Hype Cycle for Digital Identity, 2023

Published 26 July 2023 - ID G00792128 - 74 min read

By Analyst(s): Ant Allan, Nathan Harris

Initiatives: Identity and Access Management and Fraud Detection; Build and Optimize Cybersecurity Programs

Modern society is increasingly digitized. As digital identity becomes fundamental in everyone's lives, organizations' identity and access management challenges multiply. The innovations in this Hype Cycle can help security and risk management leaders solve these challenges.

Analysis

What You Need to Know

Electronic identification, authentication and authorization have existed for over 60 years. However, most organizations address the challenges of account takeover (ATO) fraud, identity theft, data breaches and governance with siloed solutions — often eroding user experience (UX).

Over the past 20 years, there has been an increase in the use of identities (such as federation and portable identities) across organizational boundaries. Technologies like identity wallets will continue to grow, enabling people and systems to share information selectively or prove eligibility while maintaining privacy.

Digital identity extends personal identity beyond physical presence and is becoming widely distributed across multiple organizations and systems. Also, organizations are challenged to manage identities for machines — for example, workloads and devices.

There is an emerging ecosystem of people, machines and organizations that uses, shares and protects elements of their identities via trusted infrastructures to get access to assets or validate claims. Substantial, continued innovation underpins and enables new business models.

Most recently, vendors are boosting capabilities that coordinate digital identity protection among disparate controls using methods like shared signals.

Advice in this research applies to both private- and public-sector organizations. For the second, terms such as "revenue" or "margins" can be mapped to relevant mission outcomes, while the term "business" can refer to agency program areas and the term "customer" can be interpreted as "constituent."

The Hype Cycle

This Hype Cycle focuses on innovations that enable secure and trusted digital interactions among people, machines and assets. These interactions are, in turn, based on digital representations of people and machines' physical (real-world) and virtual (electronic) identities.

Post-trigger innovations outside the digital identity space, such as the metaverse, Web2.5 and generative AI (GenAI), will likely drive specific digital identity innovations in the coming years. Most innovations specific to digital identity now lie beyond the peak of the Hype Cycle.

Continuous Access Evaluation Profile (CAEP), which provides mechanisms to share security events between security and identity tools, has moved forward only a little. Other protocols that underpin a modern digital identity fabric will continue to mature and now lie beyond the trough, namely System for Cross-Domain Identity Management (SCIM), OAuth 2.0 and OpenID Connect (OIDC).

Journey-time orchestration (JTO) has quickly moved past the peak. This is a result of its success in reducing the complexity of managing multiple identity verification, ATO prevention and authentication vendors in the user journey and its increasing availability with customer identity and access management (IAM) tools.

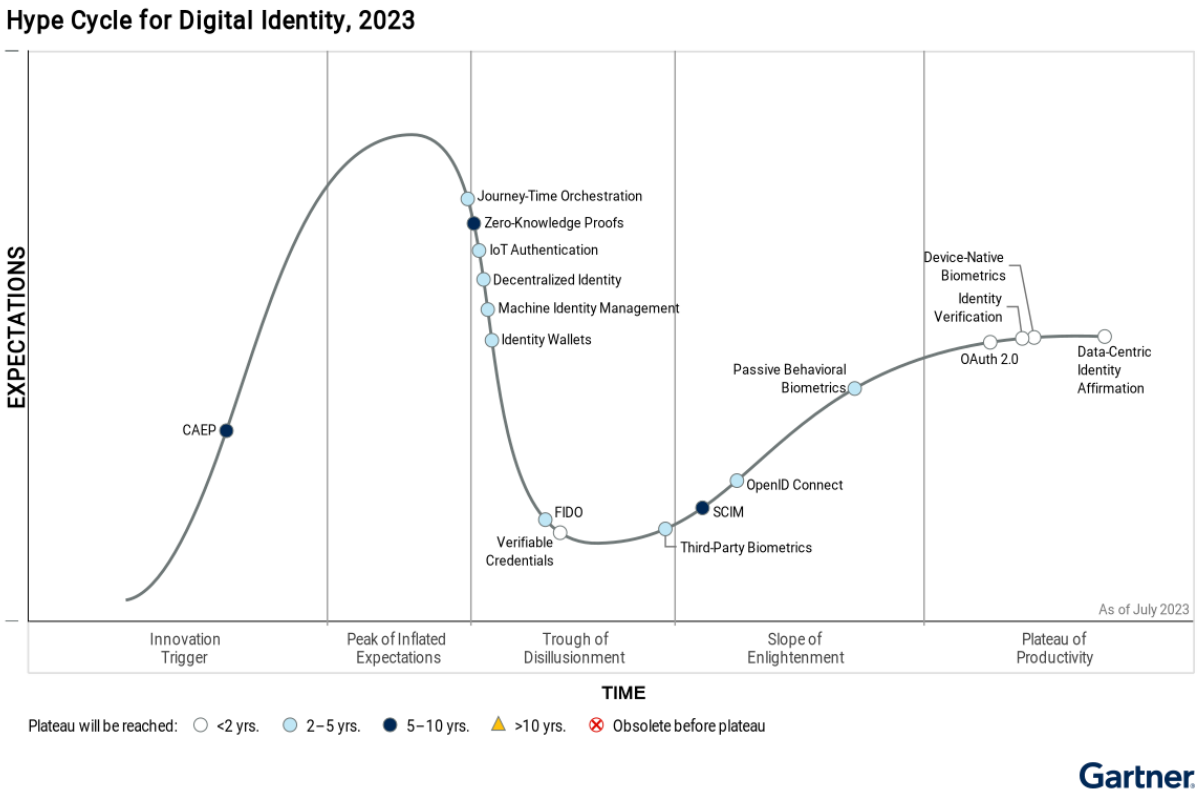
A variety of innovations that enable people and organizations to validate and share identities and attributes while preserving privacy are now past the peak, namely zero-knowledge proofs, decentralized identity (DCI) and identity wallets.

Verifiable credentials are further advanced and moving quickly, with many IAM vendors already offering verifiable credentials or adding this capability to their portfolios.

Innovations that manage and assert the digital identities of machines have made significant movements past the peak. This includes Internet of Things (IoT) authentication and machine identity management (MIM).

Authentication methods will continue to mature, with Fast IDentity Online (FIDO) authentication protocols having the most forward momentum, driven by the interest in passkeys — that is, multidevice credentials. Innovations providing confidence in real-world identity claims are reaching plateau. This includes identity verification and data-centric identity affirmation (DCIA).

Figure 1: Hype Cycle for Digital Identity, 2023



The Priority Matrix

Transformational innovations in this Hype Cycle revolve around DCIs and verifiable claims (VCs). These technologies establish, broker and manage trust in digital identities while allowing users to own their digital identities. Although these technologies are no longer nascent, there isn't much experience of how they would work at scale — and there are competing specifications. Also, trust needs a guarantor. This requires business models that allow third parties to vouch for information about other identities.

Managing the digital identities of machines, such as devices and workloads, is a concern for virtually any organization.

Finding the balance between appropriate levels of trust and UX remains critical for every organization's employees and customers. Different biometrics, such as biometric-enabled FIDO methods, offer better authentication UX than passwords and tokens.

CAEP enables sharing of risk signals, contributing to adaptive access approaches and continuous session management in decentralized environments.

Table 1: Priority Matrix for Digital Identity, 2023

(Enlarged table in Appendix)

Benefit	Years to Mainstream Adoption			
↓	Less Than 2 Years ↓	2 - 5 Years ↓	5 - 10 Years ↓	More Than 10 Years ↓
Transformational	Verifiable Credentials	Decentralized Identity		
High	Identity Verification OAuth 2.0	FIDO Identity Wallets IoT Authentication Journey-Time Orchestration Machine Identity Management OpenID Connect Third-Party Biometrics		
Moderate	Data-Centric Identity Affirmation Device-Native Biometrics	Passive Behavioral Biometrics	CAEP SCIM Zero-Knowledge Proofs	
Low				

Source: Gartner (July 2023)

Off the Hype Cycle

Due to maturity and market penetration, social identities are off the plateau. Social login and sign-up is a well-established and mainstream technology that provides people with digital identities managed by social media and digital consumer platforms, such as Facebook, Google, WeChat and Twitter.

Secure multiparty computation was removed from the Hype Cycle because it now has no significant relevance to digital identity and will likely be obsolete before the plateau.

Document-centric identity proofing (DCIP) has been renamed as identity verification to reflect the term most often used by vendors and buyers. The verifiable claims profile has been renamed as verifiable credentials to reflect World Wide Web Consortium (W3C) standards and the broader industry convergence on “credentials.”

On the Rise

CAEP

Analysis By: Erik Wahlstrom

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Continuous Access Evaluation Profile (CAEP) is a standard that enables IAM, security tools and the services they protect to continually share security events to enable session management, mitigate breaches and to reenforce policies in a decentralized environment. CAEP profiles the Shared Signals and Events (SSE) Framework that defines mechanisms to communicate events between trusted parties to enable continuous runtime access decisions.

Why This Is Important

- Applications and services are consumed and deployed in a hybrid and decentralized IT environment. A decentralized environment requires new session management mechanisms.
- The sharing of events between systems requires a standardized event-based protocol.
- CAEP helps resolve challenges with long-token lifetimes, step-up authentication, the continuous assessment of assurance levels and device postures, and provides mechanisms to communicate and respond to identity life cycle events.

Business Impact

CAEP increases security in services that are connected with identity federation, by enabling continuous exchange of security events. This enables higher assurance levels of sessions and a better user experience. CAEP provides a near-real-time mechanism to validate claims, request step-up authentication and to manage sessions. It thus enables centralized security in a hybrid and decentralized IT environment.

Drivers

- The increasing decentralization of applications and services in organizations' hybrid and multicloud environments has made continuous session management hard. For example, the implementation of single logout has historically been impossible to implement at scale.
- Organizations need a way to understand what's going on in applications after users are authenticated. Organizations have therefore been looking at technologies beyond federated identity flows that just protect the "front door" to also understand what goes on "behind the doors" of protected applications. Cloud access security brokers (CASBs) have historically been the only alternative to add this control, due to the lack of an industry standard that allows for the event-based sharing of access signals.
- OAuth 2.0 provides refresh and access tokens to keep sessions up to date, but it's not responsive enough. Keeping assurance levels high throughout a session have required users to be reevaluated at a central identity provider, thereby interrupting user journeys.
- A tightly woven identity fabric, where an organization weaves multiple IAM tools together to solve its identity use cases, requires event-based and runtime communication mechanisms to be established to evaluate and establish trust, and orchestrates the right tools for the use cases. For example, an event saying a claim about a user is no longer valid, or an out-of-compliance security posture of a device must trigger other IAM tools to respond to that event and reevaluate their access decisions in runtime.
- CAEP is a profile of the SSE Framework defined by the acclaimed OpenID Foundation.
- Using CAEP to continuously feed signals into an adaptive access engine enables the engine to have more data and make more accurate access decisions.
- The community is starting to offer CAEP testbeds such as caep.dev to provide education, and also to test CAEP implementations and thereby driving adoption.

Obstacles

- All identity standards take a long time to be commonly implemented. Identity standards have a “chicken and egg” problem before they reach wide deployment. Target applications wait to see if a standard takes off and IAM vendors wait for wide support in their target applications. This is also true for CAEP. The number of deployments is now growing from small numbers. Deployments are within a vendor’s own tools or between close partners. For example, Microsoft has implemented CAEP in Azure Active Directory and uses it for Exchange, Teams and SharePoint Online.
- CAEP is still not commonly known and understood by IAM professionals, or by application and service developers. Also, product documentation and education material from IAM vendors about CAEP is still limited.

User Recommendations

- Define an IAM architecture that supports centralized/decentralized systems. CAEP is a protocol next to other modern identity protocols such as JSON Web Tokens (JWTs) and Open Policy Agent (OPA) that enable it.
- Ask IAM vendors about their roadmaps. Gartner expects CAEP and other related standards — like the Risk Incident Sharing and Coordination (RISC) profile of the OpenID SSE Framework Specification to share security and risk events across decentralized systems — to become increasingly important going forward.
- Add CAEP as an optional RFP criterion when procuring new applications, specifically SaaS apps. Support is still emerging, but Gartner expects the adoption of CAEP to grow. Configuring a new application in an IAM tool should, over time, include standardized life cycle management, single sign-on and the sharing of events.

Sample Vendors

Amazon Web Services; Broadcom; Cisco; Google; Microsoft; SGNL

Gartner Recommended Reading

Modern Identity: OpenID Connect, OAuth 2.0, JWTs and SCIM 2.0

Identity-First Security Maximizes Cybersecurity Effectiveness

At the Peak

Journey-Time Orchestration

Analysis By: Akif Khan

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Journey-time orchestration solutions improve risk management along digital user journeys to deliver improved user experience (UX). Most organizations manage many identity verification, authentication and fraud detection tools, and adjacent capabilities such as access management. An orchestration solution manages vendor integrations, simplifies assessment of risk at each event in the journey and facilitates delivering dynamic UX.

Why This Is Important

Protecting the integrity of digital user journeys and offering a compelling UX is the foundation that digital transformation is built upon. Organizations without available developers struggle to manage the broad range of capabilities that this requires, including identity verification, user authentication, fraud detection, identity provider (IdP) resilience and A/B testing. Further complexity arises when integrating with adjacent capabilities, such as access management and risk analytics, and UI components.

Business Impact

Use of a journey-time orchestration solution can:

- Remove the operational complexity of managing multiple vendor integrations leading to cost savings.
- Empower business users to do more in a low-code/no-code manner by removing the need to customize business logic in code.
- Improve the efficacy of risk management along the digital user journey, and help organizations manage the delicate balance between security and UX. Increasing security while improving UX is a dream for most businesses.

Drivers

- Managing multiple vendor integrations is a drain on an organization's resources at a time of skills shortages. Abstracting away that development effort to the orchestration tool reduces cost and complexity.
- Chief information security officers (CISOs) and app developers are both looking to enable more dynamic, risk-based UX, which is easier to achieve with an orchestration solution due to the fine-grained user journey control intrinsic to such solutions. The orchestration solution optimally acts as the connective thread between the analytics solutions and the UI layer to reduce fraud risk while enabling a great UX.
- The need to facilitate A/B testing in DevOps is pushing the adoption of orchestration. Optimization of a risk management strategy is facilitated by a strong orchestration platform in the form of A/B testing. For example, traffic could be split across two different identity verification vendors to assess which delivers better conversion rates. Also, the use of different signals, such as passive behavioral biometrics or location intelligence, could be tested against one another at specific events in the user journey to find the optimal balance of detecting fraud versus the cost of detection.
- Organizations seek to improve resilience in their vendor connections. In high-throughput B2C use cases, vendor uptime is critical. For certain categories of capability, an orchestration platform can improve such resilience. For example, if a given vendor is down or showing too high a degree of latency, the orchestration vendor can be configured to use a designated alternative vendor, if appropriate.
- Enabling tight integrations with access management and other identity and access management (IAM) tools introduces additional efficiencies to cybersecurity organizations. The creation or acquisition of orchestration capabilities by many consumer identity and access management (CIAM) vendors is lowering the barrier to adoption, and tightly integrating orchestration with the access management layer.

Obstacles

- Reliance on the orchestration vendor to maintain updated and certified integrations with a large number of downstream IAM and fraud detection vendors. This can be mitigated by a model in which some orchestration solutions allow a client to add their own integrations.

- Dependency on the orchestration vendor's roadmap with respect to enabling new features from downstream vendors, and relying on the orchestration vendor to make all top-level data — for example, decision or risk score — along with metadata — for example, the basis for the signal — from vendors available for use in rules and policies.
- Lack of transparency or negotiability for pricing if relying on the orchestration vendor to manage the commercial relationship with a range of IAM and fraud detection vendors.
- Resilience risks are introduced by having a single point of failure in the orchestration vendor to manage all IAM and fraud detection tools in play along the digital user journey. Organizations will need to plan for how they would handle downtime from their orchestration vendor.

User Recommendations

- Abstract away the complexity of managing multiple vendor integrations by leveraging a journey-time orchestration solution to deliver a marketplace of ready-made connections to identity verification, authentication and fraud detection solutions.
- Deliver tailored and dynamic risk-based UX and customer experience (CX) by using a journey-time orchestration solution to connect the analytics layer and UI layer to broker calls between systems along the user journey.
- Assess orchestration vendors' resilience and business continuity plans carefully, given the risk that presents itself when using a single vendor to manage connectivity to multiple downstream vendors.
- Use orchestration for SaaS resilience of IdPs, but also plan for contingency if the orchestrator itself is offline. For example, enable mission-critical apps to authenticate manually against two IdPs in case of failure (see Quick Answer: How Can We Reduce the Risks of SaaS-Based Identity and Access Management?).

Sample Vendors

ForgeRock; LexisNexis Risk Solutions; Ping Identity; Spec; Strata; Strivacity; Transmit Security

Gartner Recommended Reading

Innovation Insight: Journey-Time Orchestration Mitigates Fraud Risk and Delivers Better UX

Market Guide for Identity Proofing and Affirmation

Market Guide for Online Fraud Detection

5 Essential Ingredients of a Successful Access Management Strategy

Sliding into the Trough

Zero-Knowledge Proofs

Analysis By: Mark Horvath, Bart Willemsen

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Zero-knowledge proofs (ZKPs) are privacy-preserving messaging protocols that enable entities to prove that information available to either or both of them is correct, without the requirement to transmit or share the underlying (identifiable or otherwise sensitive) data. ZKPs enable entities to prove information validity without the requirement to transmit personal or confidential data.

Why This Is Important

Following increasingly imminent digital threats and legislative data protection requirements, security and risk management (SRM) leaders must support use cases that enable digital business while ensuring in-use protection. These protocols limit the requirement for mass decryption/encryption of data elements, which benefits the efficiency of work — including potential adoption of blockchain-based systems.

Business Impact

ZKPs are being applied for many use cases, especially in the context of authentication and transaction verification. Other use cases include payments, decentralized identity, custody management, anti-money-laundering (AML), know your customer (KYC), consumer identity and access management (IAM), age verification, etc. With the addition of ZKPs to blockchain platforms, SRM leaders can cover information security use cases that require confidentiality, integrity and availability (CIA). Some blockchain platforms have evolved to include this.

Drivers

- Traditional data protection techniques typically focus on data in motion (i.e., transport layer security) and data-at-rest encryption. Data-at-rest encryption, as commonly implemented, does not provide strong protection from data theft and privacy disclosures. It is unable to secure data in use and data sharing scenarios.

- New use cases and maturing privacy legislation worldwide present new privacy and cybersecurity concerns that require data-in-use protection. There are also scenarios where the data itself does not need to be shared. ZKPs enable such data-in-use protection.
- Concerns about data security in several scenarios, including collecting and retaining sensitive personal information, processing personal information in external environments such as the cloud and information sharing.
- Privacy violations (due to the exposure of sensitive information).
- Need for mitigation of sensitive data leakage and cyberattacks.

Obstacles

- Even with a variety of web applications (e.g., ZKProof), ZKPs remain in an emerging state. They still require a common framework for applications to leverage.
- Only a limited number of practical implementations have emerged to date.
- The variety of methodologies and the multiplicity of approaches to data management inhibit adoption. ZKPs will need to scale at the rate of blockchain transactional volumes to be effective.
- ZKPs require integration into applications. Downstream applications, such as CRMs and databases, will need some modification.
- Some ZKPs, like ZK-SNARK, have a dependency on existing encryption/hashes (ECDSA in this case) as part of their implementation. This adds a potential complexity in upgrading them to quantum-safe protocols and limits available staff/experts.

User Recommendations

- Work with SRM leaders to gain a deeper understanding of the nature of these controls, understanding that ZKP techniques are a paradigm shift.
- Be realistic with the current immaturity of ZKP solutions and approaches when evaluating ZKP benefits for privacy protection.
- Evaluate how ZKP controls may impact transaction authentication and, ultimately, consumers.
- Assess the impact on the broader information management strategy.

- Assess the architectural implications for using ZKP with different blockchains and distributed ledgers.

Sample Vendors

DropSecure; Evernym; IBM; Ligero; Microsoft; Ping Identity; QEDIT; Sedicii; StarkWare

Gartner Recommended Reading

Three Critical Use Cases for Privacy-Enhancing Computation Techniques

Emerging Tech: Assess Zero-Knowledge Proof Technologies to Strengthen Competitive Advantage in Decentralized Ecosystems

Predicts 2022: Privacy Risk Expands

Top Strategic Technology Trends for 2022: Privacy-Enhancing Computation

IoT Authentication

Analysis By: Michael Kelley

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Internet of Things (IoT) authentication is the mechanism of establishing trust in the identity of a thing (typically a device) interacting with other entities, such as devices, applications, cloud services or gateways operating in an IoT environment. Authentication in IoT takes into account potential resource constraints of IoT devices, the bandwidth limitations of networks they operate within and the mechanized nature of interaction among various IoT entities.

Why This Is Important

From automotive, to smart houses and smart buildings, to the smart appliance market, to industrial IoT (IIoT), operational technology (OT), IoT is exploding as a market. However, these connected devices can bridge cyber and physical worlds, and open up entirely new threat vectors. Sound IoT security requires strong identity in IoT devices coupled with strong IoT authentication, with the goal of mitigating and minimizing cyberattacks, and/or other issues and vulnerabilities.

Business Impact

IoT authentication can mitigate:

- Privacy issues that directly impact liability and brand reputation for consumer devices.
- Attacks against connected devices that could lead to disruption in product or service offerings.
- Attacks against industrial devices that lead to operational impacts and, potentially, catastrophic events in safety-critical production areas.

Drivers

- IoT solutions blend the physical and digital worlds by creating cyber-physical systems (CPS), transforming the way we live and work. The explosive growth of IoT is creating connectivity between humans and machines in an unprecedented way.
- IoT endpoint electronics revenue is forecast to grow by 11% in 2023. Organizations are investing in IoT technologies to drive cost optimization and operational efficiency. These investments will drive attention and spend on IoT authentication methods (see Forecast: Internet of Things, Endpoints and Communications, Worldwide, 2022-2032, 1Q23 Update).
- Secure credential storage and rotation approaches for IoT authentication are sorely needed. Ongoing work for defining this, as well as for identifying devices, is happening in the public sector.
- Many use cases stemming from IoT could change traditional business models, such as substituting in-person healthcare with virtual and remote monitoring. However, the authentication requirements for the use cases are highly industry-specific and require industry-level understanding of the market needs.
- Certificates continue to be the primary way devices are identified and authenticated, public key infrastructure (PKI) vendor investments and focus in this space include DigiCert, Entrust, Keyfactor and Sectigo, leveraging their PKI capabilities to solve IoT authentication use cases.
- Standards helping to provide consistent approaches, and solidifying investments, viability and utility, include RFC 8628; the CSA's Connectivity Standards Alliance (Matter); OAuth 2.0 Device Authorization Grant extension; and the ACE working group within the Internet Engineering Task Force (IETF), which is also specifying how OAuth 2.0-based authentication and authorization exchanges can be optimized for constrained devices for use over Constrained Application Protocol (CoAP), Message Queuing Telemetry Transport (MQTT) and other messaging protocols.

Obstacles

- The IoT security landscape is complex, including determining the right people, process and technology to employ due to a fragmented market, and difficulties productizing due to inconsistent device types and operating environments.
- Some authentication methods are not good candidates due to certain IoT devices that are resource or feature constrained with low computing power and limited secure storage capacity.
- Support of authentication methods via IoT platforms is immature or incomplete. Use-case areas, such as IIoT, have protocols that are not interoperable with each other and, many times, not operable with standards like TCP/IP, creating ongoing challenges for authentication approaches. In addition, most IIoT systems are self-contained and use native proprietary means for authentication.

User Recommendations

- Catalog and establish capabilities for each category of device in its IoT network. Leverage device- and network-based contextual information to gain additional assurance.
- Evaluate and adopt authentication frameworks that support the range of device types across the IoT realms in operation.
- Make use of trusted computing techniques, such as hardware root of trust, that help to protect against physical attacks on devices and sensors, as well as against the external software attacks that could enable unauthorized reading, analyzing and manipulating of software code.
- Explore use cases where the high cost of people or processes in existing approaches would justify investment in IoT solutions.
- Use fusion teams to manage the disparate technical and regulatory requirements of IoT projects and implementations (see Fusion Teams: A Proven Model for Digital Delivery).

Sample Vendors

Atos; DigiCert; Entrust; IN Groupe (Nexus); Keyfactor; Microsoft; Sectigo; V-Key; Venafi; Xage Security

Gartner Recommended Reading

Innovation Insight for Cyber-Physical Systems Protection Platforms

Managing Machine Identities, Secrets, Keys and Certificates

Cross-Industry Insight: IoT Market Opportunities and Top Spend Use Cases

Decentralized Identity

Analysis By: Michael Kelley, Akif Khan, Arthur Mickoleit

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Decentralized identity (DCI) allows an entity to control their own digital identity by using decentralized identifiers (DIDs) to connect and authenticate themselves to other entities. Private keys and verifiable credentials (VCs) are contained in digital wallets, supported by an identity trust fabric for making DIDs discoverable. By establishing trust, privacy and security, DCI is an attractive alternative to traditional models of storing, sharing and verifying identity data.

Why This Is Important

Identity fragmentation is a problem due to service providers (banks, retailers and governments) forcing consumers to create individual identities for every service. DCI offers an attractive approach with increased security, privacy and usability compared to traditional digital identity approaches like federated identity. While legislative efforts to secure privacy and ensure interoperability are multiplying around the world, standards continue to be refined, and DCI use cases continue to emerge.

Business Impact

Users gain greater control of their identities and data, and service providers gain higher trust, speed and confidence. Currently, providers collect huge amounts of identity information about users to increase assurance to an acceptable level. DCI can provide trust, security, privacy and convenience, and can provide portability of identity data for end users without needing centralized data, reducing risks of data breaches, account takeovers and privacy compliance violations.

Drivers

- Vendor investments in DCI: Due to the volume and influence of vendors investing in this space, there is high potential to drive the DCI market forward, and significant investments have been made by IBM, Microsoft and Ping Identity. In addition, Gartner has been tracking more than 80 startups and vendors of DCI technologies and DCI components (e.g., digital wallets and trust fabrics).
- Government activity: Public sectors are increasingly shaping digital identity trends around DCI. The EU, national governments like Finland or Canada, as well as states and provinces like Utah and Ontario are actively pursuing and investing in DCI use cases that span public and private sector interests.
- Privacy regulations: Countries continue to formalize the requirement for user privacy, specifically for collecting and securing large amounts of user data through regulations. DCI provides a more user-centric way of complying with privacy regulations through decentralized user data.
- Client and overall market interest in DCI: Interest is increasing due to attractive elements such as the ability to enable new digital business opportunities while maintaining client privacy. For example, using DCI to share verified claims, such as age/income, employment status, professional credentials, educational credentials without exposing sensitive personal data.
- Standards: Standards are maturing, led by entities such as the World Wide Web Consortium (W3C), the Decentralized Identity Foundation (DIF), the OpenWallet Foundation and OpenID for verifiable credentials to create a consistent approach to DCI. Expanding and maturing standards will help move the market forward.
- User experience: Asking users to repeatedly go through identity proofing and affirmation processes for every online interaction with a service provider is a broken model. Significant friction can be removed from UX if users could assert their identity using a digital wallet with full control over their identity data.

Obstacles

- Authority of issuers: Ensuring that an organization is authoritative to issue a VC (e.g., only an accredited facility issuing educational credentials).
- Adoption: Service providers may resist accepting identity claims via DCI unless they see user adoption, and users may be reluctant to adopt DCI wallets unless they see meaningful use cases for them.
- Interoperability: Adoption is slow due to most development taking place in pockets and a continued lack of standards.
- Technical challenges: Concerns about performance, interoperability, scalability and maturity, as well as wallet standards.
- Regulations: More work is required for how verifiable claims can be used in regulated use cases such as KYC, as required in financial services, online gambling and other industries. Governments are exploring regulatory needs for citizen interactions.
- User interface challenges, ID proofing and account recovery processes are vulnerable for security and privacy, and will require standard approaches.

User Recommendations

- Explore use cases for verifiable claims by identifying tasks and processes that are expensive, complex and time-consuming in the real world, which will benefit from a verifiable claims approach.
- Build a business case for trialing acceptance of DCI by targeting reduced identity proofing and affirmation costs and an improved UX.
- Identify attainable use cases through following successful POCs, such as a DCI solution focused on remote employee onboarding, educational credentials, health credentials and passwordless authentication.
- Partner with existing vendors to understand the possibilities and potential of DCI. Track government activities around use cases for citizen IDs.
- Be cautious of overly optimistic vendor claims. Evaluate the technical security aspects of centralized and partially decentralized identity trust fabrics or using blockchain platforms under consideration. In particular, examine vendor plans for support of standards, such as W3C, DIF and the OpenWallet Foundation.

Sample Vendors

1Kosmos; Evernym; IBM; IdRamp; Microsoft; Nuggets; Ping Identity; Scytale; SecureKey; Wise Security Global

Gartner Recommended Reading

Guidance for Decentralized Identity and Verifiable Claims

Innovation Insight for Decentralized Identity and Verifiable Claims

Predicts 2023: Users Take Back Control of Their Identities With Web3 Blockchain

Top Trends in Government for 2022: Digital Identity Ecosystems

Machine Identity Management

Analysis By: Erik Wahlstrom, Felix Gaehtgens

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Machine identity management establishes identity, trust, observability and ownership of workloads and devices such as services, applications, scripts, containers, VMs, robotic process automation, IoT and mobile devices. It includes the management of the life cycle of machine identities, as well as policies and credentials such as secrets, keys and certificates that are used for trusted identification and authorization.

Why This Is Important

- Organizations have more machines than humans and this expands the threat landscape.
- Organizations struggle to protect machine credentials such as secrets and certificates properly, leading to their leakage and abuse.
- Machine identity management needs a strong focus on observability, ownership and automation to be able to scale.
- Machines are used by many different business units within an organization, so a common set of standards and a well-aligned strategy to manage them is needed.

Business Impact

Organizations have and use many machine identities. However, these identities are rarely managed properly, exposing them to risk. Proper machine identity management allows organizations to secure communications between workloads and/or devices, enabling current and new digital use cases. Machine identity management is critical to secure DevOps workflows by automating security through management of credentials used within the tool chain, and for machine-to-machine communication.

Drivers

- Attacks against machine identities are on the rise, because hackers see them as “soft targets” that many organizations don’t govern and properly lockdown.
- Interest in secrets management solutions continues to drive Gartner client inquiries.
- New vendors have entered the space, resolving problems with the decentralization of workloads. Rather than storing and issuing all machine identities in a central place, new approaches discover, govern and control them in multiple places.
- Initial trust establishment — secret zero — remains a hard-to-solve issue and continues to cause frustration and security concerns. Many Gartner clients continue to store unprotected API keys used by workloads to authenticate to secrets managers.
- Stand-alone secrets management vendors are experiencing rapid growth through adoption of this technology. However, Gartner clients tell us that high pricing/licensing and reach into platforms are big obstacles to using one vendor for managing all secrets.

- There is an ongoing, but slow, convergence in the market. For example, IaaS/PaaS providers offer native capabilities, privileged access management (PAM) vendors add support for more workloads, and PKI and certificate management vendors extend into SSH and symmetric key management.
- Cloud infrastructure entitlement management (CIEM) tools (offered as stand-alone tools or part of an IaaS, identity governance and administration [IGA] or PAM suite) increase their focus — from low levels — on discovery and reporting of machine identities across systems.
- Integrations and hybrid or multicloud single-pane-of-glass functionality are becoming more important for organizations. The aim is to help increase organization efficiency and decrease response times.

Obstacles

- Different machines, their identities and the credentials used are managed disparately, which requires a combination of different tools. Examples are tools that manage service accounts, secrets management and PKI. It is currently not feasible to manage all machine identities with only one technology.
- There are different definitions of machine identities, exacerbated by vendors providing their own interpretation and messaging. This makes selecting the right tooling difficult.
- Different business units have different needs and tool preferences. The establishment of a cross-team strategy is, therefore, critical to balance expectations around centralized governance and operations.

User Recommendations

- Define your scope when managing different machine identities and how their management differs from IAM for humans.
- Establish ownership for machine identities using a fusion team. Also use the team to govern multiple tools and set expectations.
- Use a best-of-breed approach via multiple tools that can provide continuous observability (discovery, monitoring and behavior analysis) of machines.
- Provide tailored guidance to developers, I&O, DevOps and security teams by defining how the tools in the technology stacks should and shouldn't be used, and under what circumstances new tools or instances can be acquired and deployed. The lack of a single pane of glass increases the importance of best practices.
- Use emerging products and capabilities that address fragmentation of secrets by providing a governance and administration layer across environments via support of a bring your own vault (BYOV) approach coupled with deeper discovery.

Sample Vendors

Aembit; Akeyless; Amazon Web Services; AppViewX; CyberArk Software; Entro Security; HashiCorp; Keyfactor; Microsoft; Venafi

Gartner Recommended Reading

Managing Machine Identities, Secrets, Keys and Certificates

Innovation Insight: Secrets Management Tools

IAM Leaders' Guide to Privileged Access Management

Identity Wallets

Analysis By: Michael Kelley, Akif Khan, Arthur Mickoleit

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Identity wallets, both in the form of mobile and web apps, enable users to store, manage and selectively disclose digital identity data from different sources and for various purposes. Users can also use identity wallets to hold their credentials to validate claims. Overall, identity wallets represent an interface for issuing and verifying credentials.

Why This Is Important

A digital identity wallet provides individuals greater control over their identity data and has the potential to enable higher trust for validation of identity claims. For service providers, identity wallets can enable new service models that require consented sharing of identity data. Use cases can involve commercial and government entities for verifiers and issuers of credentials and attributes. Governments are exploring the need for standards and regulations around identity wallets.

Business Impact

Identity wallets help individuals manage personal data from any public or private source. For example, ID cards, driving license data, employer data, COVID-19 vaccination, digital passports and tickets. Use cases span from in-person identity verification and online transactions to contactless check-ins. The data managed by identity wallets include verifiable claims for decentralized identity (DCI), digital representation of electronic data, like airline or concert tickets, and even cryptocurrency and non-fungible tokens (NFTs).

Drivers

- **Privacy and security:** Digital wallets prioritize benefits like security, privacy and anonymity through zero-knowledge protocols and data minimization.
- **Health information:** Digital wallets can safely and securely communicate health information from patients to medical providers.
- **Citizen credentials:** Mobile driver's licenses and other documents providing proof of citizenship. These specific use cases contribute to the growing public interest and debate about digital wallet services on the smartphone.
- **Growing traction of decentralized identity:** Interest in identity wallets is growing with increased interest in DCI. Global standards, like World Wide Web Consortium (W3C) verifiable credentials (VCs) and decentralized identifiers (DIDs), are driving additional use cases for verifiable claims in digital wallets. These enable the creation of open, interoperable identity wallet services.
- **Payments and fintech:** Identity wallets are serving payment-related use cases. For example, to manage financial assets and transactions. The confluence of identity and payment use cases in mobile apps, like Apple Wallet, are already visible today.
- **User experience (UX):** Identity wallets will reduce the need for users to repeatedly prove their identity across multiple service providers. Mobile devices will become the primary means for proving identity claims. Asserting an identity claim from already verified identity attributes will reduce onboarding friction and likely become a competitive advantage.
- **Future monetization of identity data:** Today's identity wallets are focused on nonremunerated consent for sharing personal identity data. Future iterations and use cases for identity wallets may include an individual granting consent of their personal data for commercial use in return for remuneration or other rewards.

Obstacles

- **Market understanding:** There is confusion about the term “identity wallets.” The term can refer to proprietary mobile ID apps — where identity data is confined to a centrally defined ecosystem — and to open standards-based wallets that enable decentralized, portable and interoperable identity.
- **Wallet standards:** The market and governments are actively working on standards and strategies for interoperability. The OpenWallet Foundation is currently working on defining an open standard for interoperability.
- **User acceptance:** The adoption of identity technologies will be driven by relevant use cases. Focus on use cases that effectively communicate the tangible benefits of identity wallets.
- **User experience (UX):** The interface for the identity wallet must be easy to use and intuitive. Alternatives to mobile devices must be explored.
- **Trust and recoverability:** When users begin to store and manage personal or payment data with their wallet, data security, encrypted keys and recoverability after loss or theft will be a top priority.

User Recommendations

- As soon as standards evolve, be prepared to support multiple wallets for varied use cases. For example, a wallet for concert tickets, a government-issued wallet for citizen-identity information, a personal wallet holding banking, employment and educational credentials, or a wallet for storing cryptocurrency or processing payments.
- Explore emerging use cases, like verifiable claims for decentralized identity, cryptocurrency and NFTs, while supporting traditional use cases — for example, digital representations of physical things, such as airline and events tickets, driver’s licenses, digital passports and other government-related documents.
- Observe or participate in shaping regulations, standards and reference frameworks that are relevant to your geography. For example, the EU’s ongoing large-scale pilots and electronic identification, authentication and trust services (eIDAS) regulation revision.
- Investigate the value of digital wallets for representing identity in online digital communities, like Web 3.0 and metaverse applications.

Sample Vendors

1Kosmos; Apple; Evernym; ID.me; Google; Microsoft; Nuggets; Ping Identity; Scytáles; SecureKey

Gartner Recommended Reading

Guidance for Decentralized Identity and Verifiable Claims

Innovation Insight for Decentralized Identity and Verifiable Claims

Predicts 2023: Users Take Back Control of Their Identities With Web3 Blockchain

Predicts 2022: Identity-First Security Demands Decentralized Enforcement and Centralized Control

Top Trends in Government for 2022: Digital Identity Ecosystems

FIDO

Analysis By: Ant Allan, James Hoover, Robertson Pimentel

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

The Fast IDentity Online (FIDO) authentication protocols published by the FIDO Alliance combine public-key credentials in a hardware or software authenticator with a local "gesture" (e.g., a PIN or a biometric method). The majority of new FIDO deployments use FIDO2, which includes enabling the W3C Web Authentication (WebAuthn) standard. FIDO2 supports platform authenticators on single or multiple endpoint devices and roaming authenticators such as FIDO2 security keys and passkey-enabled phones.

Why This Is Important

Digital identity hinges on authentication that can provide credence in an identity claim, sufficient to bring account takeover risks within an organization's risk tolerance, ideally without adding unnecessary friction to the user journey. FIDO, particularly FIDO2, including passkeys, promises phishing-resistant passwordless authentication, as a robust alternative to widely used multifactor authentication (MFA) methods, and with better user experience (UX).

Business Impact

Identity and access management (IAM) and other security leaders across all industry verticals and geographies can benefit from adopting FIDO, which can:

- Improve UX by eliminating passwords.
- Elevate trust by providing phishing-resistant passwordless MFA in a variety of employee and customer use cases.
- Enable consistency across different use cases.
- Simplify the implementation of third-party biometrics (for improved accountability) in some use cases.

Drivers

The adoption of FIDO protocols is mainly driven by:

- The imperative to avoid the vulnerabilities, risks and user frustration associated with passwords, which drives interest in passwordless authentication generally.
- The increase in phishing and similar attacks against phone-as-a-token authentication methods, including mobile push, as well as legacy one-time password (OTP) tokens, and the emerging imperative to use phishing-resistant MFA.
- Wide availability of physical FIDO2 security keys (i.e., "dedicated devices") from a variety of vendors, some with embedded fingerprint sensors, and increased availability of FIDO2 platform authenticators (i.e., "embedded credentials") in Apple, Google and Microsoft operating systems.
- Support for multidevice FIDO2 credentials, or passkeys, which can be synced across all of a user's devices (including hardware security keys) without them having to separately enroll every device for each service provider.

- Support for cross-device authentication, enabling a user to use a passkeys-enabled phone as a FIDO2 roaming authenticator (i.e., “companion device”) to log in to an app or website from another device that the user doesn’t own or which can’t support passkeys.
- Widespread support for FIDO2/WebAuthn in popular web browsers and mainstream access management (AM) platforms, including Microsoft Azure Active Directory Premium (AADP), enabling the use of a variety of FIDO2 platform and roaming authenticators, potentially including passkeys. Emergence of specialist vendors facilitating the use of passkeys for customer authentication adds impetus.
- Increasing advocacy of passkeys by Apple, Google and Microsoft and visible support for login with passkeys from well-known social networks and service providers such as BestBuy, Cloudflare, eBay, GitHub, PayPal (U.S.), Stripe and WordPress.
- Microsoft’s support for FIDO2 security keys, as well as Windows Hello for Business (WHfB), in Windows 10 and 11, which enables login to corporate AD networks as well as the cloud (via AADP).

Obstacles

- FIDO2 security keys may not be easily used by people with manual disabilities.
- Passkey syncing is currently limited to single-vendor ecosystems. Synced passkeys not in the user’s sole possession may not meet strong customer authentication (SCA) or employee MFA requirements.
- Employees can use FIDO2 security keys for Windows login, but these have high overheads. Cross-device authentication for Windows is limited to proprietary options, but these require desktop software or dongles. Older VPNs and legacy applications that cannot be federated or otherwise integrated with a FIDO2-enabled identity provider are unsupported.
- Among customers there is not yet enough penetration of passkeys or awareness of passkeys as an option. People’s privacy concerns that ecosystem vendors might collect and monetize information about their online behaviors may be an inhibitor. Additionally, standard FIDO implementations can use only local biometrics, whereas nonlocal architectures can support multiple customer channels and life cycle events.

User Recommendations

For employees:

- Seek near-term opportunities in discrete use cases. Consider using passkeys as a password replacement within a legacy MFA scheme. Take advantage of support for device-bound passkeys to enable their use as an MFA option for access via an AM platform. Evaluate the benefits of using FIDO2 security keys for passwordless Windows login against the supply chain and provisioning overheads; consider proprietary options for using device-bound passkeys on smartphones as an alternative.
- Be cautious about continued investment in legacy tokens, but note that these may be needed to support legacy nonweb applications. Multiprotocol tokens and authenticator apps can span transitional needs.

For customers:

- Support and advocate passkeys as a passwordless option for those that can use it; highlight passkeys as a login option and make enrollment easy. An additional factor might still be needed to meet SCA needs.
- Weigh the benefits of using FIDO2 to simplify the integration of third-party biometrics in mobile apps against the need for nonlocal architectures.

Sample Vendors

Apple; Corbado; FEITIAN Technologies; Google; Hanko; HYPR; Microsoft; Nok Nok; Okta; Yubico

Gartner Recommended Reading

Innovation Insight for Many Flavors of Authentication Token

Take 3 Steps Toward Passwordless Authentication

Market Guide for User Authentication

Verifiable Credentials

Analysis By: Homan Farahmand

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

A verifiable credential (VC) is a self-contained, trusted piece of information about an entity. The term VC refers to the attributes of the entity that establishes its existence and/or uniqueness. The VC is issued and cryptographically signed by an entity (issuer), passed to the user (holder) and presented to relying entities (verifiers). VCs are validated independently of the issuers. They can be used as proof of identity, entitlement, qualification, achievement and/or ownership.

Why This Is Important

Verifiable credentials will significantly improve data sharing, privacy, data security and data quality in decentralized identity ecosystems. This approach enables independent issuance, custody and verification of verifiable attributes, or provides proof of attributes. VCs will dramatically reduce the need for intermediaries to attest to the validity of a given set of data and/or facilitate the data exchange process.

Business Impact

VCs enable digitalization and automation of secure and compliant data exchange in multiparty business processes, at lower cost and higher velocity. These types of validation are common in most industries. They usually require verification of entities' credential(s) to admit users, triage their eligibility, perform tasks and/or generate output for handoff to other parties. Verifiable credentials can cut onerous verification by more than 90% and reduce the risk of data proliferation and exposure.

Drivers

- **Decentralized identity (DCI) trend:** The growing adoption of DCI is a key driver for implementing VCs to streamline business processes. DCI enables VCs by providing discoverable, pairwise, unique identifiers for each relationship between the identity and other entities, independent of any of the ecosystem participants. The initial deployments may rely on bring-your-own-identity (BYOI) or pseudo-DCI infrastructure (that is, DCI architecture with centralized components).
- **Overall interest and adoption urgency:** Interest in VCs is increasing due to their ability to enable new digital business opportunities while maintaining entities' privacy. VCs can improve the efficiency of business processes in data exchange use cases by streamlining eligibility, credentials, document or identity verification.
- **Government identification and trust initiatives:** The use of VCs is becoming a key part of government identification and trust architecture strategies. Europe's eIDAS regulation foresees identification and attribute-sharing across public and private sectors by means of citizen-held identity wallets. There are many governments in different regions that are similarly evaluating or piloting identity wallets and VCs.
- **Continuous investment:** The ubiquity and influence of vendors investing in this space (e.g., Microsoft, IBM and Ping Identity) drive the market forward. Significant investments have been made by organizations in many industries, including government. A growing number of vendors have embraced VCs, such as access management and customer identity and access management (CIAM) vendors, as well as blockchain technology providers.
- **Standards enabling consistency:** Standards are currently emerging and maturing, led by the W3C recommended standards for decentralized identifiers and verifiable credentials, as well as Decentralized Identity Foundation specifications to create and drive a consistent approach to VCs and related technologies.

Obstacles

- **Establishing viable ecosystems:** Interoperable ecosystems with authoritative issuer and verifier participation are essential to enable adoption of VCs. However, it takes time to educate organizations and users to form these ecosystems, build relevant use cases and increase the user base.
- **Changing business processes and refactoring applications:** Organizations have to adapt their business processes to exchange data using VCs. They also have to refactor their IAM tools and applications to issue and consume VCs.
- **Interoperability and standardization:** As the standardization of VC continues, there has to be a parallel effort to enable interoperability between VCs issued and/or consumed in different ecosystems, as well as existing identity protocols that are major industrywide undertakings.
- **Decentralized identity maturity:** Although VCs can be implemented in the interim using wallet-based BYOI or pseudo-DCI infrastructure, the full benefit will be further realized only when DCI goes mainstream.

User Recommendations

- **Evaluate candidate ecosystem participants and business processes:** The project team should identify issuers, users and verifiers, and understand the data flow among them. The analysis will reveal opportunities to implement VCs for automating data exchange.
- **Make a business case for implementing verifiable credentials in the ecosystem:** The project team should define a business case that motivates participation in the ecosystem. It is important to educate participants on benefits such as reducing friction while enhancing efficiency, privacy, compliance and security.
- **Implement proof-of-concept VCs that can scale over time:** The project team should start with a minimum viable solution, using the existing vendor's capability, while having the ability to broaden and scale the solution over time. Examples are proof of employment, remote onboarding (workforce or customers), passwordless authentication, eligibility/entitlement verification or certification verification.

Sample Vendors

1Kosmos; Evernym; Finema; IBM; IdRamp; InfoCert; Microsoft; Ping Identity; SecureKey; Sphereon

Gartner Recommended Reading

Guidance for Decentralized Identity and Verifiable Claims

Innovation Insight for Decentralized Identity and Verifiable Claims

Third-Party Biometrics

Analysis By: Ant Allan, Robertson Pimentel, James Hoover

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Third-party biometrics encompasses technologies that enable the use of a person's unique morphological or behavioral traits to provide credence in a claim to an identity established for interactive access to an organization's digital assets. Typically offered as proprietary software enabling creation, storage and matching of a biometric template local to the user's device or in infrastructure, they may be implemented alone or in conjunction with nonbiometric authentication methods.

Why This Is Important

Digital identity depends upon authentication that can provide credence in an identity claim, sufficient to bring account takeover risks within an organization's risk tolerance, ideally without adding unnecessary friction. Using biometrics provides advantages over other credential-based approaches, potentially freeing the person from having to remember a password or carry a token, thus optimizing user experience (UX) and providing greater accountability (as inherent traits are not easily shared).

Business Impact

Identity and access management (IAM) and other cybersecurity leaders in many industry verticals and geographies can benefit from third-party biometrics, which can:

- Be adopted in a wide range of use cases for employee and customer authentication.
- Be used alone or as an element of multifactor authentication (MFA).

- Enable passwordless authentication to avoid the risks and frustration that passwords engender.
- Improve trust and accountability.
- Optimize UX.
- Enable high-assurance remote account recovery.

Drivers

- Ubiquity of device-native biometrics has driven interest in third-party biometrics that can make use of standard inputs (camera and microphone).
- Third-party biometrics offers organizations greater control over configuration, enrollment, choice of modes and improved customer trust. Nonlocal (central or decentralized) architectures enable portability and consistency across devices and channels.
- Organizations become increasingly interested in and have successfully deployed passwordless authentication by embedding third-party biometrics in (1) customer-facing mobile apps, especially in banking; (2) proprietary smartphone apps for passwordless MFA tools for employee and customer authentication; and (3) Fast IDentity Online (FIDO) authentication protocols, especially FIDO2.
- Increased emphasis on UX more generally, for both employee and customer authentication, gives the imperatives to improve employee and customer experience (EX/CX) within a total experience strategy. Gartner surveys have indicated that more bank customers trust third-party biometrics than trust device native biometrics, increasing customer trust in a bank that implements third-party methods.
- Organizations are increasingly adopting identity verification (“ID + selfie”) for customer onboarding and want to leverage biometric face recognition data for customer authentication and account recovery across multiple channels. This potentially extends to employee authentication, especially for gig workers.
- Voice recognition has been successfully utilized in contact centers as a welcome alternative to knowledge-based verification (KBV), which people often find frustrating and attackers readily defeat (thus providing very little confidence in an identity). It is also a natural fit for virtual personal assistant (VPA or “smart speaker”) use cases.

Obstacles

- Regional privacy laws are often seen as a barrier. However, in practice these add effort to, but do not obstruct, implementations.
- Some people view biometrics as creepy or otherwise objectionable, due to a variety of concerns, such as the risk of their biometric data being exposed or used in nefarious ways; the fear of being spied on, especially given the use of biometrics in surveillance; demographic bias; and religious, cultural and civil rights objections.
- An attacker might use a presentation attack (e.g., using a picture of the target's face). Vendors' presentation attack detection (PAD) claims require careful scrutiny. Exhaustive evaluation is beyond the capability of most buyers. Active PAD techniques may erode UX benefits. Generative AI ("deepfake") attacks demand more sophisticated countermeasures, which becomes the key differentiator among vendors.
- Usability and reliability vary across modes, populations and use cases, limiting the success with any single technology.

User Recommendations

- Optimize authentication UX or enhance trust and accountability by implementing third-party biometrics across a wide range of use cases to: (1) increase confidence in the possession of a device with embedded credentials; (2) elevate trust and accountability for higher-risk activity; (3) enable device-independent passwordless authentication; (4) support enrollment, credentialing and account recovery scenarios; and (5) support multichannel use and integration with identity verification.
- Drive acceptance of third-party biometrics usage by being open and transparent about how the technology is used, and engaging in outreach to address people's concerns.
- Fully address privacy and security needs by meeting regulatory due diligence requirements, choosing technology that can provide robust data security and demonstrate genuine human presence, and favoring privacy-preserving deployment options.

Sample Vendors

Daon; FacePhi; FaceTec; fraud.com; Imageware; iProov; Nuance; Spitch; Veridas

Gartner Recommended Reading

Innovation Insight for Biometric Authentication

Market Guide for User Authentication

Market Guide for Identity Proofing and Affirmation

Innovation Insight for Many Flavors of Authentication Token

Climbing the Slope

SCIM

Analysis By: Brian Guthrie

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

The System for Cross-Domain Identity Management (SCIM) specifications provide a protocol, schema definition and extension model for provisioning and managing identity data in cloud/hybrid applications and services. The protocol supports create, read, update and delete (CRUD) operations of identity resources, such as users, groups and custom resource extensions. SCIM is not a complete solution for full life cycle management, but defines the interfaces and formats for identity provisioning.

Why This Is Important

SCIM is a popular starting point for basic user provisioning to cloud-based targets, given its broad adoption by identity access management (IAM) vendors and ease of deployment due to standardization. SCIM helps establish and standardize the communications and identity data exchange between two different applications. SCIM is easier to implement than other non-standards-based provisioning adapters.

Business Impact

SCIM reduces the costs of building connectors, lowering technical debt and:

- SCIM is designed to be the standards-based provisioning protocol that increases an organization's application portfolio and eases provisioning without using custom connectors.
- Synchronizes and consolidates identity data.
- Simplifies use cases when provisioning to an API friendly system is required.
- Streamlines merger and acquisitions, enabling the coexistence of multiple identity providers and identity sources.

Drivers

- SCIM is being profiled to enable user event-based correlation and directory synchronization.
- After roughly ten years, implementation libraries like i2scim are getting mature enough to dynamically discover and represent different schemas and identity resources out of the box.
- SCIM has emerged as the standard for developing life cycle management in SaaS interfaces.
- SCIM is a replacement for legacy and proprietary provisioning protocols.
- Organizations looking to implement IGA or life cycle management processes include SCIM as a mandatory requirement. Most IAM vendors offering user provisioning capabilities have adopted SCIM.
- Good progress continues to be observed in the use of SCIM in provisioning gateways (i.e., Aquera, Curity, Kapstone, Radiant Logic and UNIFY Solutions), which essentially act as provisioning plug-ins. The gateways also normalize, transform and augment the data where needed.

Obstacles

- Organizations still are not familiar enough with SCIM, therefore APIs and custom connectors are still deployed instead.
- SCIM defines some standard attribute definitions and relies on custom extensions for a large portion of use cases. Not all implementations of SCIM support custom extensions. Some implementers lack libraries and schema discovery mechanisms to leverage the full power of the SCIM protocol.
- When no native SCIM connector is available, custom code will still be necessary to develop a SCIM adapter that translates requests into native APIs.
- Many providers have provisioning integration that either predates, or doesn't use SCIM. Given the pressure for integration on IGA and AM products, there is little pressure for the application providers to change.
- Inbound SCIM provisioning is still much rarer than outbound provisioning in IAM tools.

User Recommendations

- Simplify provisioning where native connectors are not available by leveraging SCIM. SCIM is an identity standard that exists today with good adoption, which can help avoid vendor lock-in.
- Replace old customized connectors, and avoid creating new connectors by adopting SCIM.
- Provide modern life cycle management protocol support and integrations to legacy systems and user storages through adopting SCIMs.
- Utilize SCIM as part of a broader fulfillment strategy, including indirect methods, like ITSM and RPA.
- Move to open protocols, such as SCIM, which standardizes the exchange of user identity information.
- Require SCIM support as part evaluating new applications.

Sample Vendors

Aquera; Curity; Kapstone; Microsoft; Okta; One Identity; Radiant Logic; SailPoint; UNIFY Solutions

Gartner Recommended Reading

IAM Leaders' Guide to Identity Governance and Administration

Modern Identity: OpenID Connect, OAuth 2.0, JWTs and SCIM 2.0

Improve IAM Architecture by Embracing 10 Identity Fabric Principles

OpenID Connect

Analysis By: Erik Wahlstrom, Brian Guthrie

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

OpenID Connect (OIDC) is an identity federation protocol built on the OAuth 2.0 framework that enables web services to externalize authentication functions. It enables applications (e.g., web-based, mobile and JavaScript) to authenticate human end users, as well as obtain basic profile information over an API.

Why This Is Important

- OIDC lets application owners and developers authenticate human users across websites and applications without having to create, manage and maintain identities.
- With OIDC, you can provide single sign-on (SSO) and use existing enterprise or social accounts to access applications and thereby improve usability, security and privacy.
- OIDC provides consent management, support for hybrid and multicloud environments, and also support for more client types than previously developed federation protocols.

Business Impact

Built on top of the OAuth 2.0 protocol, OIDC offers a flexible, efficient alternative to SAML. Its main benefits are:

- Improving user experience by providing lightweight authentication and authorization, and fine-grained consent management.
- Reducing the data entry burden during user registration with SSO and federation support.
- Providing better support for key discovery and rotation than SAML.
- Efficiently supporting token and API-centric architectures with mobile and single-page applications.

Drivers

- There is an increased interest in the protocol, which has replaced SAML in terms of preference for new client-facing and enterprise applications. The benefits that OIDC brings to API access controls, privacy regulation, consent management, step-up authentication, compliance and implementation of adaptive access will accelerate its time to plateau and become mainstream.
- Extensions built for OIDC establish a federation of federation services (multilateral federation), which is commonly used in higher education and with select industries such as healthcare, in which a common set of policies is followed.
- OIDC is a way to use a single set of user credentials to access multiple sites.
- OIDC has been proven to allow identity interactions to be conducted more seamlessly and with less friction for developers than XML-based standards, such as SAML, or purely proprietary implementations, and with greater security than preceding protocols.
- Finance, government and healthcare institutions can benefit from its increasing work to profile OIDC specifications to support, and be fine-tuned for use by, industry verticals.
- There is ongoing work to extend OpenID Connect to support more use cases. This includes fast trust establishment between OpenID providers and relying parties, support for verifiable credentials, and the establishment of standards to share risk signals.
- OIDC is mature, well supported and organizations can find certified solutions through the OpenID Connect Foundation that certifies solutions against server conformance profiles of OIDC.

Obstacles

- The list of SaaS applications supporting OIDC continues to grow; however, it still has smaller market penetration than SAML.
- Developers often underestimate the intricacies of the protocol and build homegrown libraries with “cherry-pick” features from the specification, making implementations unsecure. Instead, they should use proven and well-tested, open-source and/or vendor-provided libraries that are up to date and meet the latest security recommendations.

User Recommendations

- Give preference to OIDC over SAML. Use OIDC for modern application “greenfield” developments.Leverage an access management tool that centralizes adaptive access engines, supports multiple protocols and can translate among protocols, especially between SAML and OIDC, and other proprietary security token formats.
- Use OIDC for human user authentication, not for machines (workloads and devices) that instead should rely on the OAuth 2.0 framework to get tokens.
- Use OIDC instead of proprietary authentication methods to avoid vendor lock-in and balance security, privacy, usability and scale when building and deploying applications and services.
- OIDC is often seen as a panacea for API access control, and the ID token issued in an OIDC flow next to an access token is sometimes misused as a credential when calling APIs. Instead of using the ID token, use the access token to access APIs and therefore focus on validation of that token.

Sample Vendors

Cloudentity; Curity; ForgeRock; Gluu; Google; IBM; Microsoft; Okta; Ping Identity; Red Hat

Gartner Recommended Reading

Modern Identity: OpenID Connect, OAuth 2.0, JWTs and SCIM 2.0

Buyer’s Guide for Access Management

IAM Leaders’ Guide to Access Management

Magic Quadrant for Access Management

Architect a Modern API Access Control Strategy

Passive Behavioral Biometrics

Analysis By: Ant Allan, Akif Khan, Robertson Pimentel

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Passive behavioral biometrics silently evaluates a person's behavioral biometric traits (e.g., gestures, keystrokes), as well as other recognition and risk signals derived from how they interact with endpoint devices and application interfaces, as the basis for user authentication or otherwise to mitigate account takeover risks or new account fraud. This can be used alone or (more often) as part of a broader set of analytics.

Why This Is Important

Digital identity depends upon authentication and other methods that provide credence in an identity claim and mitigate account takeover and fraud risks to bring risks within an organization's tolerance. Evaluating recognition and risk signals from a person's normal interactions with an endpoint device and application interfaces during onboarding, login and interactive sessions can elevate trust without adding unnecessary friction to the user journey, thus optimizing user experience (UX).

Business Impact

Identity and access management (IAM) and other cybersecurity leaders in many industry verticals and geographies can benefit from investment in passive behavioral biometrics, which can:

- Mitigate onboarding and account takeover (ATO) risks for employees as well as customers.
- Be combined with other recognition and risk signals to enable continuous adaptive access.
- Elevate trust and accountability (as inherent traits are not easily shared).
- Optimize UX by reducing the need to actively challenge users.

Drivers

- Extensive use of passive behavioral biometrics to mitigate application fraud (where an attacker attempts to open a new account using someone else's identity or a synthetic identity). Analysis of behavioral biometric signals can reliably distinguish behavior patterns associated with genuine and fraudulent activity within the account opening process. It can also distinguish between people and bots.
- A desire to mitigate ATO risks without adding friction to use journeys, to enable continuous adaptive access (as part of identity-first security and a zero trust strategy) and to enhance identity threat detection and response (ITDR) approaches drives increased interest in analytics, consuming a variety of recognition and risk signals, including passive behavioral biometrics.
- Increased emphasis on UX more generally given the imperatives to improve employee experience (EX) as well as customer experience (CX) within a total experience strategy. Adding passive behavioral biometrics to other signals analytics elevates the level of trust that can be achieved, thus reducing the frequency of trust elevation (e.g., step-up authentication) needing explicit user action.
- Successful use of passive behavioral biometrics in ATO prevention as a way of counterbalancing potentially spurious risk signals that can lead to false positives. Wrongly identifying legitimate customer interactions as ATO attacks can interrupt customer journeys with prompts for step-up authentication or transaction authorization or abruptly curtail the journey altogether. So, reducing the volume significantly benefits customer UX.
- Increasing social engineering scams in which bank customers are tricked or coerced into logging into their own accounts and transferring funds to the fraudsters. Spotting signs that a user is behaving differently post-login (e.g., pausing as if receiving instructions) helps detect a scam in progress.

Obstacles

- Passive behavioral biometrics alone may not be able to provide sufficient credence in an identity claim or reliably identify fraudulent activity or other attacks.
- Baselining for each different device requires multiple interactions, making this technology unsuitable for people who log in infrequently. Some modes (e.g., handling, gait) work with only handheld devices.
- Performance can vary because of physiological differences across human clines, limitations of machine learning algorithms and training data, or circumstances (such as injury).
- For biometrics used for identification and authentication, regional privacy laws are often seen as a barrier. Restrictions on the use of advanced analytics may also inhibit adoption.
- Some people view biometrics as creepy or otherwise objectionable due to a variety of concerns, such as (1) the risk of their biometric data being misused; (2) the fear of being spied on; (3) demographic bias and potential discrimination; and (4) religious, cultural and civil rights objections.

User Recommendations

- Leverage analysis of biometric signals (in addition to investments in identity proofing) to reduce fraud and other attacks during new account opening and for remote onboarding of new employees, especially gig workers.
- Optimize authentication UX and elevate trust and accountability by implementing passive behavioral biometrics — always in combination with other recognition and risk signals — to mitigate ATO risks, enable continuous adaptive access and enhance identity threat detection and response (ITDR). Recognize that this provides less value for infrequent users and evaluate compensating controls.
- Drive the broadest acceptance of passive behavioral biometrics (and other analytics) by being open and transparent about what data is held and how it is used and engaging in outreach to address people's concerns.
- Fully address privacy and security needs by meeting regulatory due diligence requirements, choosing technology that can provide robust data security and favoring privacy-preserving deployment options.

Sample Vendors

BioCatch; Callsign; Keyless (Sift); LexisNexis Risk Solutions; Ping Identity; Plurilock Security; TypingDNA

Gartner Recommended Reading

Innovation Insight for Biometric Authentication

Market Guide for User Authentication

Market Guide for Online Fraud Detection

How to Mitigate Account Takeover Risks

Enhance Your Cyberattack Preparedness With Identity Threat Detection and Response

Entering the Plateau

OAuth 2.0

Analysis By: Abhyuday Data

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

OAuth 2.0 is an authorization protocol that is designed to delegate access to applications and services and to protect APIs. It enables any type of application (i.e., OAuth 2.0 client) such as a web application, desktop application, mobile application or an internal or external service to prove that they are authorized to access services.

Why This Is Important

OAuth 2.0 provides specific authorization flows and it underpins other identity protocols like OpenID Connect (OIDC). OAuth 2.0 enables organizations to instantly, and at scale, handle authorization to and from applications and services, and is commonly used to protect APIs and services. OAuth 2.0 also has built-in capabilities to handle privacy and can enable impersonation, delegation, consent and obfuscation of personally identifying information (PII) when needed.

Business Impact

OAuth 2.0 helps IAM leaders:

- Enable authorization to targets like web, mobile and single-page apps; APIs; microservices; and Internet of Things (IoT) use cases.
- To Improve security and simplify internal architectures in and behind API gateways by using common token formats, such as JSON Web Token (JWT), which is digitally authenticated, potentially encrypted and trusted to transfer data between various parties.
- To be able to share data of users without having to release personal information.

Drivers

- OAuth 2.0 and its derivative standards are fundamental in API access control techniques used in access management (AM), API security and API gateway technologies.
- Increasing need to support authentication and authorization decisions for modern targets like web apps, mobile and single-page apps; APIs; microservices; and IoT devices.
- Growing adoption of OIDC leads to an identity layer on top of OAuth 2.0 for new development and implementations.
- Legacy identity protocols, like Kerberos and API keys, cannot meet the security, privacy, usability and scalability requirements for modern target applications and services and they may not work for many new types of apps and services that are now being deployed.
- Increasing need to improve an organization's internal authentication and authorization architecture to make implementations easier and deployments flexible by standardizing on a token format to convey claims that are used for authorization decisions.
- Increasing need to enable privacy-preserving authorization and comply with the growing adoption of regional privacy regulations where end users can allow or deny access to their data.
- Increasing need to implement fine-grained permissions during an authorization request, for example, FAPI and Open Banking scenarios.
- Increasing need to implement interoperable step-up authentication by introducing a mechanism to check whether a presented access token satisfies authentication requirements or not and specify how to meet them.
- Emerging frameworks, such as OPA, are evolving to manage and define authorization at scale and are being used to validate JWTs received by an app through OAuth 2.0.
- All AM vendors Gartner surveyed for the latest Magic Quadrant for Access Management provide support for core OAuth 2.0. The support of OAuth 2.0 and other modern identity protocols lays down a foundation of success for broader AM programs.

Obstacles

- OAuth 2.0 is an evolving framework, and, in some specific cases, there is a lack of clearly defined best practices. Gartner clients frequently ask about the usage of OAuth flows, tokens to be used and storage of credentials.
- OAuth 2.0 is challenging to implement, due to the disparate nature of OAuth 2.0 clients and their applications. The framework specifies several grant types for different use cases. Organizations need to use optimized patterns and relevant grant types for each application type and keep track of the latest usage and recommendations, but proven patterns are hard to find.
- Many organizations still possess legacy systems where technologies like LDAP, Kerberos, certificates, API keys or just username and passwords will continue to be adopted and deployed by organizations, often regrettably, until the day the last legacy system that requires them is decommissioned.

User Recommendations

- Continue to use OAuth 2.0 to abstract authorization and balance security, privacy, usability and scalability.
- Use OAuth 2.0 to provide "just enough" privilege to calling apps and build more resilient, zero-trust-enabled systems that better withstand credential theft.
- Leverage OAuth 2.0 when applications need limited access to services; they act on behalf of the user in a limited capacity; they act on their own behalf with no human intervention.
- Use the right flow for the right type of application. A native application, a service and a single-page web application have different security capabilities and must be treated differently. Utilize the security best practices specification of OAuth 2.0 to get more details on what to do and what not to do with details on why.
- Leverage OAuth 2.0 specifications such as token exchange, Mutual TLS (MTLS) client authentication and Proof Key for Code Exchange (PKCE) to better secure OAuth 2.0 interactions.

Sample Vendors

Cloudentity; Curity; ForgeRock; IBM; Keycloak; Microsoft; Okta; One Identity; Oracle; Ping Identity

Gartner Recommended Reading

IAM Leaders' Guide to Access Management

Buyer's Guide for Access Management

Modern Identity: OpenID Connect, OAuth 2.0, JWTs and SCIM 2.0

5 Essential Ingredients of a Successful Access Management Strategy

Architect a Modern API Access Control Strategy

Device-Native Biometrics

Analysis By: Ant Allan, Robertson Pimentel, James Hoover

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Device-native biometrics encompasses embedded technologies that enable the use of a person's unique morphological traits to provide credence in a claim to an identity established for interactive access to an organization's digital assets. The technologies, which ordinarily enable access to the device itself, are integrated with a mobile business app or a third-party authenticator app via a vendor software development kit (SDK) or with Fast IDentity Online (FIDO) authentication protocols.

Why This Is Important

Digital identity depends on authentication that can provide credence in an identity claim, sufficient to bring account takeover risks within an organization's risk tolerance, ideally without adding unnecessary friction. Integrating device-native biometrics within authentication flows — typically as an alternative to a password or PIN — takes advantage of users' everyday familiarity with them to optimize user experience (UX).

Note that this is distinct from someone's access to the device itself.

Business Impact

Identity and access management (IAM) and other cybersecurity leaders in many verticals and geographies can benefit from device-native biometrics, which can:

- Be adopted in a wide range of use cases for employee and customer authentication.
- Be used alone or as an element of multifactor authentication (MFA).
- Enable passwordless authentication to avoid the risks and frustration that passwords generate.
- Optimize UX.

Drivers

- Device-native biometrics are ubiquitous in smartphones and widely available in other endpoint devices, including face and fingerprint modes in Windows Hello for Business (WHfB) in Windows 10 and 11.
- Organizations become increasingly interested in and have successfully deployed passwordless authentication by integrating device-native biometrics are integrated in (1) customer-facing mobile apps, especially in banking, (2) mobile authenticator apps providing general-purpose passwordless MFA for employees and customers, and (3) Fast IDentity Online (FIDO) authentication protocols, especially FIDO2 generally and passkeys specifically.
- Organizations' imperatives to improve employee and customer experience (EX/CX) within a total experience strategy increase interest in optimizing UX for both employee and customer authentication.
- Device-native biometrics may ease compliance with privacy mandates in comparison with third-party biometrics.

Obstacles

- Some people view biometrics as creepy or otherwise objectionable, due to a variety of concerns, such as: the risk of their biometric data being exposed or used in nefarious ways; the fear of being spied on, especially given the use of biometrics in surveillance; demographic bias and potential discrimination; and religious, cultural and civil rights objections.
- An attacker might use a presentation attack (e.g., using a picture of the target's face). The resistance of device-native biometrics to such attacks is often unknown to relying parties.
- Many implementations, such as WHfB, offer a nonbiometric alternative to biometric authentication by default (typically a PIN), which cannot provide the same credence or accountability.
- Availability, usability and reliability vary across devices, supported modes, populations and use cases, leading to inconsistent UX.
- Matching thresholds are set by device vendors, likely favoring UX over security.
- There is a lack of control over enrollment (WHfB is a notable exception).

User Recommendations

- Optimize authentication UX or enhance trust by exploiting device-native biometrics across a wide range of use cases, especially for "everyday" authentication, as an alternative to passwords and PINs.
- Drive acceptance by being open and transparent about how the technology is used, and engaging in outreach to address people's concerns.
- While device-native biometrics give people exclusive control over their biometric data, do not neglect broader privacy concerns and any regulatory due diligence requirements that may apply.
- Bear in mind that the organization typically has no control over enrollment, matching thresholds, and so on, limiting the security benefits. (Some implementations, like WHfB, can partly mitigate these limitations.)
- Evaluate the use of third-party biometrics or other alternatives for higher-risk interactions, to provide device-independent authentication, to reflect the diversity of and personal preferences among the target population, and so on.

Sample Vendors

Apple; Google; HTC; Microsoft; Samsung

Gartner Recommended Reading

Innovation Insight for Biometric Authentication

Market Guide for User Authentication

Innovation Insight for Many Flavors of Authentication Token

Identity Verification

Analysis By: Akif Khan

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Identity verification involves capturing a photo identity document and checking for signs of tampering or forgery. Capture and analysis of a photo or video clip of the person determines genuine presence. Finally, a comparison of the photo with the one in the document determines whether the person is the legitimate document bearer. Data can be extracted via optical character recognition (OCR) or from the document's chip, using near-field communication (NFC).

Why This Is Important

Establishing confidence in identity is basic to many digital interactions involving customers or employees. Although that need has persisted, the requirement for high-assurance, remote identity verification has become stronger as rapid digital transformation efforts continue. Identity verification enables organizations to be confident as to who is at the other end of that digital interaction, either prior to authentication credentials being established, or as part of the credentialing process.

Business Impact

Identity verification can be a key enabler of remote employee or customer interactions, where a high level of assurance in the claimed identity is needed for fraud prevention or compliance purposes. These use cases can include onboarding or account creation, account recovery scenarios, or elevated trust during a high-risk activity, such as a large funds transfer. This can be an alternative to using an orthodox, credential-based authentication method for such events.

Drivers

- Digital transformation has led most businesses to offer the ability to register for services online. This trend is most apparent in financial services, in which the need to "know your customers" (KYC) demands confidence in a customer's identity.
- Continued moves toward remote working have created a need for remote identity verification. In a world in which a person can apply for a job, be interviewed, land a job, then start working without ever meeting the employer face-to-face, organizations needed to adapt their processes.
- The increase in identity-based fraud in government services, such as citizens claiming benefits online, has also led to deployments of identity verification, as a fraud mitigation function, rather than a component of mandated KYC processes.
- Increasing requirements for trust and safety on marketplace platforms or gig economy platforms, in which knowing a counter-party's identity builds confidence for those using the service.
- The convergence of identity verification and authentication presents opportunities to leverage identity verification beyond the point of registration. The process can be deployed to establish confidence in identity at high-risk events, such as account recovery, should the user experience (UX) be deemed appropriate.
- Alternatively, the selfie data obtained during the identity-verification process can be used as an authentication credential, enabling features such as "login via selfie." This results in a tight coupling between the authentication event and the identity-verification event. Additional use cases involve the use of identity verification in in-person scenarios.
- The increasing obsolescence of purely data-centric techniques that rely on a user entering personally identifiable information (PII) data, which is then checked against such sources as credit bureaus, electoral rolls or, in some regions, government databases. In the face of continual breaches of data, it is prudent to assume all PII data is known to everyone.

Obstacles

- Usage costs can be prohibitive for many use cases. Outside regulated industries, where such costs are accepted to maintain compliance, difficult decisions need to be made in which cost is balanced against the tolerable level of confidence in a user's identity.
- The UX is considered too onerous by some. Questions persist about dropout rates.
- An identity-verification process that depends on users having a smartphone or a webcam raises questions about inclusion.
- Concerns persist regarding how effectively document authenticity can be assessed via remote visual inspection, and whether deepfake attacks could fool the liveness detection.
- Popular acceptance is not assured, due to concerns from users about the use of biometrics and the privacy of their data.
- The proliferation of vendors in this space makes it challenging to differentiate among them and to assess which will best meet requirements.

User Recommendations

- Assess whether identity verification is required for your use case. This can be done by asking stakeholders a critical question. "In addition to seeking evidence that the real-world identity exists, is it a requirement to have a high level of assurance that the rightful claimant of that identity is genuinely present in the digital interaction?"
- Manage a carefully considered vendor selection process by following the guidance in Buyer's Guide for Identity Proofing.
- Determine whether vendors can perform OCR tasks on non-Latin character sets, such as Arabic or Cyrillic, should users be coming from geographies using those scripts.
- Recognize that, although identity verification can be a key pillar of a mandated KYC process, it does not constitute the entirety of that process, even when vendors describe it as "eKYC." The full KYC process also involves taking the verified identity and checking it against sanctions lists and other compliance sources.

Sample Vendors

ADVANCE.AI; Daon; Incode; Inverid; Jumio; Mitek; OCR Labs; Onfido; Shufti Pro; Veridas

Gartner Recommended Reading

Buyer's Guide for Identity Proofing

Market Guide for Identity Proofing and Affirmation

Data-Centric Identity Affirmation

Analysis By: Akif Khan

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Data-centric identity affirmation (DCIA) involves checking personally identifiable information (PII) against various sources to assess an identity claim. These data sources are typically curated by vendors from multiple feeds to create identity graphs that link different identity attributes. These attributes include name, address and phone number; financial attributes such as card numbers or bank details; and digital attributes such as email, IP and device ID.

Why This Is Important

DCIA remains the mainstay for gaining confidence in a presented identity for many online use cases, either as a stand-alone capability or to augment document-centric identity proofing (DCIP). Some geographies don't have authoritative databases, such as the government databases available in many markets in Latin America (LATAM) and Asia/Pacific (APAC). In this case, vendor-managed solutions with proprietary identity graphs represent a cost-effective way to gain confidence in a presented identity for many organizations and use cases.

Business Impact

Bringing confidence in a user's identity within organizational risk tolerance is a critical business requirement for many online use cases — ranging from e-commerce to financial services and government/citizen interactions. Business benefits involve reducing fraud losses and maintaining regulatory compliance.

Drivers

- As digital transformation efforts proceed at pace, the majority of businesses offer the ability to register for services online. This registration process is open to abuse, with identity fraud and synthetic identity fraud remaining a significant challenge.
- For organizations who do not want to pay the costs for or offer the UX associated with document-centric identity proofing ("ID plus selfie"), the most viable alternative is data-centric identity affirmation. Vendor-curated identity graphs offer the most accessible way to deliver such data-centric checks. In some cases, data-centric identity affirmation is combined with ID plus selfie as part of a tiered process. It can also be used to verify the identity attributes extracted from the identity document.
- In regulated environments with formally defined know-your-customer requirements (e.g., banking, online gambling), assessing identity is very prescriptive. In some regions, it may require data-centric checks, which are most easily facilitated via vendor solutions.
- In nonregulated environments, the use of data-centric identity affirmation represents "good enough" when assessing user identity. The data-centric affirmation enables organizations to avoid the higher costs and more challenging UX of the document-centric identity proofing ("ID plus selfie") process.

Obstacles

- Querying user-entered PII against a vendor-curated database delivers identity affirmation, but fails to offer identity proofing — the assurance that the user is the rightful owner of that PII. In many cases, this may be considered acceptable based on risk tolerance, in others it will not.
- Vendors that offer identity graphs build them by procuring databases of identity data and by storing the identity attributes passed to them with each incremental identity-checking event. Some organizations will not be comfortable in passing their users' PII to a vendor who will be storing that PII to augment their own solutions.
- No single vendor has a global view of identity. Organizations dealing with a global user base will need to deal with a patchwork of regional vendors to obtain sufficient coverage.
- The steady stream of mass data breaches means that it is best to assume that all PII is known by everyone. This lowers the value of DCIA that relies on static data elements alone, especially since it does not align with a dynamic identity-first security approach.

User Recommendations

- Assess whether DCIA is sufficient for your use cases. The modest costs and relatively friction-free UX are balanced by lack of high assurance regarding the user's identity. Ensure that stakeholders are aware of this.
- Check whether the use of DCIA is sufficient to maintain compliance during the onboarding process if operating in a regulated environment.
- Increase assurance levels by using a DCIA solution that incorporates dynamic data (such as device ID) as an additional affirmation attribute on top of the more typical physical, financial and digital attributes.
- Combine the use of DCIA with DCIP to create a layered approach in which all users are checked against a vendor-curated identity graph. Only those deemed risky are then "stepped up" to DCIP for a higher assurance check. This approach can help balance security and UX concerns.

Sample Vendors

Ekata; Experian Information Solutions; GBG; LexisNexis; Pipl; Socure; TransUnion

Gartner Recommended Reading

Market Guide for Identity Proofing and Affirmation

Appendixes

See the previous Hype Cycle: Hype Cycle for Digital Identity, 2022

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 2: Hype Cycle Phases

(Enlarged table in Appendix)

Phase	Definition
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Source: Gartner (July 2023)

Table 3: Benefit Ratings

Benefit Rating ↓	*Definition* ↓
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2023)

Table 4: Maturity Levels

(Enlarged table in Appendix)

Maturity Levels	Status	Products/Vendors
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2023)

Document Revision History

Hype Cycle for Digital Identity, 2022 - 25 July 2022

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Understanding Gartner's Hype Cycles

Tool: Create Your Own Hype Cycle With Gartner's Hype Cycle Builder

Table 1: Priority Matrix for Digital Identity, 2023

Benefit	*Years to Mainstream Adoption*			
↓	*Less Than 2 Years* ↓	*2 - 5 Years* ↓	*5 - 10 Years* ↓	*More Than 10 Years* ↓
Transformational	Verifiable Credentials	Decentralized Identity		
High	Identity Verification OAuth 2.0	FIDO Identity Wallets IoT Authentication Journey-Time Orchestration Machine Identity Management OpenID Connect Third-Party Biometrics		
Moderate	Data-Centric Identity Affirmation Device-Native Biometrics	Passive Behavioral Biometrics	CAEP SCIM Zero-Knowledge Proofs	
Low				

Source: Gartner (July 2023)

Table 2: Hype Cycle Phases

Phase	*Definition*
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Phase ↓	Definition ↓

Source: Gartner (July 2023)

Table 3: Benefit Ratings

Benefit Rating ↓	Definition ↓
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2023)

Table 4: Maturity Levels

Maturity Levels ↓	*Status* ↓	*Products/Vendors* ↓
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2023)