accenture

Decentralized Digital Identity

A new approach for identity in a digital world

Unlike the physical world where driver's licenses and passports are universally accepted forms of personal identity, the digital world relies on a growing number of individual credentials, profiles, and accounts to authenticate users and provide services.

Organizations hold scores of the same sensitive user data—often unnecessarily. The practice has led privacy advocates, regulators, and the general public to scrutinize organizations' use of this siloed digital identity data and push for strong measures to safeguard it with measures such as GDPR in the EU or LGPD in Brazil, among others.[1] In addition, many common activities, such as employment and account onboarding, still rely on high-assurance *physical* documents like passports and diplomas to verify identity—a requirement that often adds time, cost, and frustration to the process.

Though we continue to rely on physical credentials, there is an increasing interest and push towards building digital identity that can be widely used and shared across organizations in a digital context. Reflecting the increased demand, the digital identity market is expected to grow to over $40 billion USD by 2027.[2]

To support the accelerated transition to digital ecosystems and deliver a seamless, transparent, and privacy-preserving digital experience that meets the needs of users, governments, and organizations requires a new approach for sharing and using identity information.

This paper discusses the role and capabilities of two types of identity systems—Identity and Access Management (IAM) and Decentralized Identity—and why the two approaches combined could serve the digital identity needs of both users and organizations in a rapidly changing and growing digital economy.

Keywords: Identity and Access Management, IAM, Decentralized Identity, Digital Transformation, Verifiable Credentials, Cryptograph, Public Key Infrastructure, PKI, Innovation, Collaboration

The evolution of digital identity models

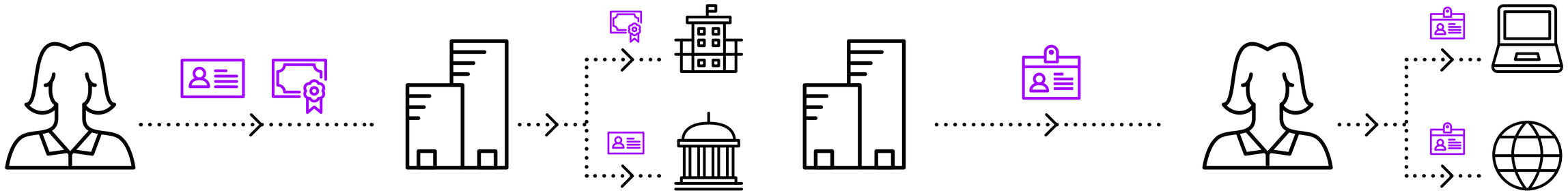
Over time the world has shifted away from physical transactions in favor of digital transactions. In the move to digital—from governments providing access to social benefits online to retailers offering mobile-based shopping experiences—organizations have built digital identity systems to support new ways of engaging with and providing services to their employees, customers, and constituents.

As technology and the prevalence of digital interactions evolve, different models for digital identity systems emerge to best support the digital identity journey.

To illustrate one example of how identity is shared and used today: Maya, a recent university graduate, is in the process of getting a new job. Her journey of sharing information and receiving credentials from her new employer, which grants her access to company buildings and systems, is represented below.

In steps 1 and 2, Maya shares information for her employer to validate. In steps 3 and 4, Maya is granted credentials by her employer after successful verification and uses her employee identity, which proves she is a valid employee of the company, to access workstations and company tools. Two key models for digital identity, Identity and Access Management (IAM) and Decentralized Identity, can support these identity processes digitally.

Figure 1: An identity journey today



1 Maya shares her University credentials and passport with her new employer

2 Her Employer receives the credentials and needs to verify them with other entities, such as the University

3 After verification, her Employer offers her the job and onboards her with new credentials

4 Maya can use her new Employee credential to log on to her workstation or access a third-party system

Identity and Access Management

Organizations everywhere use IAM systems to issue a unique set of credentials to an individual and to centrally manage user accounts, access controls, and identity workflows (e.g., signup, authentication, etc.). This set of credentials enables the individual with specific access and privileges, defined by the relationship between the individual and the organization that issued the credential. IAM systems are built to serve the organizations that own them and issue credentials to individuals solely for their specific relationship.

IAM systems are widely used for many of today's digital interactions. Such systems support two archetypes of digital identity: centralized and federated. In a centralized digital identity system, a single entity provisions and manages identity credentials. Maya's new enterprise login credentials, for instance, may be supported by a centralized system managed by her employer (steps 3 and 4).

Federated models allow the use of identity credentials established by one organizational domain to be used in another, such as in step 4 where Maya uses her employee credentials to access a third-party system. Social media-enabled logins are a common example of federation. These steps, however, usually only occur once a user has gone through the process of identity verification (steps 1 and 2).

IAM systems primarily provide functionality to establish a digital relationship (e.g., account), authenticate a user (e.g., "logging in"), and manage authorization and access to services (e.g., what a user can see and do once logged in). For the organization, IAM systems also provide mechanisms to manage workflows for the above processes, such as access request approvals or dynamic authentication flows, and they provide features to ensure regulatory compliance.

Controls to define service access rules, such as a government entity defining rules for who has access to certain benefits on their online portal, are often provided by an IAM system. Such rules are critical to the appropriate provision of services.

Though existing IAM systems may be critical to the business operations of each organization, IAM models are not designed to enable individuals to share data across a large number of organizations. For instance, Maya's IAM-based employer credentials are only used within the context of her employer's systems or limited partners (federations), even though Maya might need to prove her employment to gain access to other services such as a mortgage.

Unfortunately, over time, this approach has forced individuals to generate countless identity credentials as they form relationships with different organizations. While some, like a passport, are regularly used for verification purposes, many credentials are created and then rarely used, such as a login for a once-visited research site.

In the physical world, the use of identity credentials is already decentralized but sharing and using credentials is facilitated by paper and humans. This paper-based process often requires physical verification, e.g., a bank would have to call an employer to find out whether a set of credentials is real. In a digital world, decentralized identity capabilities need to emulate the trust between various entities in the ecosystem, and in turn enable individuals to use their identity credentials efficiently, securely, and seamlessly.

Decentralized identity

A relatively new model for identity, decentralized identity systems leverage the tamper-evident nature of cryptographic technology to provide trust in digital identity credentials, without requiring a centralized authority to coordinate the issuance, use, or verification of credentials. At the heart of a decentralized identity system is the user. A user can see, manage, and control the use of their credentials; share them with other entities, such as a bank or employer; and use them for authentication. Underlying this user-centric model for digital identity is a decentralized public key infrastructure (PKI) rooted in blockchain technology.

Decentralized identity systems are useful for the secure sharing and verification of cryptographically verifiable credentials across an ecosystem or ecosystems (such interoperability is emerging). Users can see and manage their verifiable credentials in an identity wallet and share them with others in a privacy-preserving way.

This can be accomplished, for instance, through selective disclosure and Zero-Knowledge Proofs. A zero-knowledge proof is a "cryptographic algorithm that allows users to verify information without actually disclosing the information—verifying only that the information is indeed correct with a very high probability."[3] Relying Parties or Verifiers can, in turn, easily and quickly check that the credentials shared are real and valid.

Decentralized identity can be used across much of the identity lifecycle, from identity proofing through authentication. Such systems provide greater control to the individual over what, with whom, and when their identity information is shared, which aligns with increasing regulations on privacy and user control of identity information. For organizations, decentralized identity systems offer trust in the underlying identity data being shared with them.

At Avast we see huge opportunities to enhance today's IAM solutions using Decentralized Identity technology. Organizations of every size will not only be able to provide new seamless customer and employee experiences, but will be able to save costs, reduce fraud, improve compliance and even open up new business models—all at the same time. The potential is enormous.

—Drummond Reed
Director of Trust Services, Avast

For instance, steps 1 and 2 in Maya's example, where she shares her university credentials with her employer before being onboarded, can be supported by Decentralized Identity solutions. Authentication, such as where Maya uses her employer credentials to access a system, could also be supported by decentralized identity constructs if she were issued a decentralized identity credential by her employer. This credential could be digitally shared with and verified by other entities, such as a bank or mortgage broker, and enable more seamless and fully digital experiences.

Decentralized identity systems shift the model of identity such that the user is at the center of an ecosystem whereby organizations provide credentials to an individual that can be shared with and verified by others. These credentials need to be trusted and verifiable without adding significant burden to the issuing organization or verifying parties, and without compromising the privacy and rights of the individual. Every individual and entity can own, store, use, and control their trusted credentials in a privacy-preserving way.

Decentralized identity systems should enable individuals to use digital identity credentials like they currently use physical identity credentials, e.g., a government-issued passport is presented as a trusted, verifiable credential to another organization, like a border agency or new employer. Where necessary, organizations will check the validity of the credentials against a data source or multiple data sources, or in some cases the organization accepts and trusts the credential once it has checked the physical qualities of the credential, e.g., a hologram or other physical security features.

In the digital world, decentralized identity has the capability to create an equivalent mechanism to verify the authenticity of the credential (e.g., passport really came from the government) and its data (e.g., passport's name and date of birth are real and correct). Cryptography and decentralized PKI are the mechanisms that allow decentralized identity systems to emulate the trust we have in physical credentials in a digital context, leveraging mature capabilities in how identities are verified today.

Modern IAM enables a no-compromises approach—security plus respectful personalized experiences—making it possible for enterprises to build and foster trusted digital relationships with consumers. Enabling people to share verified personal data as decentralized credentials can be a powerful new way to add value to both enterprises and consumers.

—Eve Maler
Chief Technology Officer, ForgeRock

PKI: An example of how identity is verified today

PKI[4] is a technology that has for decades helped facilitate trust in credentials, such as passports with a digital chip. Today, PKI-based digital identity systems, such as the International Civil Aviation Organization's Public Key Directory that supports electronic machine-readable travel documents, are critical to the verification of many trusted documents today. PKI-based digital identity systems typically have mature governance structures that control who have access to the system and who can issue and verify credentials.

PKI, however, is limited in its extensibility and capabilities. As accessibility to verify credentials secured by PKI is centrally managed and controlled, it is difficult to add organizations or entities. A network of legal agreements must be navigated before an organization is granted the ability to verify (or issue) PKI-based credentials, and access is still sometimes restricted to certain organizations or entities. In addition, PKI-based digital identity systems are often limited in the information that can be verified and lack some needed privacy features, such as selective disclosure.

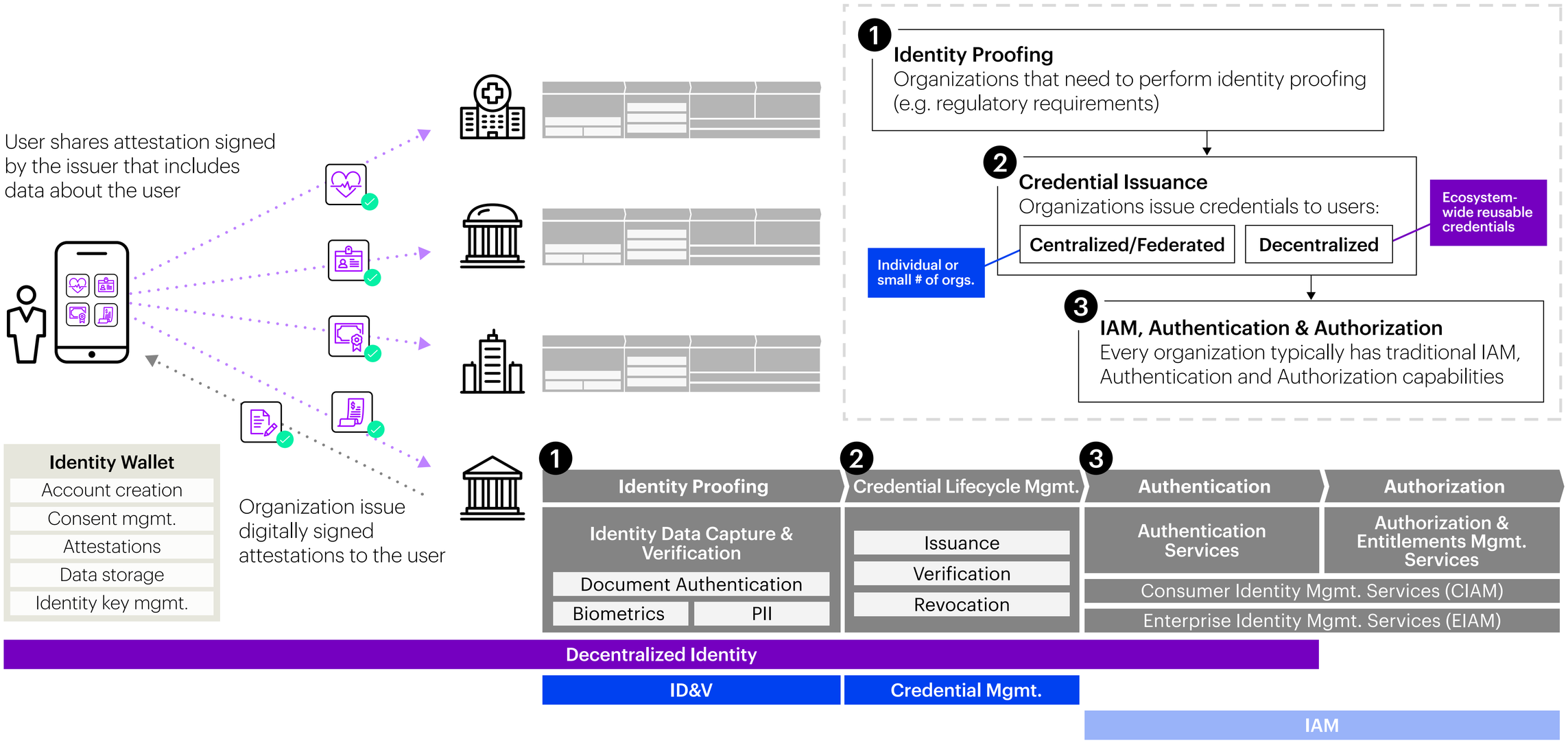
Nonetheless, PKI remains a key component to digital credential verification. PKI emerged to digitally verify credentials, and under this context have formed a well-defined, tightly governed set of verifiers and issuers. As the use of PKI and digital credentials has grown, there is an increasing need for flexibility and extensibility in PKI to grow the number of issuers and verifiers into a larger ecosystem, often beyond the immediate set of trusted parties. To truly move towards fully digital experiences, a means of trusting digital credentials must be extensible; decentralized identity models can extend the ability to use and verify credentials in larger ecosystems.

Decentralized identity and PKI are fundamentally compatible. If merged, the approach could ensure that credentials are issued by trusted entities and can be validated by a larger ecosystem of organizations to serve more use cases, including travel, healthcare, retail, banking, etc. Governance, however, must be properly established, and decentralized identity systems' governance structures continue to evolve.

> To truly move towards fully digital experiences, a means of trusting digital credentials must be extensible; decentralized identity models can extend the ability to use and verify credentials in larger ecosystems.

Why a combined approach is the future of digital identity

Figure 2: The roles of Decentralized Identity and IAM in the identity lifecycle



The future of digital identity, however, lies not in a single approach but instead in a combined approach. Joining the capabilities of IAM and Decentralized Identity enables organizations to tap each model's strengths: the portability and user control of Decentralized Identity with IAM's tailored approach that serves unique business needs. For users, the IAM-Decentralized Identity approach to identity provides more control over their data and easier, more seamless digital experiences. For organizations, the dual model helps them to maintain personalized relationships with their users with relevant trusted data, keep up with evolving standards and regulations, and reduce repetition and compliance overhead. Ultimately, a combined approach to digital identity may serve the needs of both users and organizations in a rapidly changing and growing digital economy.

In the identity lifecycle, IAM and decentralized identity provide different but overlapping approaches. IAM systems support the authentication and authorization processes once credentials are issued, while decentralized identity models support new functionality in identity wallets, the identity proofing process (identity data capture and verification), and authentication services. While decentralized identity meets the growing need for shareable, verifiable, user-controlled digital identity, IAM is specialized to meet the unique identity policy and access needs for a single organization. Combined, these two models will allow organizations to deliver more user-centric identity and digital experiences while supporting their own business and operational needs in identity and access management.

A combined approach to digital identity will also be a key enabler for participation in ecosystems—a "network of cross industry players who work together to define, build and execute market-creating customer and consumer solutions".[5] Building ecosystems is an increasingly important part of strategy for many organizations; up to 90% of C-suite executives "consider building an ecosystem business model important for… new avenues of growth".[6] More often, users are interacting with several organizations during one action, such as moving or getting a job. For users, good digital identity is a key enabler for their participation in ecosystems, where relationships with new entities can be established and maintained quickly and easily.

For instance, in our above example, Maya can take her existing relationship with her university and apply it to her employer, enabling a quicker onboarding process. By leveraging the sharing and verifying capabilities of decentralized identity with the existing approaches in IAM, organizations can maintain their existing customer and user relationships, as well as begin to engage with new users across a broader set of partners and ecosystem players.

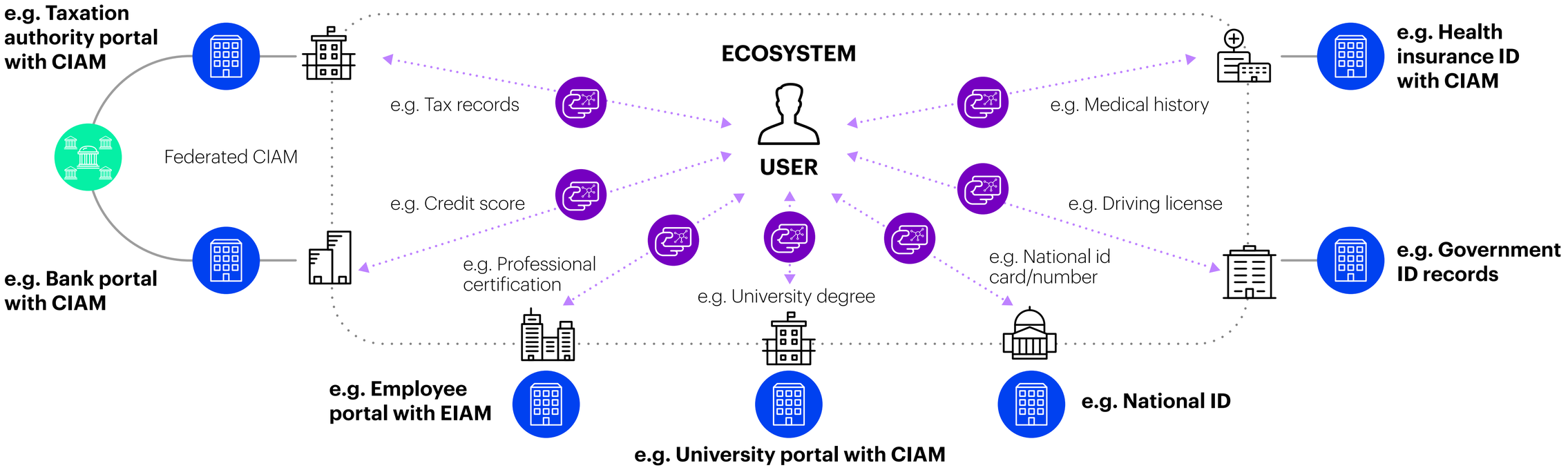
Figure 3: The future of combined identity models in a digital ecosystem

Centralized (EIAM & CIAM)
A single organization establishes and manages the identity. Trust is within the organization.

Federated ID
Administrative control by multiple, federated organizations enabling consumer and enterprise level identity services (e.g. Google sign in). Trust is 1:1 between each organization.

Decentralized ID
User control and can be used across any number of organizations on the network e.g. financial services, healthcare, education. Trust is n:n.

Example systems	Government Voter Registry Social Media Accounts	Swedish BankID Norwegian BankID	Belgian itsme Australia Post Digital ID	Known Traveler Digital Identity Canada Bank ID



This vision of digital identity as a business and ecosystem enabler is not one from the far-off future, it's now. As COVID-19 has accelerated digital adoption by users and businesses, digital identity has moved quickly to new models to support the shift.

Adopting a new digital identity approach

Introducing this new approach to digital identity systems is possible now—the technologies and tools exist and are being used today. The challenge for organizations lies in envisioning where to start and reevaluating existing business rules and processes that govern digital identity within their organizations.

What a combined approach can look like

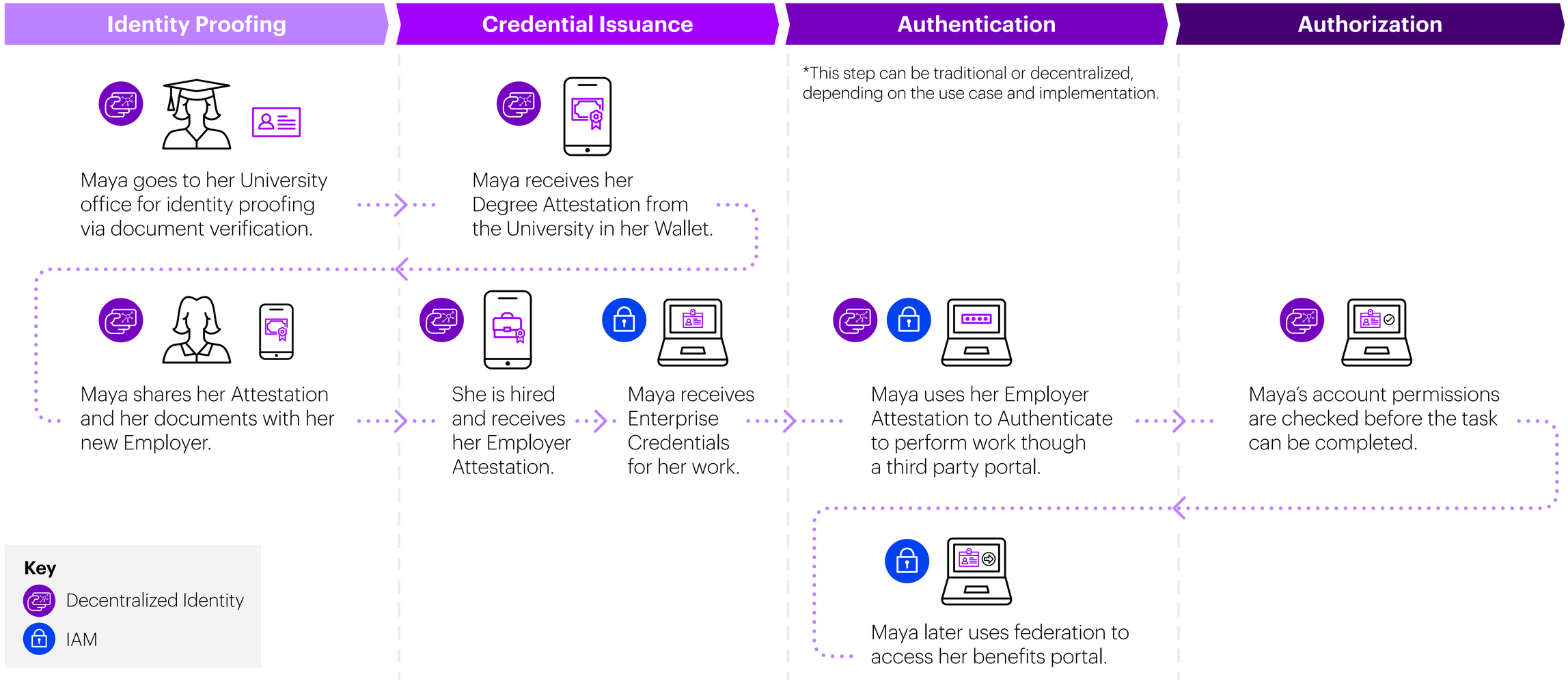
Taking our example of Maya, we can begin to envision what a combined approach to digital identity looks like in a user's journey.

In Maya's employment journey, she first needs to share her university degree with her employer. Instead of having to contact the university to send a physical copy of her paperwork to her employer, Maya is able to provide her employer with a verifiable credential issued by her university (a type of digital version of her degree certificate,) which her employer can digitally verify and trust.

Once her employer has verified her university credential (and other credentials Maya provides to her employer), she is issued both a verifiable credential from her employer and enterprise credentials for her work. These credentials are issued by the employer's IAM system. Maya can then use existing authentication methods within her enterprise to log into work systems, or use her verifiable credentials to authenticate her work portal or third-party portal using or integrating with existing systems and common authentication standards.

With a combined approach, Maya's journey is more fully digital and enables her to connect previously disjointed organizations to complete her employment journey.

Figure 4: An identity journey with a combined approach to digital identity.
Maya graduated from University. She needs to share her credentials with her new Employer and begin work.



Benefits for users and organizations

Maya's employment verification process is just one example of how a combined approach to digital identity can benefit both users like Maya and organizations such as her university and employer. Across healthcare, banking and financial services, government services, travel, and more, there are numerous processes that could benefit from this streamlined approach. From managing and sharing medical records to more effectively conducting digital banking and accessing key services distributed across several organizations, a combined use of decentralized identity and IAM unlocks new ways of doing business in a growing digital ecosystem.

To users, this combined approach introduces a way to connect their digital world and bring trusted identity wherever they interact, while maintaining their existing relationships with organizations and businesses.

Decentralized identity provides the portability needed for more seamless interactions, with enhanced privacy management capabilities, and IAM maintains a user's personalized and unique interactions with an individual organization.

With this approach, organizations gain both operational efficiency and access to a broader range of trusted data, allowing them to offer personalized services to users in an efficient, privacy-preserving way. By delivering seamless interactions to users that maintain personalization and privacy, businesses gain and strengthen user relationships. Additionally, organizations can reduce compliance overhead by replacing paper-based processes with verifiable, trusted digital identity, while maintaining their existing identity systems and organizational rules that support their services and core functions.

As the pandemic made clear, having the right IT infrastructure in place is key for our fast-evolving digital climate. Because consumer experience, security, and privacy requirements can change quickly, organizations must have the agility to support advanced digital identity approaches, such as decentralized identity, on demand. This necessitates a highly comprehensive and flexible IAM platform.

—Steve Gwizdala
Vice President Healthcare, ForgeRock

Key success factors for a new approach to digital identity

Reaping these benefits does not happen overnight. What factors make an organization's approach to a combined IAM-Decentralized digital identity successful?

To help achieve success in adopting and combining IAM and decentralized identity, organizations must have an eagerness to innovate and a willingness to adapt to a new way of thinking about digital identity. A culture that embraces innovative changes is key to ensuring existing policies, processes, and technologies are successfully adapted and integrated into a new model for identity and data sharing.

An innovative mindset also requires collaboration across different business units. It is important that an organization achieve buy-in from teams across the business, such as Security, Product, User Experience, Legal and Compliance, and Technology. For instance, changes to security policies may be required to allow new ways of authenticating users, and user experience teams will be important in ultimately designing how user interactions with the organization will change and improve.

As organizations consider new approaches to digital identity, it is critical to examine how existing proven approaches in IAM can be integrated with decentralized identity. For a digital identity to be interoperable, organizations should ensure alignment with existing open standards and protocols (e.g. ToIP, OIDC, W3C) and monitor changes as the industry and approaches evolve.

From there, an organization can embark on the process of innovation—from use case discovery and digital identity ecosystem mapping to roadmap building, through rollout and continuous innovation in digital identity. Once an organization is ready to embrace change, discovery, and an eagerness to collaborate, it can accelerate use of digital credentials across organizational boundaries.

How Accenture can help

For more than a half-century, Accenture has helped clients in different industries embrace technology innovations, including traditional IAM systems.

In the new digital era, Accenture has been a key participant in collaborating with standards bodies and global organizations, such as W3C and Trust Over IP, to drive better digital identity. In partnership with the World Economic Forum, Accenture helped launch Known Traveler Digital Identity for seamless air travel, and has worked with organizations across education, health, supply chain, finance, and more to build innovative decentralized identity and IAM systems.

Accenture has stellar capabilities to integrate a combined IAM and decentralized identity system with core organizational and business functions and cutting-edge technologies to create a holistic, future-forward solution to meet the needs of users and businesses, such as Blockchain, Biometrics, Analytics, AI, and more. As a part of an organization's journey to actualize the benefit of IAM plus decentralized identity, Accenture can assist organizations with understanding the technology landscape, planning an innovative technology strategy, and designing and co-creating digital identity systems that can launch them to the forefront of digital experiences and ways of working.

References

1. Accenture, “Jumpstart the enterprise journey to privacy-first personalization”, 2021.
2. Business Wire, “Global Digital Identity Market by Component, Authentication Type, Deployment, Organization Size, Industry Vertical, and Region,” December 9, 2021.
3. World Economic Forum, “The Known Traveller: Unlocking the Potential of Digital Identity for Secure and Seamless Travel,” January 2018.
4. For more information on PKI, see: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/public-key-infrastructure-pki
5. Accenture, “Cornerstone of future growth: Ecosystems,” May 11, 2018.
6. Accenture, “Bottling agility: Transformation through ecosystems”, February 8, 2021.

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services—all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 674,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at **www.accenture.com**

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us @AccentureSecure on **Twitter**, **LinkedIn** or visit us at **accenture.com/security**.

Accenture, the Accenture logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of Accenture and its subsidiaries in the United States and in foreign countries. All trademarks are properties of their respective owners. All materials are intended for the original recipient only. The reproduction and distribution of this material is forbidden without express written permission from Accenture. The opinions, statements, and assessments in this report are solely those of the individual author(s) and do not constitute legal advice, nor do they necessarily reflect the views of Accenture, its subsidiaries, or affiliates. Given the inherent nature of threat intelligence, the content contained in this article is based on information gathered and understood at the time of its creation. It is subject to change. Accenture provides the information on an "as-is" basis without representation or warranty and accepts no liability for any action or failure to act taken in response to the information contained or referenced in this report.

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.

This document is produced by consultants at Accenture as general guidance. It is not intended to provide specific advice on your circumstances. If you require advice or further details on any matters referred to, please contact your Accenture representative.

Copyright © 2022 Accenture. All rights reserved.
Accenture and its logo are trademarks of Accenture.

220034