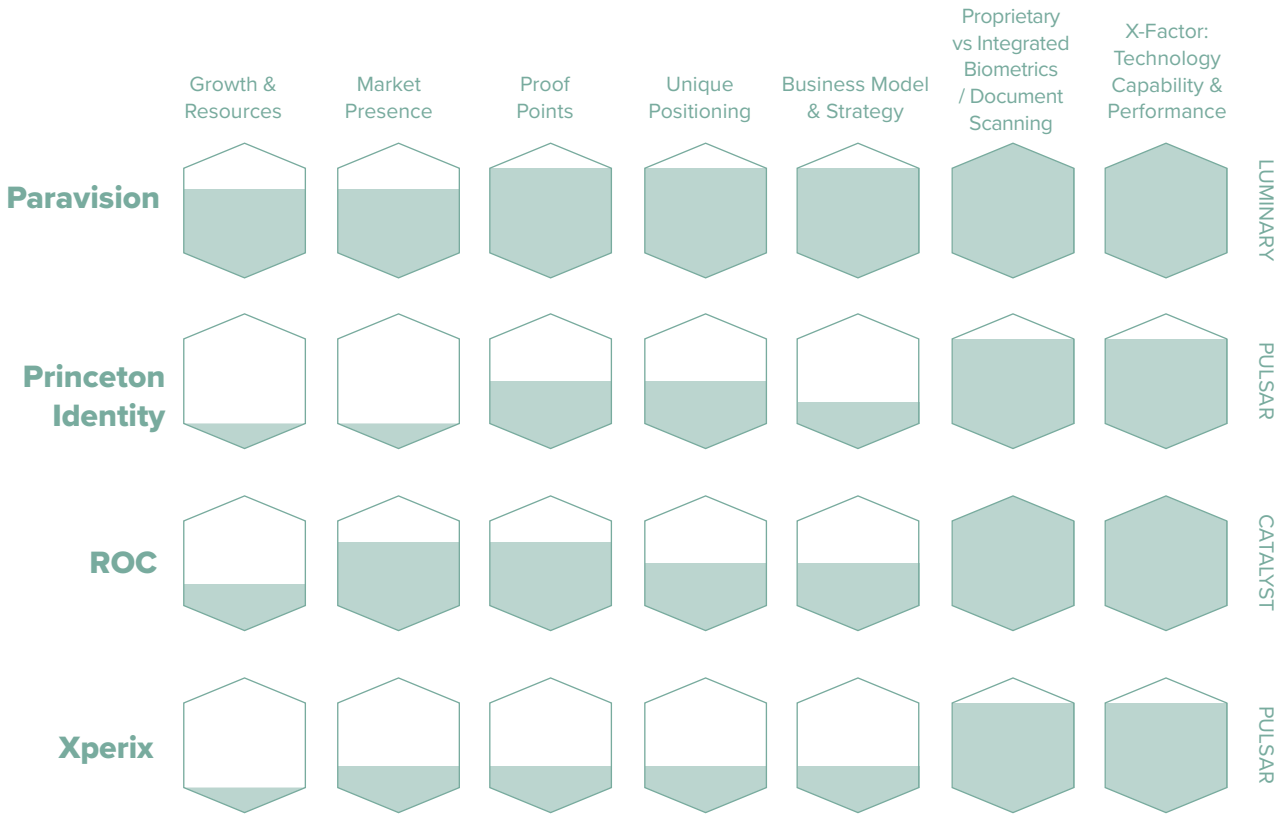
These vendors develop biometric core technology deployed across the Prism for verification, authentication, and to detect synthetic identities and deepfakes.

Prism XFactor: Technology Capability & Performance

Evaluations





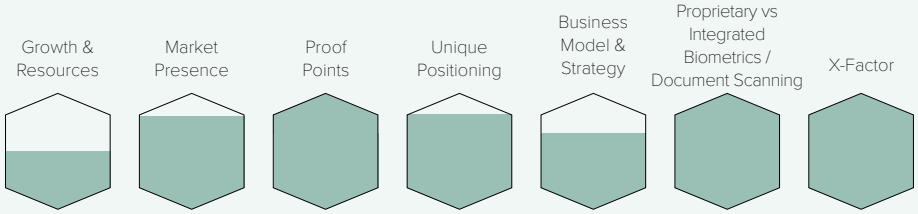


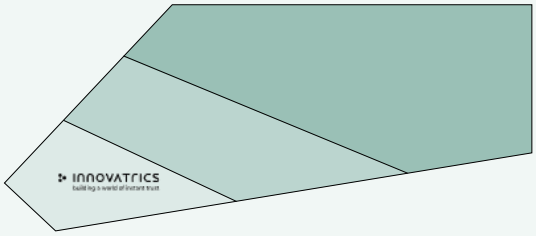
Innovatrics

innovatrics.com

INNOVATRICS
building a world of instant trust

BEAM: **Core Biometric Tech** / CLASSIFICATION: **Luminary**





Innovatrics is a Biometric Core Technology Luminary, benefiting over a billion users in 80 countries around the globe. Its flexible multimodal biometric solutions can be deployed on-premise—ensuring its customers are always in control of user data—enabling compliance with the stringent data storage and handling demands of government agencies. The company is renowned for its NIST top-ranked biometrics, powering its Automated Biometric Identification System (ABIS) and Identity Verification Toolkit (IDV Toolkit). These solutions are used to develop remote identity verification applications that are critical for government services in the era of digital transformation. They have been deployed with multiple governments around the world and in over 90% of cases show verification times of less than a minute.

The versatility of Innovatrics biometric technologies in government services is on full display globally, especially in Southeast Asia. In Indonesia, Innovatrics in cooperation with ASLI RI has contributed to electronic Know Your Customer (eKYC) services. Meanwhile, in Malaysia, these solutions help with onboarding and authentication for the country's top retirement savings fund. But Innovatrics' work with the Thai government is a particularly prime example of how it is enabling the biometric future of government. In 2019, Innovatrics ABIS was integrated by its partner CDT into Thailand's identity verification platform for national ID issuance for the Ministry of Interior, and in 2022, the government wanted to introduce remote services in line with the demands of digital transformation. Innovatrics IDV Toolkit was then deployed to enable smartphone-based unsupervised identity verification for the ThaID mobile app, building on the foundation of its ABIS to allow citizens to establish digital identity on their smartphones. The uptake is staggering. The country is now seeing 21,000 remote verifications per day from 75 million users, all of which benefit from biometrically bound foundational identity.

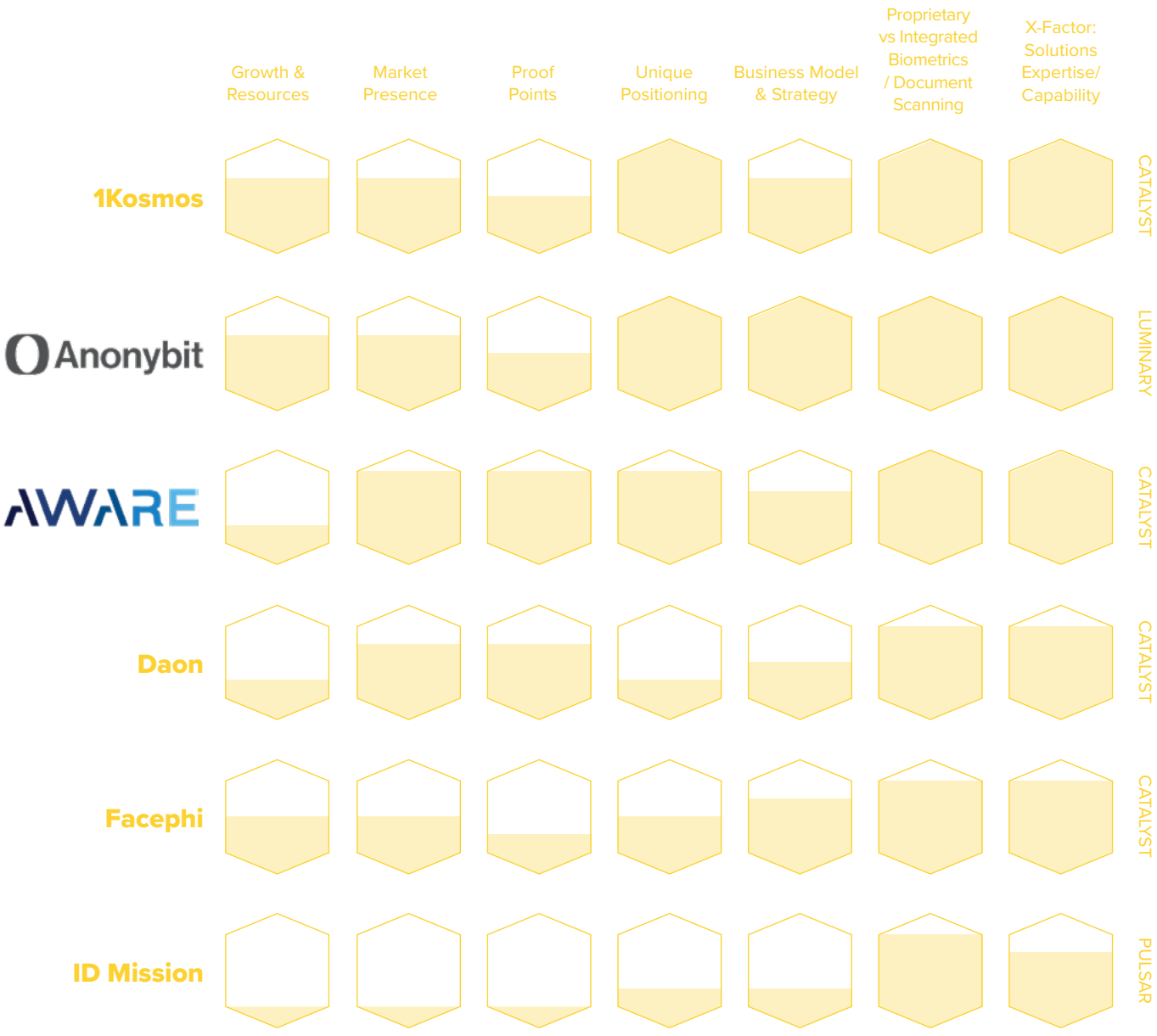
Contact Innovatrics: info@innovatrics.com

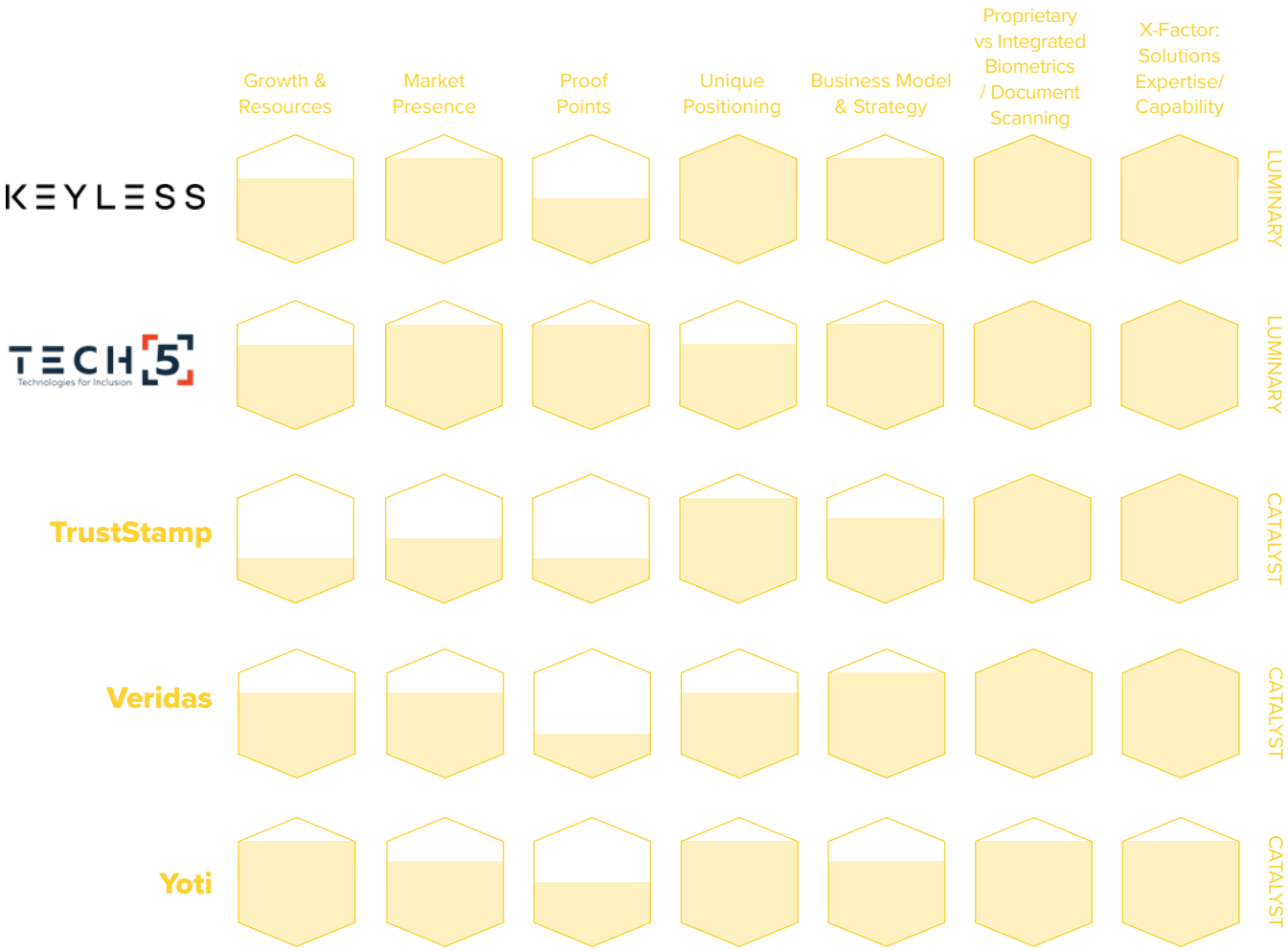
Biometric Identity Platforms

These identity platform providers enable end-to-end orchestration for identity in government services and are built on a foundation of biometrics.

Prism XFactor: Solutions Expertise/Capability

Evaluations

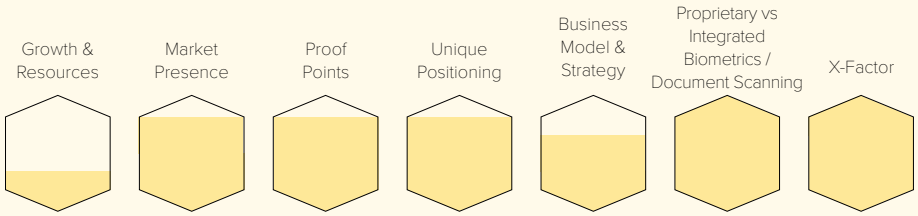


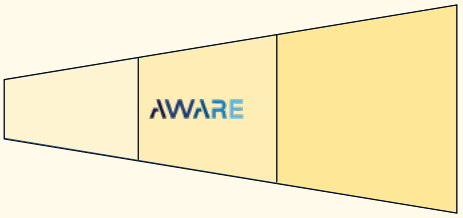


Aware

aware.com

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





A pioneer in biometric digital identity, Aware has deep roots in government applications, having collaborated with the FBI on the first large-scale fingerprint digitization effort back in 1993. Since then, the company evolved in lock-step with the biometric government services industry, offering end-to-end biometric software solutions to customers around the world, including 80 government agencies. Aware's comprehensive portfolio, spanning every biometric modality (face, fingerprint, voice, and iris), is trusted by its government clients, whether they are seeking solutions for defense and intelligence, law enforcement, border management, or citizen ID. With a reputation for being ahead of the curve thanks to consistently prescient R&D efforts, Aware's government solutions enhance security, tamp down fraud, and improve operations through accurate collection and sharing of biometric and identity data.

A Full Suite of Biometric Solutions

To call Aware's biometric digital identity offerings for government services comprehensive is an understatement. Its multimodal biometric components, developed in-house by artificial intelligence and machine learning scientists, enable the capture, comparison, analysis, and templatization of any biometric an agency needs. This core technology is supported by BioSP—Aware's Biometric Services Platform—which is easy to integrate and scale, enabling government agencies and systems to not just adopt biometrics for their needs, but interoperate with other agencies and systems.

Modular, Agnostic, Ready to Go

Government initiatives are incredibly complex. With multiple levels of buy-in required, budgetary restrictions, and byzantine funding and approval processes, the biometric digital identity solutions best suited for this environment solve problems without adding complexity. Aware's multimodal biometric components and BioSP platform are Commercial Off-The-Shelf (COTS) products. Proven reliable though extensive deployments in government use cases, these solutions are developed, tested, and ready to deploy. Aware's biometric product suite is pre-built and can meet complex demands without needing to be custom built—a process that adds time and cost to a program. The modularity of BioSP and its ability to perform well and connect in a variety of scenarios thanks to its agnostic support of biometrics and highly configurable nature has made it the choice of numerous government agencies including UK Home Office, Australian Department of Defense, U.S. Department of Defense, and U.S. Customs and Border Protection.

Full Court Spread

When an organization managing the non-judicial and administrative business of all U.S. federal courthouses required a web-based, centrally managed biometric identity enrollment solution for background investigations, Aware's approach to government services shone bright. Beyond the size and scope of the deployment, the solution needed to support multiple biometric capture devices from different vendors. The organization deployed WebEnroll, Aware's web-based enrollment solution powered by BioSP, featuring desktop and offline functionality. WebEnroll eliminated the IT overhead required to configure devices on each individual location. The organization was then able to push out updates to the various courthouses and facilitate the addition of new enrollment stations. The COTS system took about six months to customize and configure to the organization's requirements and was rolled out to its more than 358 touchpoints across 100+ courthouses. Still in use today, Aware's courthouse implementation of WebEnroll shows just how much a legacy of trust and a philosophy of usability is required to meet the difficult demands of the government services space.

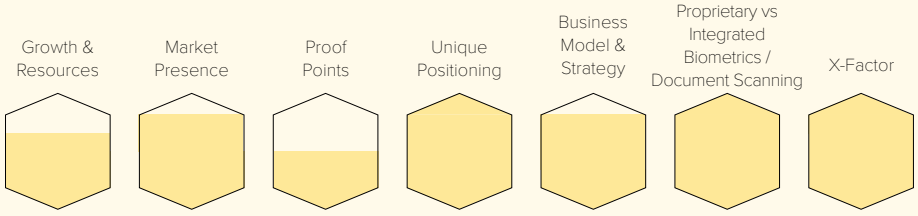
Contact Aware: Magruder Dent, Senior Director of Federal Business Development – mdent@aware.com – 240.715.5278

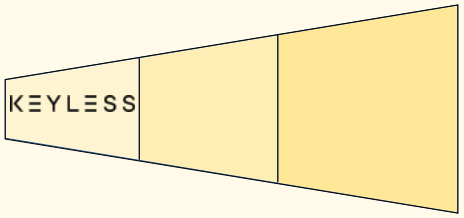
Keyless

keyless.io

KEYLESS

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





In the Biometric Identity Platform Prism Beam, Keyless stands out as a Luminary thanks to its patented Zero-Knowledge Biometrics™ technology, which ensures no biometric data is stored either on device or in the cloud. This privacy-preserving technology is at the heart of solutions like Keyless Consumer Authentication which solves government services pain points such as binding verifying claims to an individual, providing genuine identity assurance to government wallets and digital IDs, and recovering them if they are lost, stolen, or otherwise compromised. By orchestrating identity transactions with biometrics at the core across the entire user lifecycle, Keyless leverages a strong foundation to realize the full spectrum of the Identity Hierarchy, making it versatile enough to secure and enable government services that branch into other markets.

Healthy Authentication Practices

Government services have significant overlap with other markets, and when that overlap meets medicine, secure identity is crucial. Patient identity records are the most valuable PII (Personally Identifiable Information) on the dark web black market, sought after because of their application in the illegal drug trade. As such, the healthcare space has long been seen as an arena in dire need of biometric digital identity. Insufficient security, poorly managed records, and onerous account recovery processes all contribute to medical fraud. Enabling biometric digital identity to protect medical records and facilitate healthcare services can prevent that fraud while also improving the quality of care. This was the case with a regional healthcare provider within a government system in Europe that, after feeling the pinch of digital transformation, turned to Keyless for a solution.

Diagnosis: Digital Transformation

A government-funded regional healthcare provider responsible for serving tens of thousands of patients and medical professionals across many European clinics and hospitals faced numerous challenges associated with digital transformation. When operating on that scale, digital solutions are a necessity. But without biometrics at the core of its identity management, both security and usability suffered. Employees and citizens alike struggled to remember complex passwords that needed changing. Credentials were entered improperly, stored insecurely, and shared with others. And of course, phishing became a serious problem. The sheer inefficiency of the system, and the cost associated with the resulting fraud—not to mention the wider impacts of compromised medical records—led this healthcare provider to seek out Keyless.

A Prescription for Biometrics

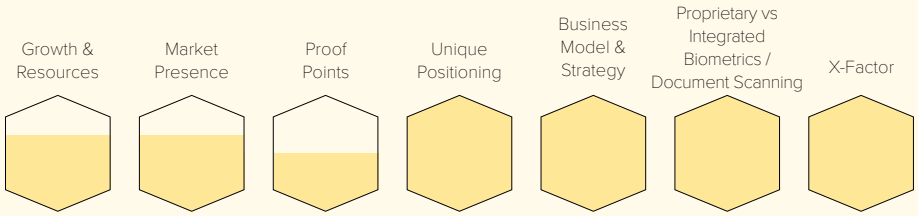
By deploying Keyless Consumer Authentication, the regional healthcare provider was able to address all the security and usability challenges inherent to digital portals and apps. Biometrics, by their nature, cannot be shared, stolen, or forgotten. That means that when the healthcare provider deployed facial recognition as a password replacement, its user base became immune to phishing attacks, and the poor password hygiene prior to implementation evaporated. Keyless' solution was fully deployed in two months, immediately speeding up the authentication process, with authentications clearing in under 300 milliseconds. Within six months, the provider saw a 64% reduction of account takeover fraud. Healthcare is safer and easier to access for tens of thousands of citizens thanks to this direct application of biometric digital identity.

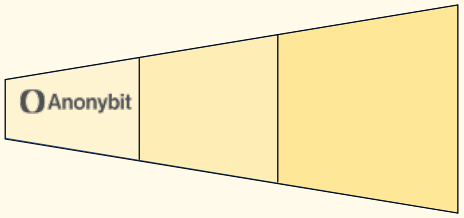
Contact Keyless: info@keyless.io

Anonybit

anonybit.io

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





Using biometrics for the high-risk applications of government services is a risky proposition, one that often requires compromise between user experience and security. Anonybit changes that. This Prism Luminary's one-of-a-kind technology takes a unique approach to data storage, breaking up biometric templates into encrypted fragments and distributing them across a network. This naturally eliminates honeypot risks—in which rich stores of valuable data are targeted by hackers—while protecting user privacy and enabling convenience in lock step with security. The data protected by Anonybit does not need to be reassembled from its fragments to be matched, allowing it to be used as a single source of identity for the entire identity lifecycle, enhancing privacy, security, and compliance while enabling transactions at every level of the Prism Identity Hierarchy. And it's flexible. Compatible with all biometric modalities—including face, fingerprint, voice, and iris recognition—Anonybit's biometric identity platform can perform 1:1 matching in under 200 milliseconds and 10 million 1:N searches in a split second.

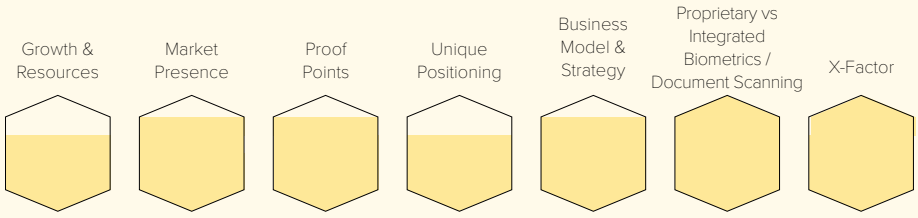
In an era defined by fraud and cyber-attacks, Anonybit secures government agencies from threats in both citizen-facing contexts and employee-facing applications. Its decentralized approach to storage and matching ensures that the data breaches of the past—like the 2015 Office of Personnel Management (OPM) disaster that affected 22.1 million records and saw the theft of 5.6 million fingerprints—are impossible. Meanwhile, it's 1:N search capabilities allow for deduplication, ensuring a user's records are all only associated with their individual biometrics, thereby creating efficient and clean databases and preventing synthetic identities from taking root. Perhaps most importantly, Anonybit's technology enables biometric enrollment and subsequent authentication that's robust against deepfakes and AI-based fraud attacks, ensuring that every point of contact between a user and their government is facilitated by unimpeachable biometric identity. From onboarding, through authentication, to account recovery, Anonybit's elegant vision of uncompromising identity is set to be a boon for governments and their citizens, closing what CEO Frances Zelazny calls "The Circle of Trust."

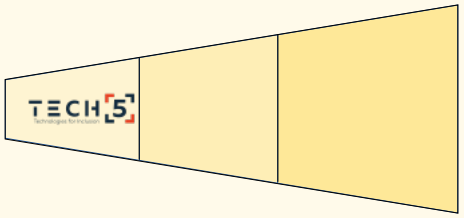
Contact Anonybit: info@anonybit.io

TECH5

tech5.ai

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





Since 2018, TECH5 has been innovating in the realm of multimodal biometrics and digital identity management. An international company, its focus on multi-modal biometric and digital identity technologies supported by AI and machine learning has consistently placed its fingerprint, face, and iris recognition algorithms at the top of the National Institute of Standards and Technology (NIST)'s performance rankings. Boasting a global footprint and guided by a mission of inclusion, TECH5 serves over a billion users. And its work in government services shows the breadth of its capabilities. From providing biometric voter registration for elections in Jamaica and Oman, to enabling secure and convenient digital transformation in Africa, to facilitating better border control with Finland's Digital Travel Credential (DTC) — this Prism Luminary is helping put biometrics at the core of people's relationship with their institutions.

When a federal government in Africa wanted to deliver services to a large unbanked population, TECH5 rose to the occasion. Supported with funding from World Bank, the UN, and its own treasury, the government in question worked with TECH5 to deploy the company's digital identity infrastructure solution. Supported by its decentralized identity technologies and an application layer that enabled the creation and issuance of digital IDs, TECH5's platform was implemented in only three months' time. Now, the country is able to create and distribute digital identity documents to every citizen. Those digital identities, biometrically bound to their users, provide the foundations needed for economic and social participation no matter where their users are from, or how their history has so far kept them from civic engagement. TECH5's work is a glowing example of how a mission to include everyone in government services, supported by real innovation and expertise, can make life more inclusive for everyone.

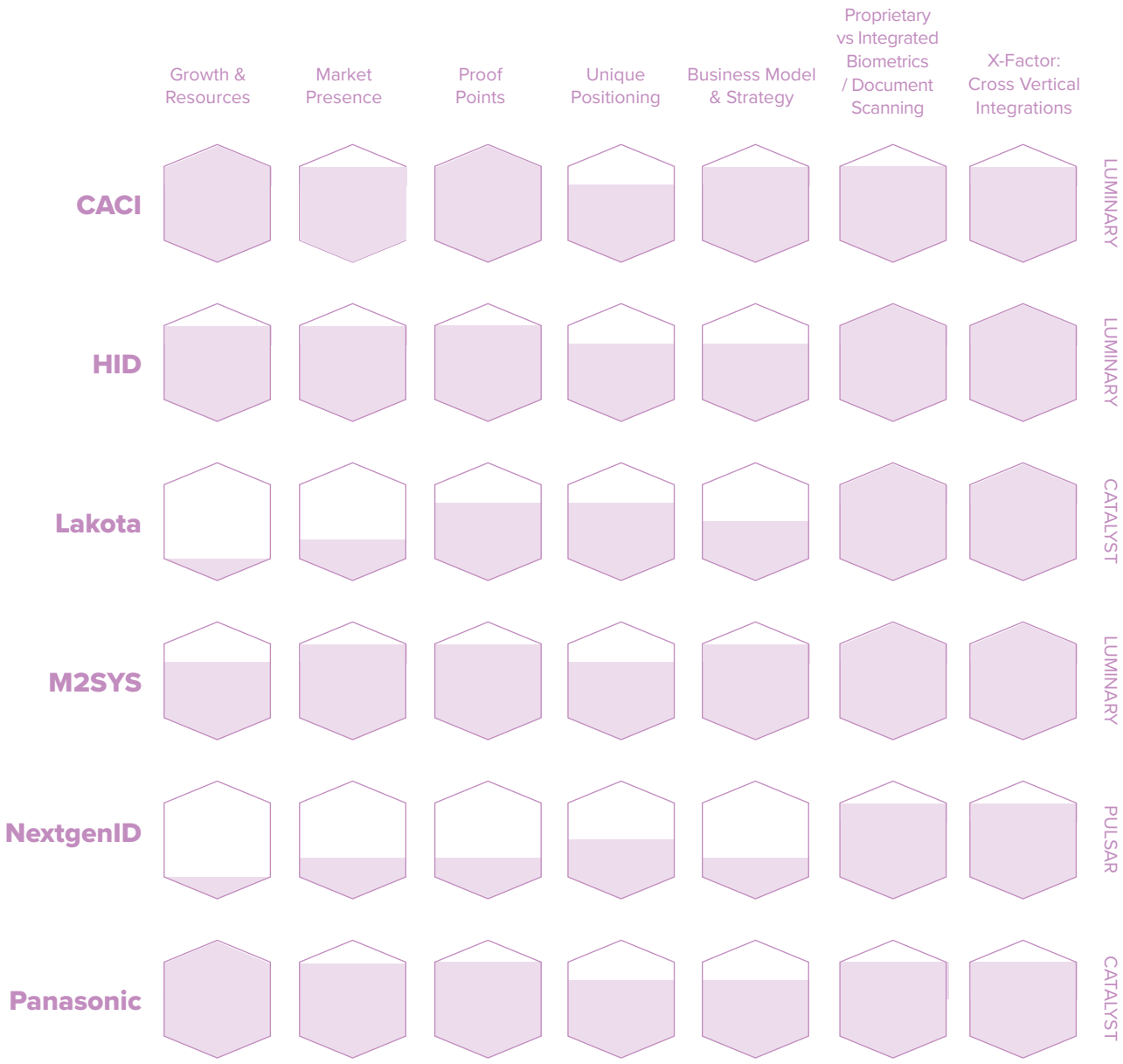
Contact TECH5: sales@tech5-sa.com

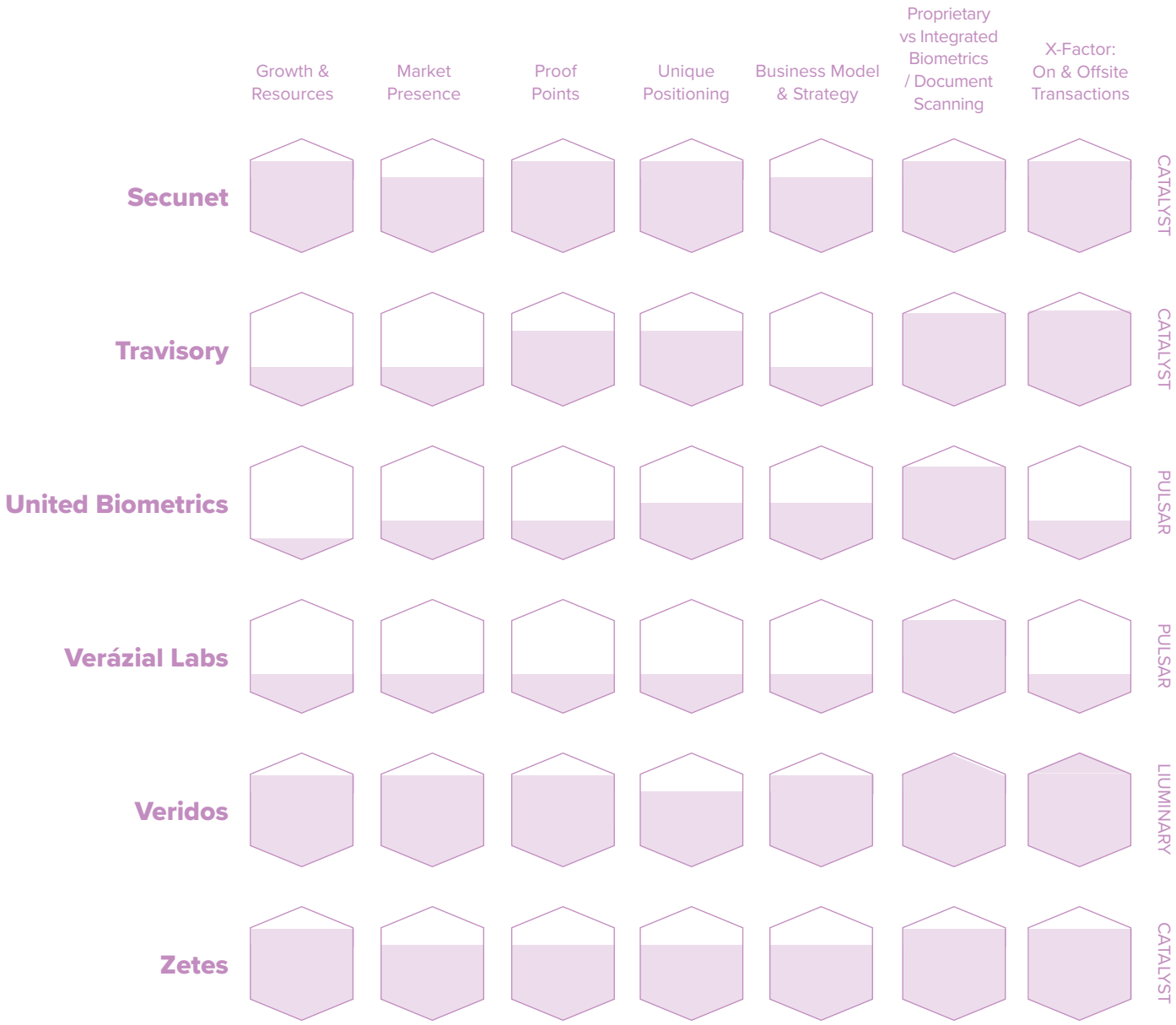
Targeted Government Services Solutions

Proprietary and native biometrics into specialized solutions purpose-built to deliver government service identity applications.

Prism XFactor: Integrated Mobile Onboarding, Payments, Cross Vertical Integration

Evaluations



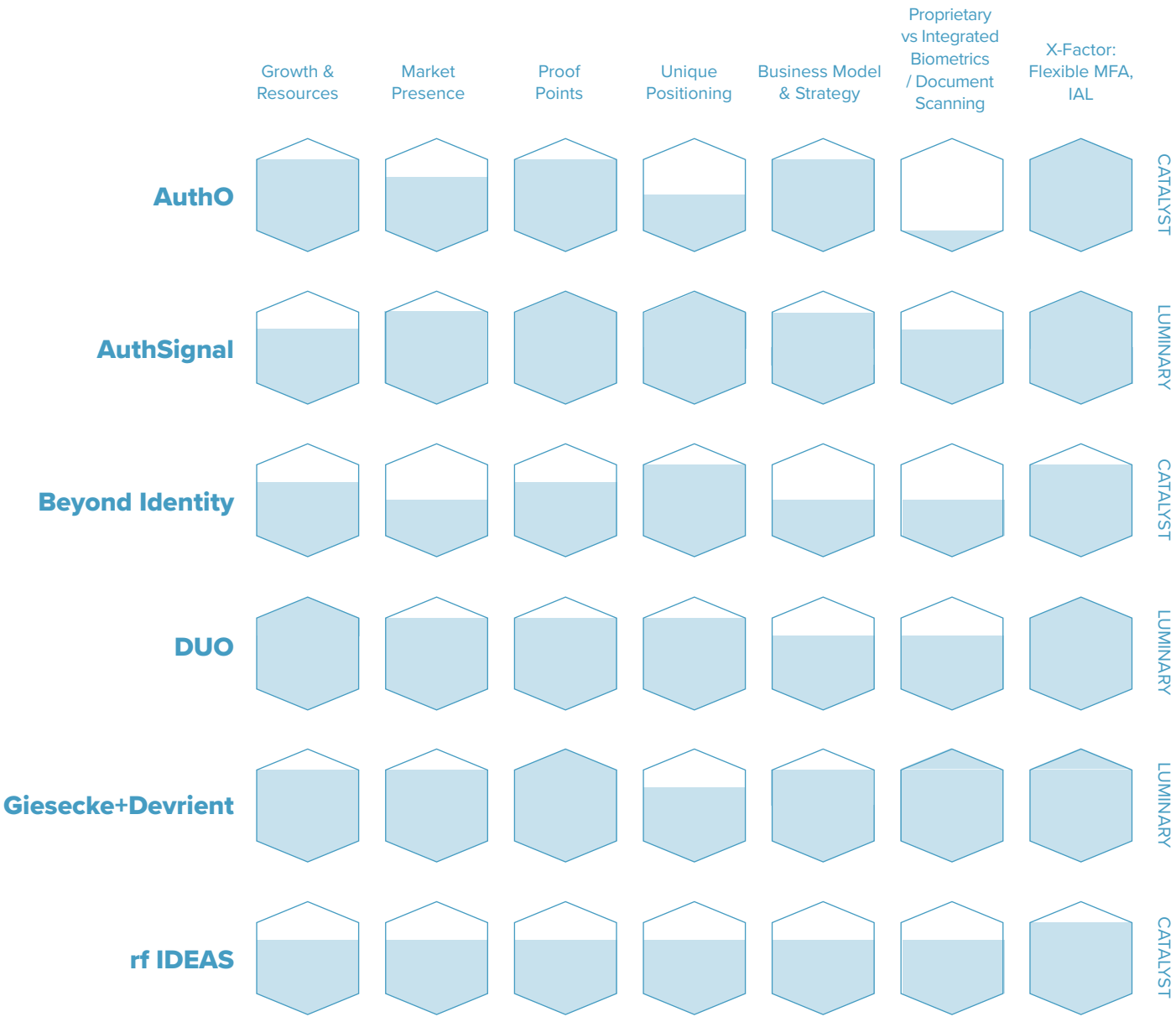


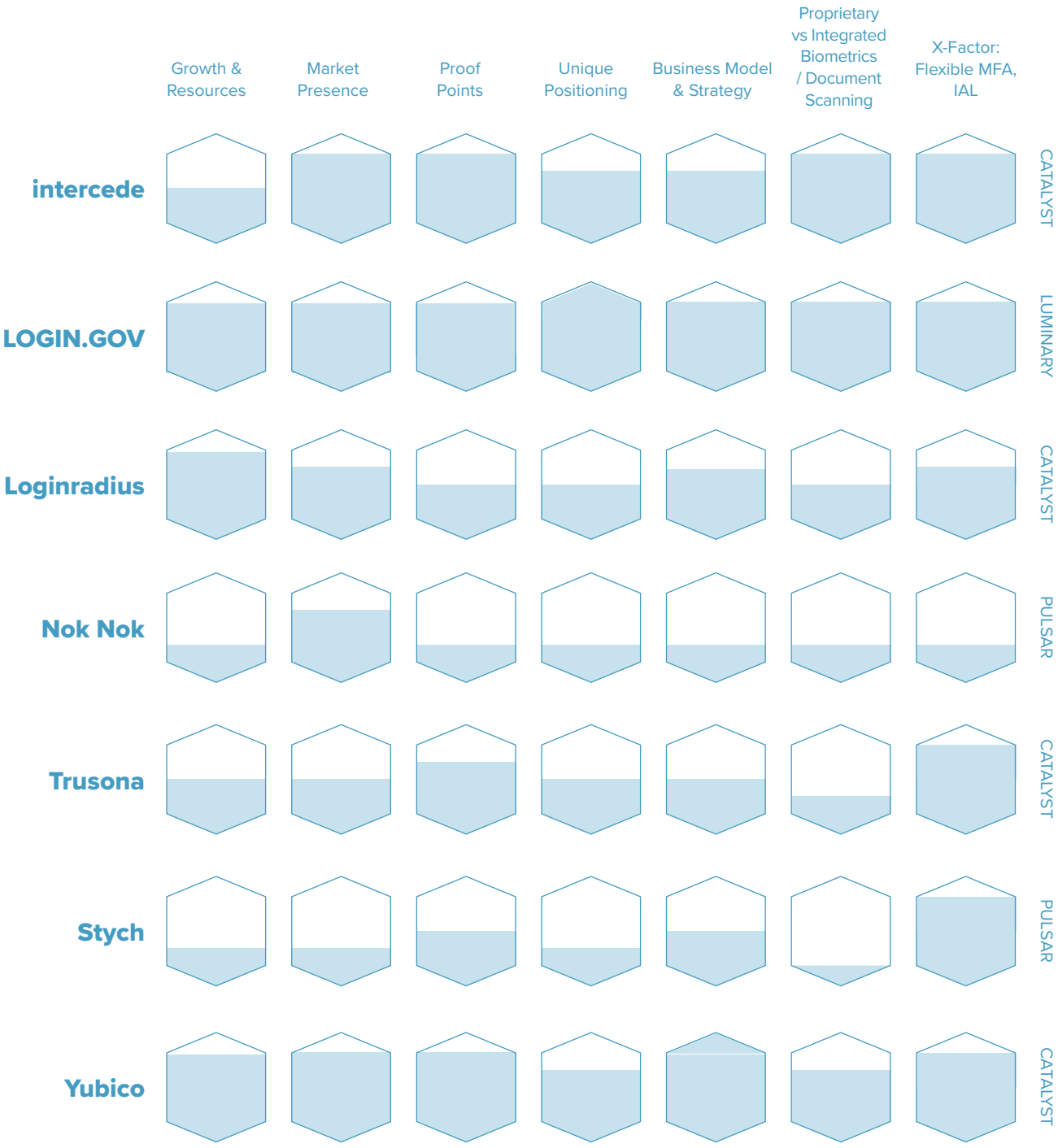
Authentication

Biometric and non-biometric security that links a digital identity to an individual for physical and logical access.

Prism XFactor: Flexible MFA (Multifactor Authentication), IAL (Identity Assurance Level)

Evaluations



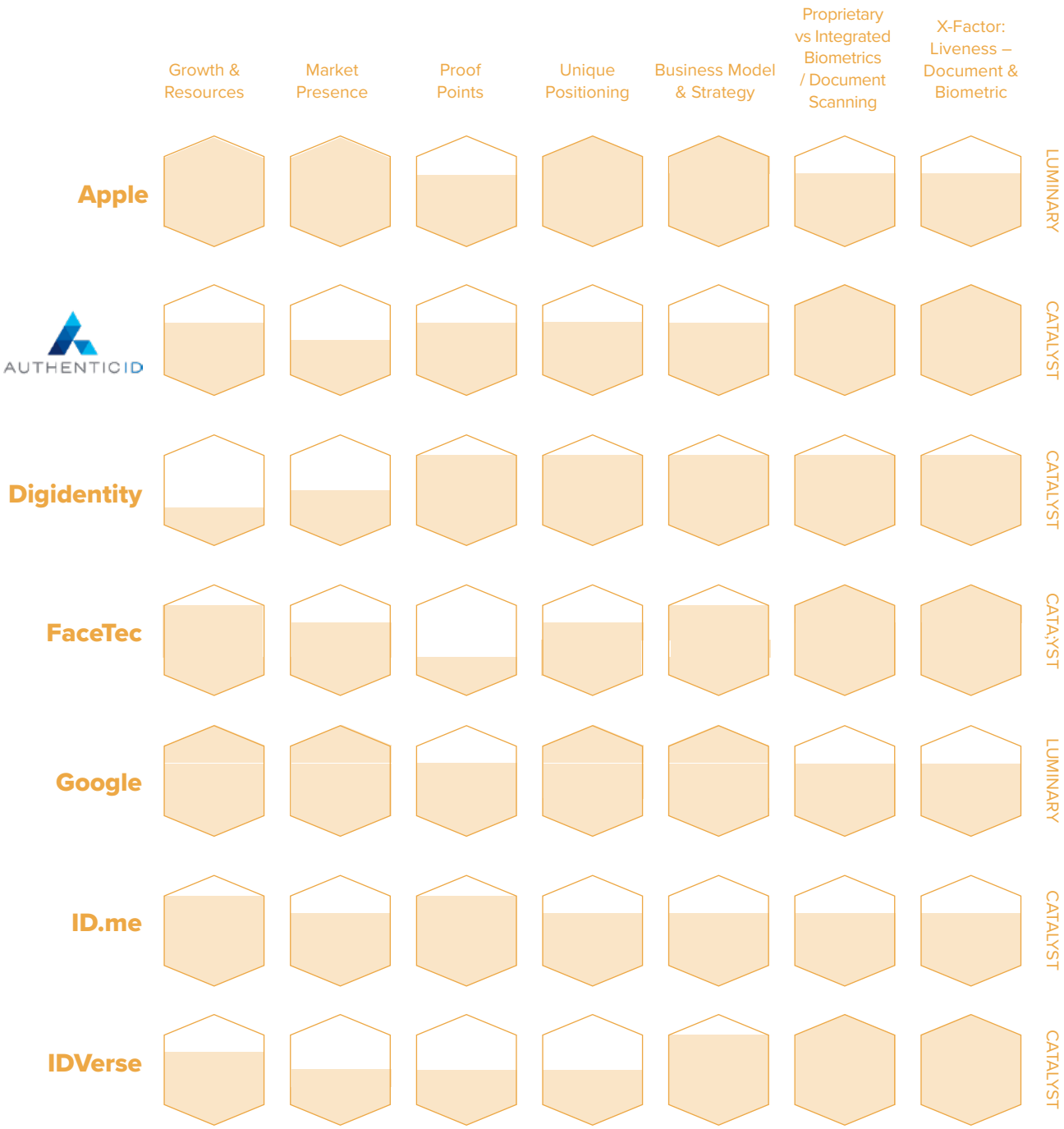


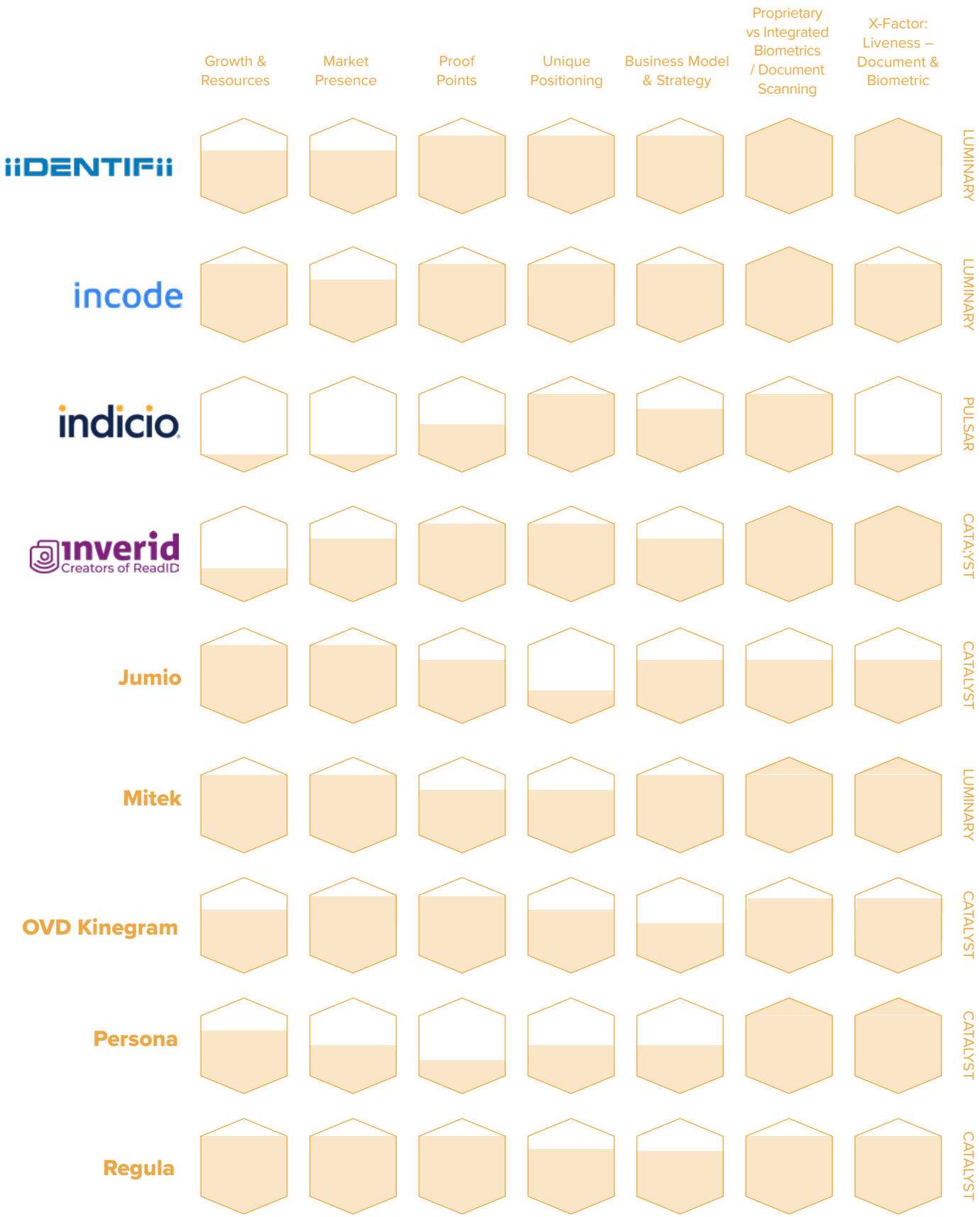
Remote Identity Proofing & Verification

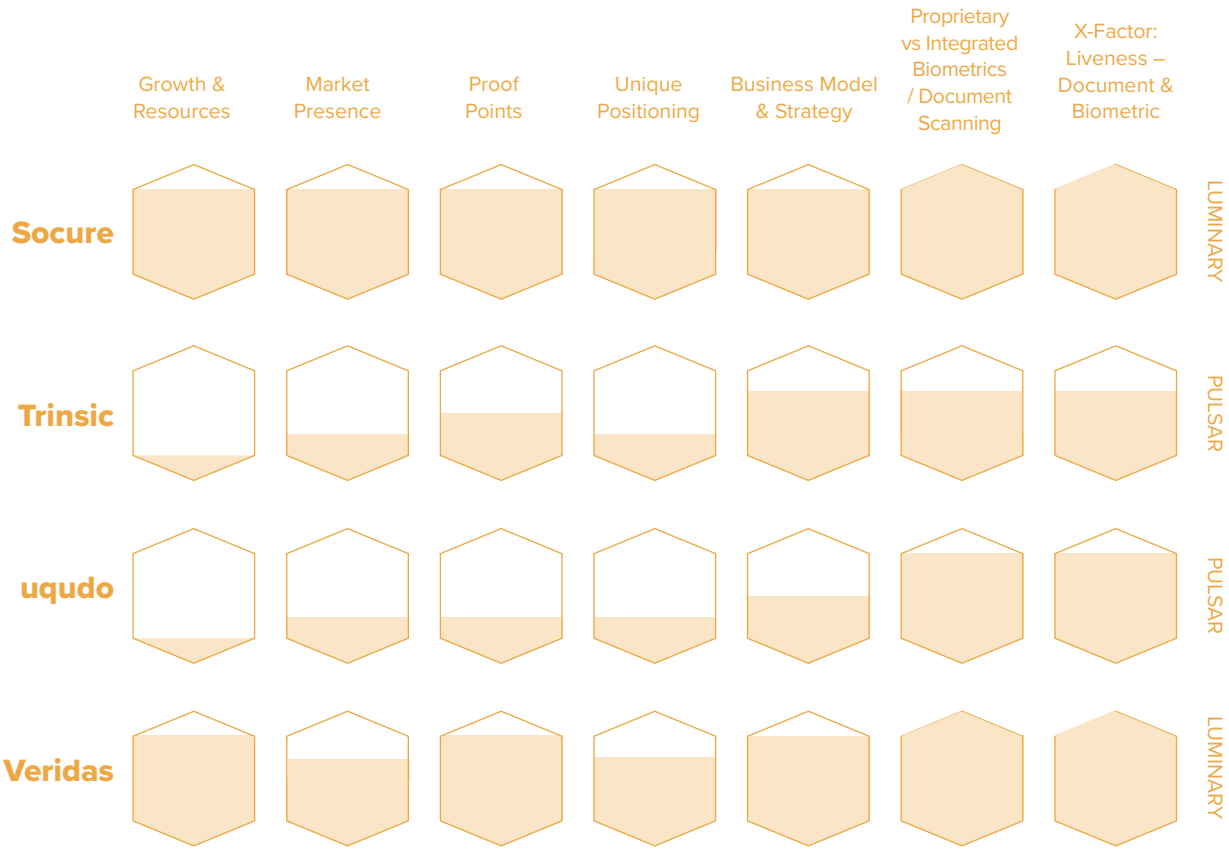
Leveraging biometrics, OCR, NFC, Verifiable Credentials, etc, to enable remote onboarding and authentication for access to a range of high-security and customer experience-enhancing applications.

Prism XFactor: Document and Biometric Liveness

Evaluations



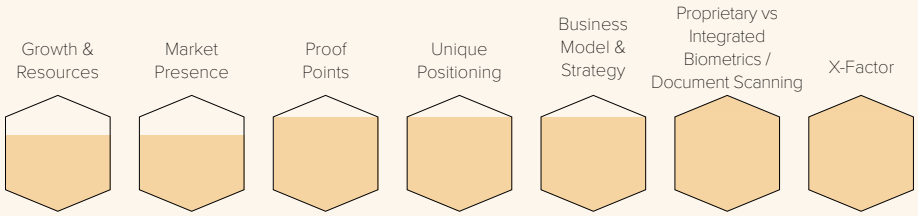


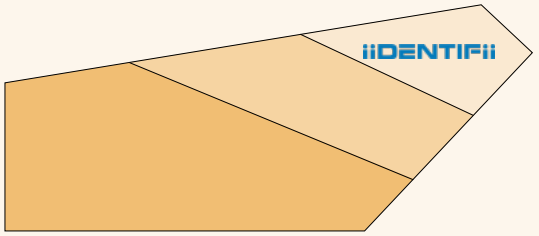


iiDENTIFii

iidentifii.com

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





Based in South Africa, iiDENTIFii is a shining example of how a strong foundation of identity, grounded in a government system of record, enables the full spectrum of transactions outlined in the Prism Identity Hierarchy. Existing integrations with government databases bind users' foundational and biographical identity with their biometric human identity, enabling high risk transactions. That assurance comes with no extra friction. With no-code and low-code solutions, iiDENTIFii's IDV technology is quick to deploy, using face biometrics supported by 3D and 4D Liveness—a proprietary technology that incorporates a dimension of time when verifying user identity. In the age of AI-enabled fraud and synthetic identities, that temporal element makes a huge difference. And that's especially true as the South African Government undergoes its digital transformation.

In government services, iiDENTIFii can enable secure access, fraud prevention, and identity verification for both public sector employees and citizens. With biometrics at the core, iiDENTIFii's government customers significantly mitigate the threat of fraud—be it account takeover or synthetic identities—while enhancing citizen experience and uptake of services. Trusted biometrics, bolstered by a system of record, means that the integrity of citizen identities verified through iiDENTIFii's technology are strong enough to enable transactions ranging from voting remotely, to collecting pensions, to verifying age of majority for alcohol purchases. And thanks to built-in redundancies that enable offline identity verification when networks go down or connectivity is out of reach, citizens can participate in government processes with the convenience they expect form a digitized future whether they're in a major city, a rural area, or a digital desert. That's the future of government services when biometrics are at the core: convenient, secure, and reliable

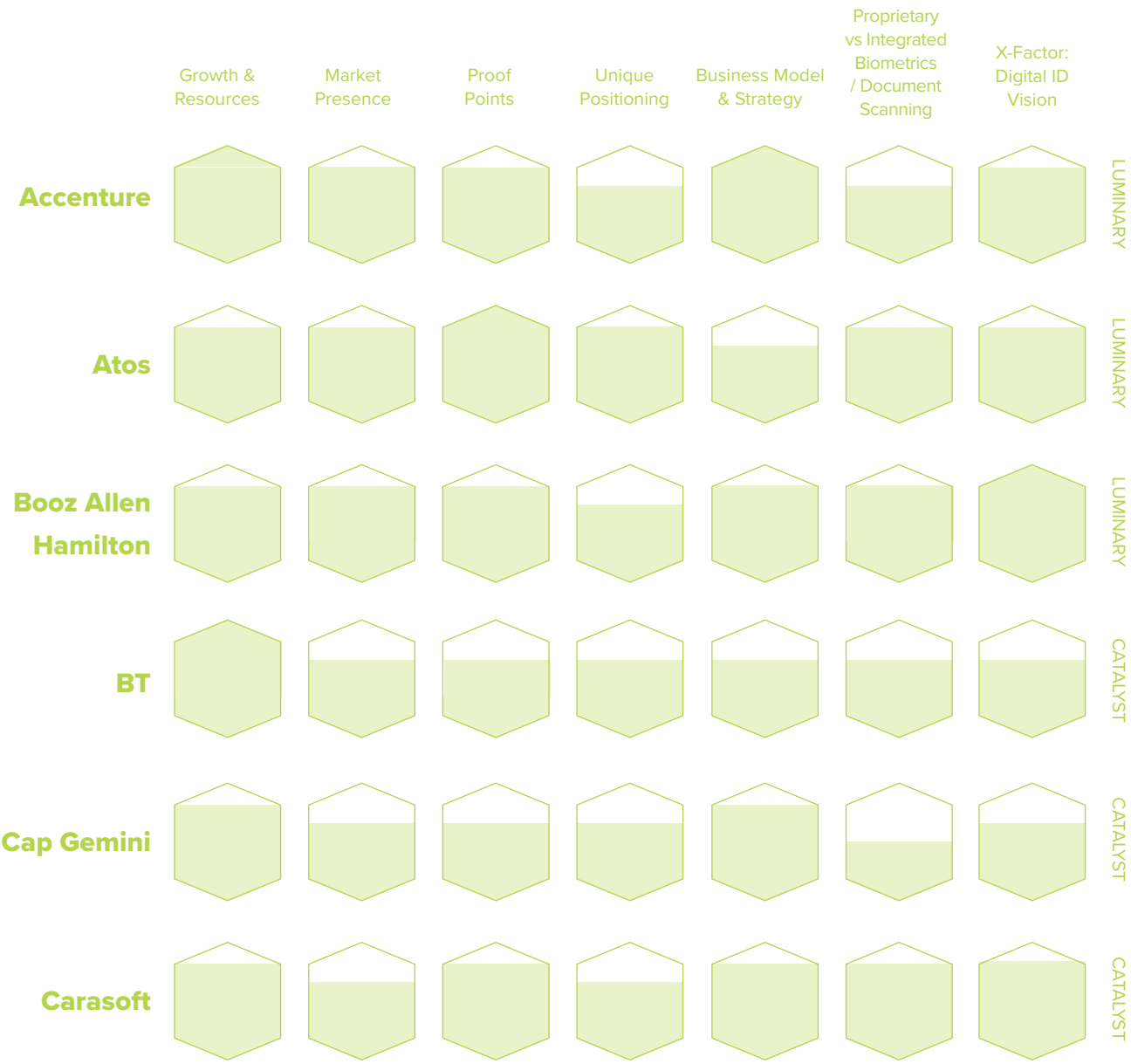
Contact iiDENTIFii: info@iidentifii.com

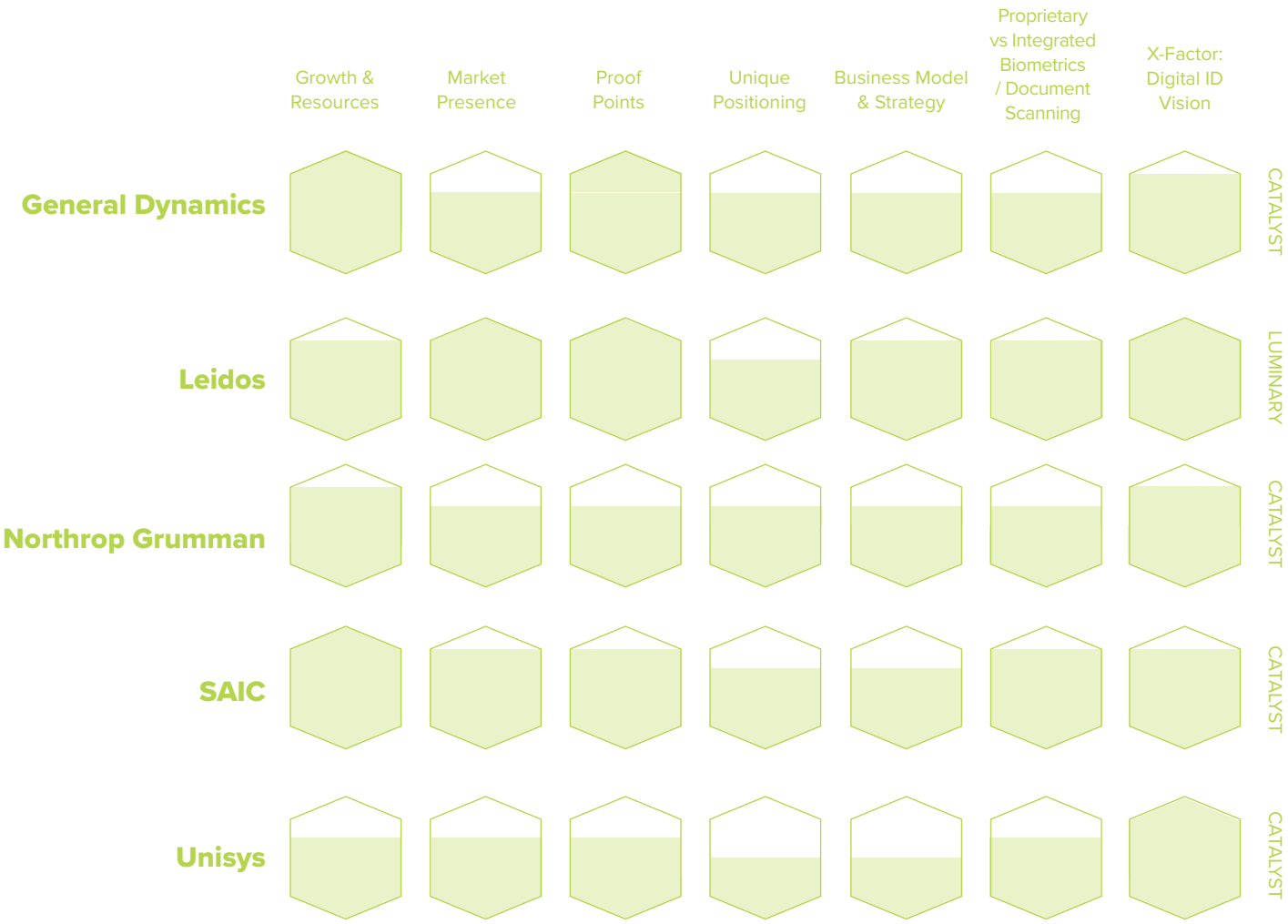
Integrators

These organizations provide customized solutions that integrate components from across the Prism Beams.

Prism XFactor: Biometric Digital Identity Vision

Evaluations





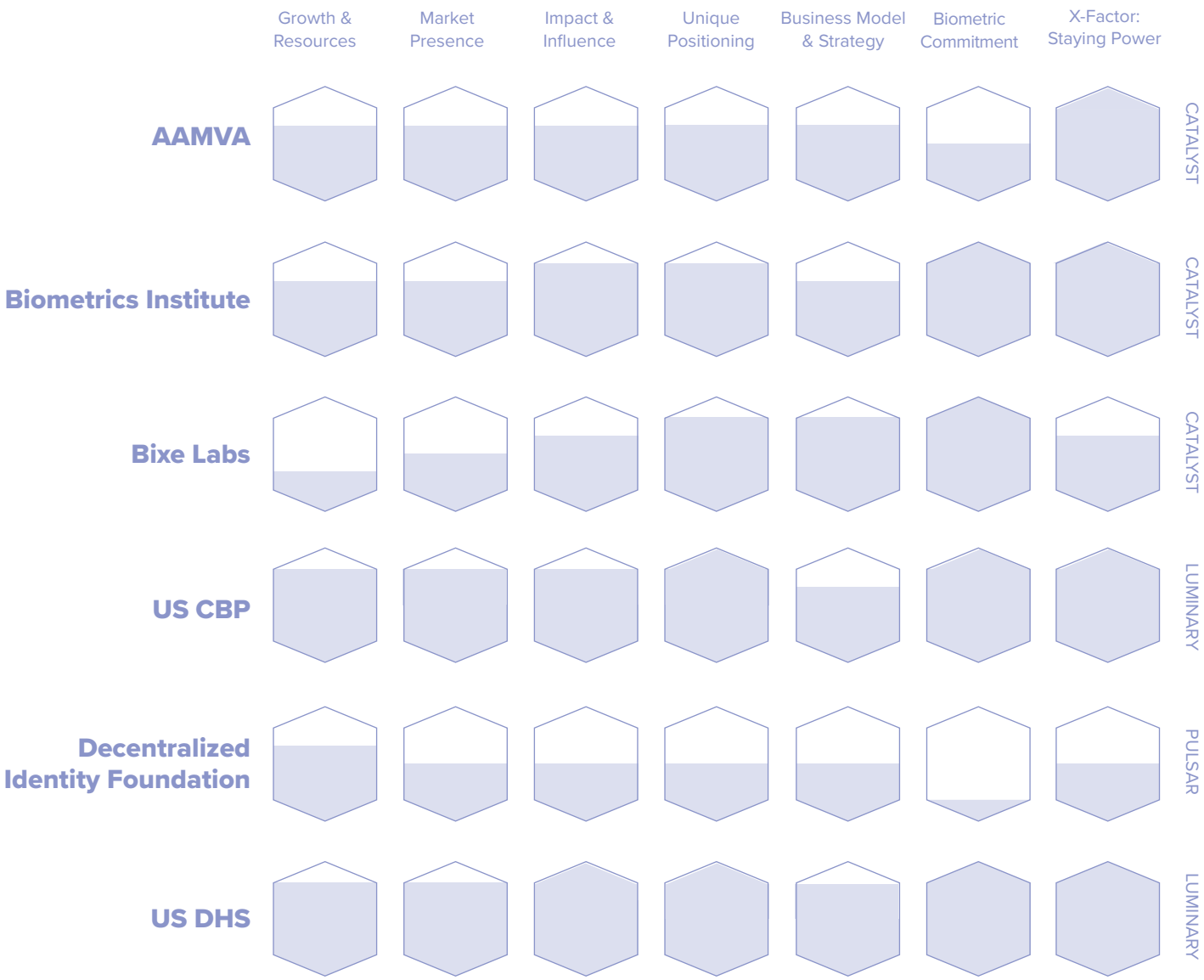
Infrastructure

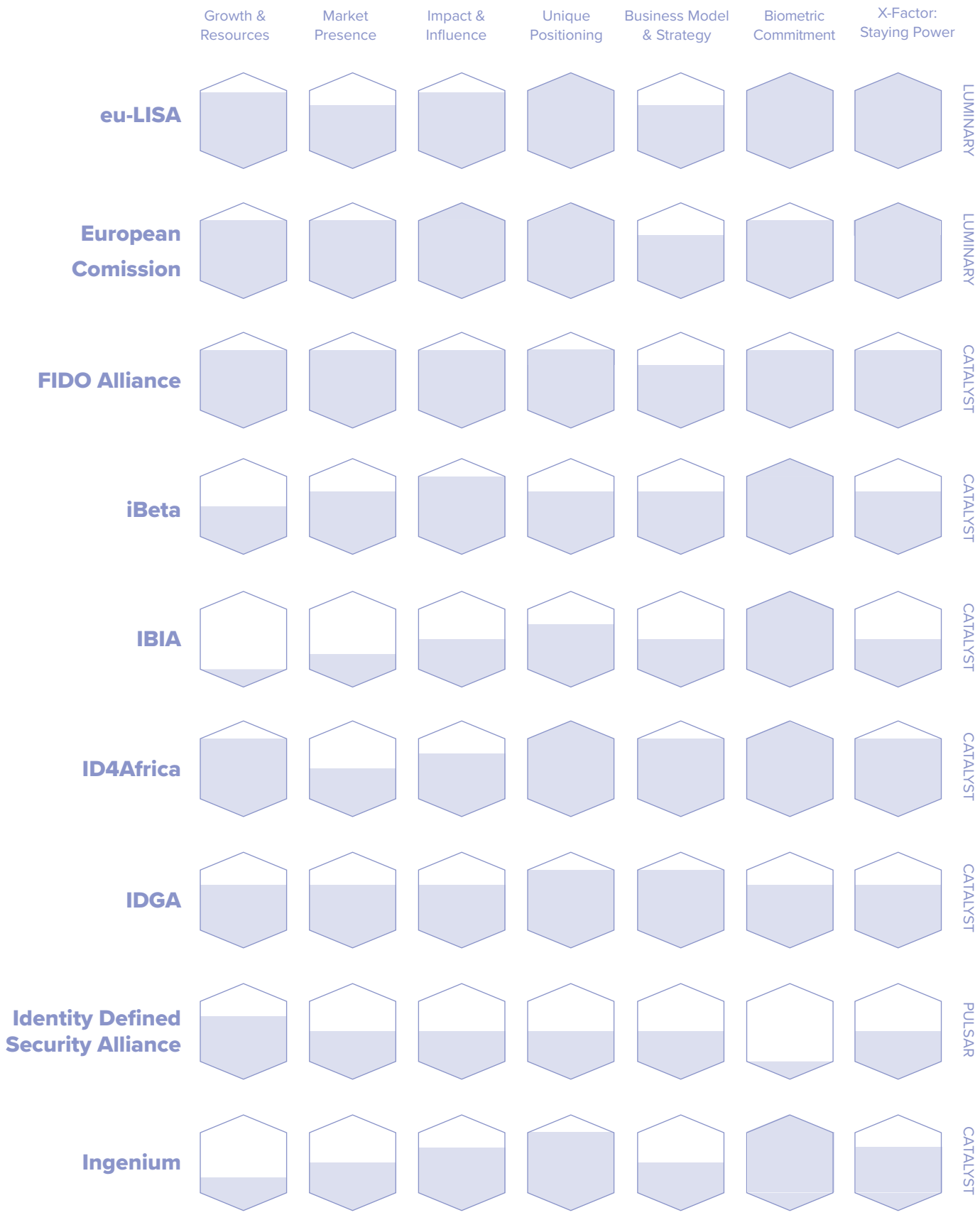
Standards bodies, testing companies, and non-governmental organizations provide the critical infrastructure required for market maturity and mainstream adoption.

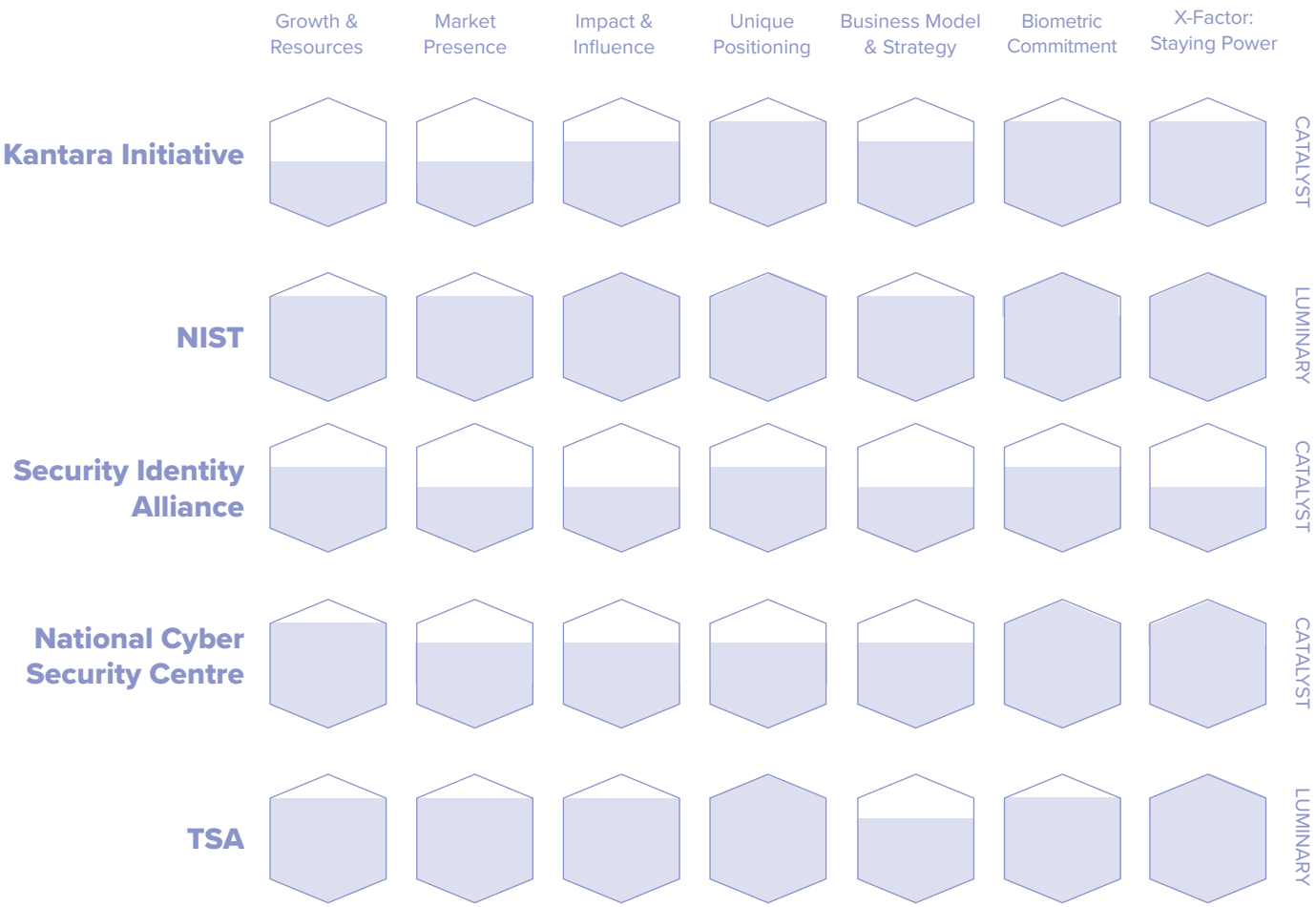
Prism XFactor: Staying Power

Evaluation Note:
The Infrastructure Prism Beam contains the unique criteria "Impact & Influence" and "Biometric Commitment."

Evaluations



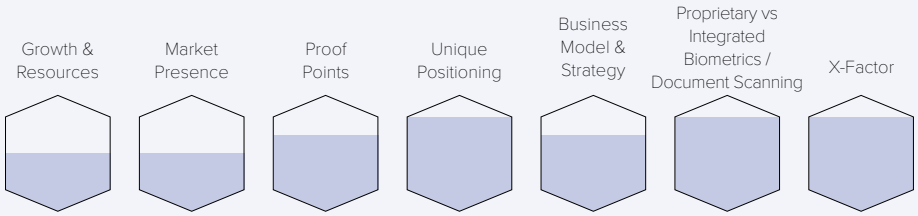


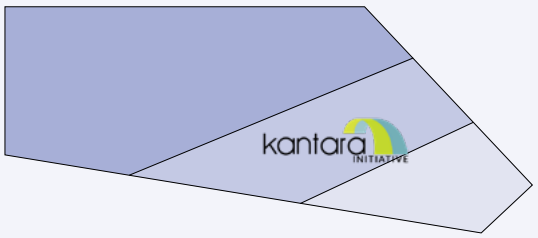


Kantara Initiative

kantarainitiative.org

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





Founded in 2009, the Kantara Initiative is a non-profit trade association dedicated to improving the trustworthy use of identity and personal data. The high-stakes nature of government services requires Infrastructure Catalysts like Kantara, which—in addition to its work groups, discussion groups, events, and reports—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. With dozens of organization members backed up by a host of notable individual contributor members, the Kantara Initiative is providing the framework that will support a future characterized by the responsible capture, sharing, storage, and verification of identity data.

Working Together

Kantara's work groups engage every major identity challenge identified by The Prism Project in the government services space. From 'Privacy Enhancing Mobile Credentials' and 'Diversity, Equity, Inclusion & Accessibility,' to 'Deepfake Threats to Identity Verification & Proofing,' Kantara Work Groups provide the identity industry's most prominent figures with the opportunity to collaborate on the groundwork for an identity-safe future that's fully inclusive, compliant, and consensual. Whether it's identifying the changes that need to happen in our rapidly digitizing society so that everyone can participate, or researching how identity proofing and verification systems—which are essential to securing digital government services—can distinguish between real users and AI generated deepfakes, Kantara's Work Groups are actively guiding the industry through engaged discussion between relying parties, government agencies, and identity leaders..

Certification Makes it Happen

In 2010, one year after the Initiative's founding, Kantara's Identity Trust Framework was formally recognized by the US government, greatly empowering it as an arbiter of identity compliance. Four years later, Kantara issued its first Trust Mark in identity assurance: a certification indicating when identity products conform to the strictest security and privacy standards. In the intervening years, the organization has certified the likes of Prism Luminaries like ID.me, 1Kosmos, Onfido, and IDEMIA, demonstrating the important role of Infrastructure in the Government Services Prism Ecosystem. With citizen identity data on the line, third party certification is essential in ensuring government agencies and relying parties are choosing the right technologies to protect users, enhance privacy, and include everyone. Organizations like the Kantara Initiative provide the essential guidance required to secure identity while enabling the benefits of digital civics.

Organization Members:

1KOSMOS · Airside (an Entrust Company) · beruku knowledge · GakuNin · CLEAR · IDPrivateid · INTERNET2 · facetec · THALES (Building a future we can all trust) · IDmachines · Proof · SLANDALA · Patient Centric Solutions · Socure · ID.me · UNITED STATES POSTAL SERVICE · YuTru · CALVERT CONSULTING · experian · IDEMIA · IDENTOS · HINDLE CONSULTING · GSA · Zygma

Contact Kantara Initiative: hello@kantarainitiative.org

The Prismatic Future of Government Services

Government services has an important role to play in the future of biometric digital identity. In providing the foundational identity required to support the entire Idnetity Hierarchy, government services stakeholders stand to significantly benefit from the biometric digital identity solutions explored in this report while also providing a solid anchor of trust for other markets.

The future of biometric digital identity in government services demands:

- AI-powered anti-fraud solutions that can compete in the ongoing cybersecurity arms race.
- Easy and accessible onboarding that can bind human biometric identity to a system of record, rejecting synthetic identities and complying with shifting regulations.
- Strong authentication 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 compromise security.

Government agencies and organizations have a multitude of biometric digital identity options to choose from. Those highlighted in this report are ready to deploy and have an eye toward the orchestration and proficiency required to make the Prism Identity Hierarchy a reality. By choosing biometrics with AI-enhanced liveness detection and full lifecycle orchestration, government services stakeholders are laying the groundworlk for an idenitty safe future everyone can enjoy.

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 initial proof-of-concept Prism graphic was developed and debuted in the winter of 2023. It instantly became the most shared asset in our history, receiving over 50,000 impressions within weeks. By September 2023, we developed that proof-of-concept into a robust Prism Report, which served as the foundation for The Prism Project. The intent of the Project is to use the Prism 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

The Prism Project will publish, promote, and distribute four reports in 2024:

- The 2024 Flagship Biometric Digital Identity Prism Report – the foundational report defining the Prism Framework initially published in September 2023.
- The Financial Serices Biometric Digital Identity Prism Report.
- The Government Services Biometric Digital Identity Prism Report.
- The Travel and Hospitality Biometric Digital Identity Prism Report.

Visit www.the-prism-project.com/prism-reports to download Previews of the reports.

Prism Project Brain Trust

The Prism Project is the brainchild of Maxine Most, Principal, Acuity Market Intelligence and Peter Counter, Author, Technology Writer, and former Editor and Chief, FindBiometrics. This innovative new 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.

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 lay, what obstacles must be overcome to successfully deploy these technology solutions, 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. Tenacious strategic marketer with a prolific career hallmarked by success designing and executing ground-breaking strategies for technology innovators and leaders.

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

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

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

Ms. Most regularly offers insight and analysis in on and off-line publications, is quoted often in industry, business, and consumer

press, and presents regularly at industry events on the evolution and development of biometrics and digital identity markets. She is a graduate of the University of California, San Diego with a multi-disciplinary degree in Mathematics and Computer Science and minors in Visual Arts and Economics.

Let The Prism Project be your guiding light!

The Prism Project (www.the-prism-project.com)
The Prism Project is the brainchild of Maxine Most, Principal, Acuity Market Intelligence and Peter Counter, Author, Technology Writer, and former Editor and Chief, FindBiometrics. This innovative new 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 decades of practical expertise in the unpredictable and volatile world of emerging technology, Acuity Market Intelligence consistently delivers original, thought-provoking, and reliable insight and analysis. Founded and staffed by proud, self-proclaimed technology business development and marketing geeks, Acuity is globally renowned for its unique ability to understand, assess, and accurately anticipate technology market evolution.

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