The Identity 25

Okta's annual look at the top movers and shakers in the Identity world

okta

okta
Ventures

Contents

The Heroes of Identity

Even as sophisticated cyberthreats rise, most people all over the world can go about their daily lives without giving much thought to Identity. This remarkable freedom is made possible by the heroic efforts of the many engineers, academics, strategists, and business leaders who've applied their talents and tenacity for decades to make authentication secure, reliable, and relatively friction-free.

The Okta Identity 25 was created to celebrate these stars of the Identity space. Last year's inaugural list honored pioneers in Identity standards, software, hardware, credentials, regulation, and implementation. This year, we're expanding our horizons, introducing you to a new set of heroes who've championed Identity work that makes digital commerce easier, government services more accessible, privacy better protected, and a whole lot more.

Digital identity is truly coming into its own. The post-pandemic years had security and IT teams scrambling to contain their enterprises' sudden digital sprawl. Fraudsters rushed in, trying to take advantage of that chaos with faked, stolen, and synthetic identities. And now, organizations all over the world have responded with a redoubled commitment to securing digital identity, with public-private digital partnerships, evolving Identity standards, digital ID cards and wallets, and other innovations.

Just look at the avalanche of innovation and progress in the Identity space that marked 2024.

- In the European Union, the Digital Identity Framework Regulation mandates that by 2026, countries must offer at least one digital Identity wallet to all citizens and residents.
- In Australia, the Digital ID Act took effect, promising to enhance Australians' digital experience by increasing privacy guarantees and cooperation between government and private industry.
- In the US, 14 states and Puerto Rico have now implemented mobile driver's license (mDL) programs, allowing US citizens to use their phone as a legal form of ID at TSA checkpoints.

These are monumental developments, many of them years in the making, and our goal is to showcase the Identity leaders whose brilliant ideas, heartfelt collaboration, and hard work got the job done. We spent time getting to know each of the 25 honorees, and we hope to help you get to know them a little as well on the following pages. We also created videos with two of this year's honorees — Login.gov's Hanna Kim and Adobe's Eric Scouten — so you can see them discuss the rewards they derive from delighting users, the care they take in protecting their information, and how they leverage standards and protocols to ensure that no one is left behind in the digital revolution unfolding around us.

Identity is a calling, and we are very excited to share the stories of these remarkable people who answered the call to help build a future in which Identity can help make people's lives safer, fuller, and richer. We hope you'll enjoy it too.

IDENTITY 25 HONOREE

Janelle Allen

Engineering Product Manager, Webex Identity at Cisco

“Identity is a calling. It is not the profession that you choose—it’s the profession that chooses you.”

Janelle Allen, an Engineering Product Manager for Cisco, leads product management for all Identity and authentication services of the Webex business unit. It’s a formidable job, given the fierce competition and incomparable visibility in the collaboration space. And her teams face a growing need for advances in leveraging Identity to strengthen and simplify access for everyone involved. “Our goal is to meet our customers’ and partners’ expectations regarding least privilege access while also enhancing the user experience for our administrators,” she says. “For all collaboration users, we continue to focus on usability and accessibility improvements for all Identity features.”

Allen is well aware of the threat that bad actors and generative AI in the wrong hands pose to Webex users and their organizations. But she remains enthusiastic about the potential for technological advancements to transform the Identity landscape. “From my perspective, AI plays a strategic role in simplifying many of the complexities of Identity, such as defining and managing authentication and authorization policies,” she says. “AI can provide a more secure and seamless user experience by enhancing Identity verification through improved biometric systems and real-time fraud detection, for example.” And she’s bullish about quantum computing’s promise to provide Identity professionals new data retrieval and storage methods that are currently impossible.

Allen is a self-described puzzle nut, and draws joy from finding specific solutions for the many constituents of today’s interconnected digital environments. “We have to solve for people that have different abilities and challenges, like a blind person might have, or the elderly,” she says. “We must solve these challenges wherever they are.” It all adds up to something that’s more than a career. “To me, Identity is more of a calling,” says Allen. “Identity is not the profession that you choose—it’s the profession that chooses you.”

Allen is a founding member and past treasurer of IDPro, whose vision is that the disciplines of digital Identity and access management should be seen as vital and vibrant counterparts to privacy and information security. At conferences like Identiverse, she tells audiences about IDPro’s Body of Knowledge, a collection of vendor-agnostic articles that are a vast improvement upon the vendor-specific materials Identity professionals used to rely upon for training. And she points to IDPro’s CIDPRO® program, which lets Identity professionals validate their skills and experience and gives employers a way of assessing their knowledge.

But Allen hopes to find new ways to inspire more young people, and laments that the infrastructure for bringing new Identity professionals out of college and into the field isn’t yet in place. “There’s just one Identity program, at UNC Charlotte,” she points out. “It’s fantastic. I hope we can carbon copy that and make that go around the world.” For this pioneer at least, Identity represents the kind of career that can deliver a lifetime of job satisfaction. “Once Identity has got you hooked,” she says, “you’ll want to be in it forever.”

IDENTITY 25 HONOREE

Lincoln Ando

Founder, idwall

> “AI will continuously adapt to fraud patterns and optimize processes, enabling businesses to create stronger, more secure Identity systems.”

Lincoln Ando, founder of Brazil’s idwall, has a theory about why his Identity management platform has enjoyed so much success: trial by fire. “Brazil is one of the most hostile environments in the world for fraud,” he explains, noting that nearly 12% of the country’s users are victims of digital fraud each year. “Operating in Brazil has allowed us to develop unparalleled expertise and is driving successful expansion into other countries.”

A typical governmental response to cybercrime is to add layers of regulation that slow processes for consumers. Ando experienced this dynamic as a solutions architect 15 years ago. At a time when opening a checking account could be a two-week ordeal, Ando helped launch Latin America’s first 100% digital bank. “I learned the importance of creating infrastructure that was not only secure and scalable but also user-friendly to support an entirely new way of banking,” he says. Freed from the tyranny of manual verifications, banks can open a new account in under three minutes, which suits Brazilians’ demand for speed and efficiency.

Next, Ando leveraged his digital banking experience to address a verification problem in Brazil’s construction sector, where contractors and suppliers need to work together but often have no prior relationship. “False construction companies rent materials and disappear without a trace,” he explains. And so Ando founded VaiVolta, a secure marketplace where construction companies and equipment firms can establish mutual trust simply and inexpensively.

Ando understood that the fraud he alleviated in construction existed in other sectors of the Brazilian economy as well, such as car rental companies, who reportedly lose hundreds of vehicles every month. This is where idwall shines, automating Identity checks for hundreds of clients across industries, and preventing more than $350 million in fraud loss in 2024 alone.

As Identity continues to evolve, Ando sees a critical role for technologies like AI, behavioral analysis, and biometrics, but he believes practitioners have a duty to use such technologies ethically and responsibly, and to recognize their limits. “Facial recognition represents a major, important advancement in many aspects,” he points out. “For its benefits to be reaped, however, ethics must be one of the main pillars for those that use it.”

Ando believes strong Identity will allow ever more complex automation that continues to simplify our lives. “Identity management will rely on platforms that streamline process orchestration,” he says. “Ultimately, they will enhance security and user experience while helping us stay ahead in a fast-evolving digital world.”

IDENTITY 25 HONOREE

Andrew Black

Managing Director, ConnectID, Australian Payments Plus

“Every day we delay implementing robust digital Identity systems is another day we fail to protect those who need it most.”

Andrew Black, the Managing Director of Australia’s digital Identity solution ConnectID, has traveled widely to participate in Identity-focused global conferences and government meetings. At each event, experts outline hurdles that stymie quick multi-country collaboration. Nevertheless, Black insists that the challenges of international interoperability pale in comparison to the potential to do good. “I was reminded not of the differences but of the consistent human issues that Identity can solve.”

Black is passionate about the potential that digital Identity tools like ConnectID have to make an impact, seeing an urgent need to provide benefits to some of our communities’ most vulnerable populations. “Every day we delay implementing robust digital identity systems is another day we fail to protect those who need it most,” he says. Natural disasters are a frequently-cited example of how people might lose their documents, but there are other common scenarios, like domestic abuse. “When someone leaves an abusive situation, a controlling partner might deliberately withhold essential Identity documents,” he points out. The promise of a secure digital Identity, in these and other scenarios, is that it can help victims rebuild their lives more quickly, and Black has dedicated himself to the task.

“We have a once-in-a-generation opportunity in Australia to get digital Identity right,” says Black. New legislation may help: The Digital ID Act 2024 went into effect in December and promises to enhance Australians’ digital experience by encouraging cooperation among the federal government, the states and territories, and private industry. However, effecting change with this kind of complex partnership poses a monumental challenge. “Doing this is not easy,” Black acknowledges. “An identity system impacts everyone and calls for intense collaboration, putting aside individual interests to ensure we get the best solutions.”

For ConnectID, the core principles of making this kind of effort a success include choice, trust, and data minimization, according to Black. “The system needs to reduce the volume of data circulating online and ensure that what we do share is protected,” he explains. “It also needs to allow people to choose whom they trust to keep their most valuable information safe.”

Black believes that while debates over technical standards and policy are necessary, they can also be a distraction. “At its core, digital Identity is about people’s safety, their right of choice, supporting their autonomy, and ensuring everyone has secure access to essential services and opportunities.” With this focus, he says, public-private collaboration, both local and global, has the potential to build future-proof systems that will allow individuals to confidently retake control over their Identities faster.

IDENTITY 25 HONOREE

Dan Boneh

Professor of Computer Science and Electrical Engineering, Stanford University

> “We want to inform not just the tech world, but also policy makers in Washington. They need to know what is possible.”

Cryptography’s importance to digital Identity cannot be overstated; it’s the mathematical backbone that lets us hide secrets in plain sight, so we can authenticate ourselves with details like age, credentials, and membership without revealing those details to public scrutiny. That’s why we need heroes like Dan Boneh, the head of the applied cryptography group at the computer science department at Stanford University, in our corner.

Boneh has collaborated with students and colleagues on a long string of novel breakthroughs in the digital space, involving web security, cryptanalysis, cryptography for blockchains, and more, that help governments and other organizations balance security and privacy. “I tend to put my work in the public domain,” says Dan. “I am thrilled when people use the work that we do.”

Boneh and his teams are engaged in some of the most important work in privacy today, designing solutions for data sharing that preserves personal privacy. BBS, a group signature scheme that Boneh created along with Xavier Boyen and Hovav Shacham, is one such development, allowing users to demonstrate that they’re a subscriber to a news service, say, or over 21 years old, without revealing their actual identity. “It allows me to prove that I am a member of a group without revealing which member of the group I am,” he explains.

Prio, a data collection system Boneh developed with Henry Corrigan-Gibbs, performs another balancing act, allowing a government or company to collect important statistical data without knowing personal information about the individuals behind the statistics. This gained a lot of traction during the COVID-19 pandemic, when public health authorities used Prio-based tools to allow people to monitor whether they’d been exposed to COVID while ensuring the privacy of everyone’s personal health information.

In addition, Boneh worked with Shacham and Ben Lynn to develop the digital signature tool BLS, which allows organizations to aggregate a massive volume of signatures into a single signature that proves the validity of all without revealing the individuals themselves. This has important blockchain applications: With BLS, a single block doesn’t have to hold hundreds of thousands of individual signatures.

At their best, complex solutions like these are invisible to users, delivering ever greater security without damaging the user experience. Boneh compares it to driving a car: “There is incredible complexity that is happening under the hood to make your car move and be safe, but the driver is not aware of all the things the car does.” In that spirit, he predicts that industries of all stripes will continue to adopt ever more advanced cryptographic techniques to protect users, using clever cryptography solutions to gain both security and utility, instead of accepting a tradeoff.

Boneh’s on a mission to make industry actors and government decisionmakers aware of what’s newly possible. “In my area of cryptography,” says Boneh, “the best interaction between industry and academia is where industry says ‘Here are the things we would like to do, but we don’t know how to do them.’ Academics come up with proposals for how to do them, put them in the public domain, and then industry adopts them and uses them to make the world better.”

IDENTITY 25 HONOREE

Brian Campbell

Distinguished Engineer, Ping Identity

> “With the rise of AI, certain types of user authentication are going to be more prone to attack…I think we’ll see a return to good old hard math.”

Brian Campbell has a good sense of humor, and his title at Ping Identity – Distinguished Engineer – has led him to joke that he wonders what a distinguished engineer actually does for a living. Turns out this humility is a feature, not a bug. “I’ve been lucky enough to be kind of smart, but not too smart, and somewhat skeptical at the same time,” he says. “So when I run into things that feel too grandiose or too hard or too complicated, I work hard to bring them back to something I can understand and implement.” It is an approach that has served him and the Identity industry well.

In his work at Ping and elsewhere, Campbell has focused on functionality, not flash. “I help ground things, make them possible, and make them real,” he says. “There may be more techno-solution dream standards, but I prefer those that are more modest in scope because they are more likely to be realized, deployed, and used by people.”

This humanistic approach guided Campbell in his role designing and building much of PingFederate, the enterprise federation server that enables user authentication and single sign-on. “I was lucky that some of the architecture was based closely on the SAML 2.0 specifications—SAML had a really nice layering and separation of concerns that worked out well,” says Campbell.

Campbell has admiration for some of the elegant new Identity solutions arising in the field, but he speaks persuasively of the value of the tried and true. “With the rise of AI, certain types of user authentication are going to be more prone to attack, and I think we’ll see a little bit of a return to good old-fashioned cryptography and hard math,” he asserts. “AI can do a lot of things, but it’s yet to break any of that stuff and probably won’t.”

Important foundational work can be hard to justify in today’s product-driven tech landscape, which is part of what makes Campbell’s success impressive. “I’m really lucky to have been at Ping a long time, and afforded the time and autonomy to do some of this work, because it is hard to directly relate back to bottom line value,” he says. “We’re not curing cancer, here, but I do think that there’s a bigger meaning, a value to producing the standards that help a larger industry and environment flourish. That keeps me coming back.”

Campbell still thinks about his late friend and fellow Identity pioneer Vittorio Bertocci (featured posthumously on Okta’s 2024 Identity 25 list). Campbell had been stymied early in his career by some difficult concept, and a colleague suggested viewing a Bertocci video that explained it. The eureka moment led to friendship, and when the pair co-authored RFC 9470, a step-up authentication challenge protocol published weeks before Bertocci’s death, Campbell made sure to include a thank you to “the shampoo manufacturers” for their help with his long-haired friend. Importantly, Campbell’s important work with Bertocci persisted even though the two of them always worked for competing companies. Putting the public good before your personal career interests? Maybe that’s what a Distinguished Engineer does.

IDENTITY 25 HONOREE

Julie Dawson

Chief Policy and Regulatory Officer, Yoti

> “30% of people online are under 18 and we are now in the process of retrofitting a wide range of protections to support an environment built for adults.”

Julie Dawson believes that in the Identity space, trust is a two-way street. As the Chief Policy and Regulatory Officer at the digital Identity platform Yoti, she’s seen how the rise of ever more sophisticated security breaches means organizations need more systems, protocols, and standards to safeguard their data. But that’s not enough: Julie advocates that more needs to be done to make it safer for people to prove who they are, including those who do not own, don’t have access, or don’t feel comfortable using an Identity document.

Thanks in part to the ethical framework developed at Yoti, the platform addresses this challenge straight on. “We provide a wide set of ways for people to prove Identity and age. Yoti has partnered with Post Office, Lloyds Banking Group, and others to ensure that people have choices, including ways in person, to prove their age or Identity.”

There are more than 1 billion people worldwide who are unable to legally prove their Identity, and are therefore at risk of being invisible, and one of the platform’s principles is to make Yoti available to anyone.

“The Yoti team keeps listening to consumers and assessing the evolving landscape,” she says — feedback that has led Yoti to develop new offerings, such e-signatures augmented with age or Identity and verified video calls.

In particular, Yoti has devoted time and resources to the issue of assessing the age of minors online. The potential for digital education and enjoyment for children is tremendous, after all, but it has to be made safe. The complex challenge includes legal and commercial issues (minors are not legally able to enter a contract) and the higher risk minors encounter in terms of contact, conduct, and content. Yoti is building age assurance approaches that go beyond document-based age verification. “The largest demand among platforms and take-up with consumers is for AI facial age estimation,” she says. Yoti’s system can analyze a face and can estimate the ages of children 6-18, across gender and skin tone, to within 1.3 years…all without unique facial recognition or image storing.

A recognized authority on digital Identity policy and a contributor to councils including the World Economic Forum, Dawson is also passionate about Yoti’s efforts to enhance the safety, privacy, trust, and interoperability of wider credentials. The company worked pro bono to support the Good Health Pass Collaborative and its Interoperability Blueprint, designed to enable the safe sharing of both physical and digital proofs of health status. And it’s now involved as an ecosystem partner in Ayra, enabling the growth of safe, secure, interoperable, and sustainable digital trust ecosystems that connect and enrich our world. “I and the Yoti team are committed to taking part in dialogue across the industry,” says Dawson. “Myself and several other colleagues take part in a range of trade bodies, oversight groups and standards development working groups spanning digital Identity, fraud prevention, online safety, and interoperability in age assurance.

IDENTITY 25 HONOREE

Paolo De Rosa

Policy Officer, European Commission

> “Identity solutions are increasingly enablers for broader societal goals, including financial inclusion and equitable access to essential services.”

A policy officer at the European Commission who heads deployment of the European Digital Identity and Trust Services Framework, Paolo De Rosa has been instrumental in developing and implementing important Identity technologies like the EUDI Wallet. A key driver for him is the memory of growing up with a feeling of disappointment in politics as usual – and the idea that technology could provide the answers people seek.

“My generation, the first of the ‘digital natives,’ came of age during a time of profound social, political, and economic change,” he says. “Disillusioned by the unmet promises of past ideologies and the limitations of traditional collective action, we turned to the internet and technology as tools to democratize access to knowledge, foster connections, and build more inclusive communities.” This experience made him determined to help build Identity systems that balance technological quality with social equity.

As Chief Technology Officer for the Italian Government within the Presidency of the Council of Ministers, De Rosa found himself facing the demands of a once-in-a-century pandemic. And as COVID-19 began to engulf the world, De Rosa’s team decided to focus on creating a Digital COVID Certificate that would combine advanced Identity technology with broad accessibility.

“On one hand, we needed a system that was efficient, scalable, and interoperable across borders,” he says. “On the other, it had to be inclusive and accessible to all segments of society, including individuals with limited access to technology.” In the end, the team embedded data in a QR code that was both machine-readable and printable, to provide secure Identity data while allowing people without smartphones to obtain important services.

The lessons from that experience have helped prepare De Rosa for a new important Identity initiative: putting the trust framework and regulations for the EUDI Wallet into action. The system, currently in a pilot-project phase, aims to ensure security and privacy while being compatible across a variety of national systems. “Member States have varying levels of digital infrastructure maturity, which complicates harmonization efforts,” he notes. “Additionally, fostering trust among stakeholders – governments, private sector actors, and citizens – requires transparency and effective communication about the benefits and security of digital Identity systems.”

Emerging cybersecurity threats and changes in technology will continue to transform the Identity space in Europe and elsewhere. But Identity pioneers like De Rosa are ready to marshal coalitions of governmental entities to work together to keep citizens safe. “Continued investment in innovation, public awareness campaigns, and collaboration across national and EU stakeholders will be critical to maintaining momentum and ensuring digital Identity systems meet future needs.”

IDENTITY 25 HONOREE

Rodger Desai

CEO, Prove Identity

“I’ve always found it fascinating that some of the best ideas in business happen because you can take the way one industry solves their problems and bring it to another,” says Rodger Desai, CEO of Prove Identity. For Desai, who helped build Spanish telco Alcatel, this notion inspired him to bring telephony solutions to the world of Identity.

“Our thought was to bring the notion of how phones work – it’s convenient, secure, private, accurate, all at the same time, without tradeoffs – to the Internet.” Phone-based authentication is deterministic, not probabilistic: Each phone is unique. And that fact brings the potential for security and accuracy at a level not possible with passwords that can be stolen, behavior analysis that can be manipulated, and bot attacks that can succeed through brute force. “If I go to Japan,” says Desai, “I’ll connect to some random phone company, and I don’t even register with them. My SIM card will act as my proxy, with humans removed from the security process.”

Desai’s life in mobile technology began back when flip phones were the state of the art, as part of Grameen Bank’s Village Phone project in Bangladesh. “We provided cell phones to rural villagers, enabling them to generate income and connect to the broader economy.” Desai says that that experience showed him the power of the phone to connect people and to improve their lives. Fast-forward to today, where strong digital Identity management has moved from a nice-to-have to occupying a central controlling position in the modern global economy. “Identity is the key to winning in digital,” he says.

At Prove and elsewhere, Desai sees a shift from defending systems to defending people. “As businesses fortify themselves, attackers are trying to scam us into essentially authorizing their frauds,” he says. The way forward is to find ways to establish reliable circles of trust. Prove is giving its customers the confidence to trust one another through an Identity platform based on cryptographically secure keys – SIM cards, passkeys, a new vehicle called AirKey, and privacy-preserving biometric keys. “Our goal is a seamless, secure experience where consumers don’t even notice the security – they simply live their lives with confidence.”

> “Our goal is a seamless, secure experience where consumers don’t even notice the security – they simply live their lives with confidence.”

It’s been standard in the Identity space for years to talk about a seemingly intractable tradeoff: how much extra friction is required to provide adequate extra security. Desai thinks that’s a false duality. “Prove has always focused on showing that convenience and security don’t have to conflict,” he says. “Now, our challenge is demonstrating that privacy and accountability can coexist.” Desai brings that big-picture thinking to his work as a trustee at Freedom House, the pro-democracy organization founded by Eleanor Roosevelt. “At Freedom House, I advocate for tools that empower those advancing democracy and human rights while protecting privacy. This balance between trust, accountability, and privacy is critical for fostering freedom and security.”

IDENTITY 25 HONOREE

Victor Dominello

Co-Founder, ServiceGen

> "The more we strengthen individuals with more control over their personal information, the more we strengthen democracy."

The Honorable Victor Dominello knows that government is in a better position to improve people's lives than any other entity. "In government, you are literally in the engine room of society," he says. The co-founder of government services delivery pioneer ServiceGen speaks from experience, having spent over 14 years serving constituents as a member of the New South Wales (NSW) Parliament. As minister, his portfolios included Digital Government, Innovation and Better Regulation, and Customer Service; Dominello reportedly became the world's first Customer Service Minister in 2019.

Soon after his first election win in 2009, Dominello realized there was a lot of improvement needed in the way NSW delivered services, and the role digital Identity would have to play. "Government departments each strive to do their best within their silos, but the most complex, systemic problems, like homelessness, require horizontal solutions that cut across boundaries," he says. Dominello believes that government services should revolve around people's lives, not force them to navigate a difficult or fragmented government system. Key to making that work was creating a digital ID for NSW, and this became Dominello's self-described number one priority. "We can't look after the most vulnerable at speed and with the agility required in the 21st century with pen and paper."

Dominello followed the ethos of 'Design big, build small.' He points to the NSW app FuelCheck, which gives users current information on fuel prices at over 2,000 gas stations, as the kind of small, momentum-building win that helped build his larger digital ID vision. "That taught me the power of real-time feedback to innovate and meet customer expectations," he says. Next came the Service NSW app – an easy way to receive government services, acquire digital licenses and credentials, and obtain vouchers – and Park'nPay, and one of the world's first digital driver licenses. For these efforts, Dominello was named one of Australia's Top 100 innovators by The Australian – the only politician to appear on the list.

With innovations like these making government services more convenient to obtain, Dominello is leveraging digital technology, innovation, and Identity to build citizens' trust in their government. "Build trust and capability," he says, "and you'll gain confidence to scale and take on more ambitious projects." These public successes helped NSW earn a first-place ranking for ease of services (and a second-place ranking for level of trust) among six Australian states and peer countries including the United States, the UK, Singapore, Canada, and New Zealand.

Dominello sees big governmental projects like these as important to the strength of the state itself. "The single most powerful unit in a democracy is the individual; the single most powerful unit in an autocracy is the state," he points out. "The more we strengthen individuals with more control over their personal information, the more we strengthen democracy."

IDENTITY 25 HONOREE

Kim Hamilton Duffy

Executive Director, Decentralized Identity Foundation

> "We can build human-centric solutions that work at scale without compromising privacy or security."

Most IAM experts seem to come from backgrounds in the sciences, not in the humanities. To some Identity practitioners, it doesn't have to be this way, because Identity isn't just about protecting data and assets – it's about empowering people. Just ask Kim Hamilton Duffy, executive director of the Decentralized Identity Foundation (DIF). "My ongoing commitment is to ensure that as Identity systems grow more sophisticated, we never lose sight of the human impact," she says.

Duffy's own training is decidedly technical, including degrees in mathematics from the University of Texas and Cornell. But out of that background emerged a passion for the human side of digital Identity work. "It began with Blockcerts and our mission to give individuals control over their learning credentials throughout their lives," she recalls. Then at Learning Machine, she worked to find solutions to problems encountered in daily life. "How do you prove your credentials through name changes, device shifts, and even the closing of institutions?" she asks. "How do you make these solutions accessible without introducing technical barriers? These practical challenges led to fundamental questions about human Identity and agency."

Duffy champions universal accessibility, solutions that work effectively across a wide range of devices and environments, including for stakeholders who might not have a seat at the table. Her human-centered approach respects individual autonomy, including the option of not participating in digital Identity systems at all – i.e. the "right to paper." This drives her to create solutions that protect privacy while empowering individuals with meaningful control over their digital identities.

Privacy looms large for Duffy. As the Executive Director of the Decentralized Identity Foundation, she speaks and writes often about how decentralized Identity, or DI, prioritizes individual control and privacy preservation in a framework that can manage a broad range of Identity credentials and claims, balancing security and privacy.

In the real world, of course, not all authentications require government ID verification, for example. Take travel: "You might need to show a passport for border crossing," she acknowledges. "But you're also constantly sharing preferences and personal attributes that don't require any authority other than yourself."

Duffy highlights DIF's participation in the 'Personhood Credentials' paper, which has sparked numerous initiatives balancing agentic AI capabilities with human-centric design principles. "Traditional Identity systems were designed with human users in mind and often struggle with scalability, agent-to-agent interactions, and evolving security requirements," she explains. "This frequently leads to compromises like credential sharing and overly broad permissions." She sees this moment as an opportunity for DIF Labs and others to build new Identity foundations that address historical challenges and emerging needs. As one example, Duffy praises the Modular Open Source Identity Platform (MOSIP) for making robust, privacy-enhancing Identity toolkits accessible to smaller nations. "An implementation like this proves we can build human-centric solutions that work at scale without compromising privacy or security."

IDENTITY 25 HONOREE

Diego Fernández

Co-creator, QuarkID and Co-founder, The Future Co.

> “The future of Identity lies in systems that work seamlessly across borders, industries, and platforms.”

“Digital Identity is not just a technological tool, but a powerful enabler of social progress,” says Diego Fernández, the co-creator of QuarkID and co-founder of The Future Co. He’s seen both sides of this equation: Before his work in the private sector, Fernández spent eight years as an official of the city of Buenos Aires, trying to help local government deliver services to large populations.

Fernández says his background in civic life underscored the importance of scalability, inclusivity and interoperability in Identity. It also gave him a deep understanding of the challenges communities face. “Governments play a central role in citizens’ lives, yet traditional systems often struggle with inefficiencies, lack of accessibility, and vulnerability to corruption,” he says. That notion, that technological innovation can transform the lives of ordinary people and change societies, is a foundational principle for two major projects.

First, Fernández saw a need for ordinary citizens to gain greater control over their lives. This led, ultimately, to his work for QuarkID, a self-sovereign protocol that allows people to own their own digital identities using decentralized, zero-knowledge proofs backed by blockchain technologies. Buenos Aires adopted QuarkID this past October – the first government-backed SSI solution employing Ethereum’s zkSync technology.

On another front, Fernández cofounded The Future Co. to focus on reducing rural poverty with initiatives like RISE (Resource Integration for Social Empowerment), which helps communities access water, energy, education, health services and other services.

Looking ahead, Fernández believes the public and private sector can work together for citizens and consumers, but it requires patience and collaboration. Stakeholders from different worlds need time to build mutual trust, and companies need to adapt to sometimes cumbersome government processes that bring accountability and inclusivity to projects. But this kind of collaboration will yield powerful benefits down the road, he believes, including interoperability.

“The future of Identity lies in systems that work seamlessly across borders, industries, and platforms,” he says.

Identity systems will also have to confront the growing threat of crime backed by powerful AI, according to Fernández. “With the rise of AI-enabled fraud and deepfakes, Identity verification will evolve to include multi-factor authentication methods powered by biometrics, behavioral patterns, and zero-knowledge proofs.”

But in the end, Fernández is an Identity optimist. When governments and organizations can work together connecting with underserved populations, we’re, in his words, “moving toward a future where trust, privacy, and interoperability are foundational pillars, empowering individuals and transforming societies at scale.”

IDENTITY 25 HONOREE

Daniel Fett

Identity Solution Architect, SPRIN-D, German Federal Agency for Breakthrough Innovation

> “As we deploy Identity to more and more users, it is critical to keep in mind that privacy is just as important as security.”

Dr. Daniel Fett is a pioneer in developing new methods for analyzing the security of web standards. He has spent significant time on both the research and the standards and applications sides, and he’s a key contributor to the Best Current Practice for OAuth 2.0 Security standard. In his current role as Identity Solution Architect for Germany’s Federal Agency for Breakthrough Innovation (SPRIN-D), he sees both progress and room for improvement. “OAuth and peer standards are being used more and more for highly critical Identity applications, and standards are becoming more secure,” he says. “However, almost a decade after I first started looking into OAuth security, I still see the same vulnerabilities popping up from time to time, and people are still discovering new flaws.”

Fett remembers the moment he recognized the need for greater collaboration between computer science academics and Identity standards experts. At the time, he was pursuing his PhD when he and his colleagues were invited to a meeting of the IETF OAuth Working Group in Darmstadt, not far from his university in Trier, to present some of the new attacks on OAuth they found. He found the meeting so productive and essential that he proposed beginning a workshop series. This became the annual OAuth Security Workshop (OSW), regarded as one of the best venues in the Identity protocols space for identifying problems and coming up with solutions. Fett continues to organize the workshops and has managed to preserve it as a non-profit event in order to make participation possible for young academics and others who want to join the Identity space.

Fett is an admirer of the egalitarian nature of the Internet Engineering Task Force (IETF), where he does some of his work. “I like the way it operates,” he says. “It attracts passionate people from all over the world who listen to each other and who agree that despite the presence of corporate interests, the best technical solution should win.” The IETF tries hard not to favor big players – and that suits Fett, too. “There are very, very few other places where representatives of a small startup from Europe and a US tech giant can speak eye-to-eye.” He hopes this will continue, for the sake of continued progress for digital Identity.

Fett is confident that as digital Identity becomes increasingly integral to daily life, commercial offerings and government services will make life easier in many respects. However, he is wary of the potential for misuse and takes seriously his duty to offer protection. “It is easy to say, ‘We’re just building technical solutions,’ but that would be shortsighted and irresponsible,” says Fett. “As we deploy Identity to more and more users, it is critical to keep in mind that privacy is just as important as security and that our decisions in the standards space matter.”

IDENTITY 25 HONOREE

Heather Flanagan

Principal, Spherical Cow Consulting

“I would see Identity becoming as recognized and ubiquitous as cybersecurity.”

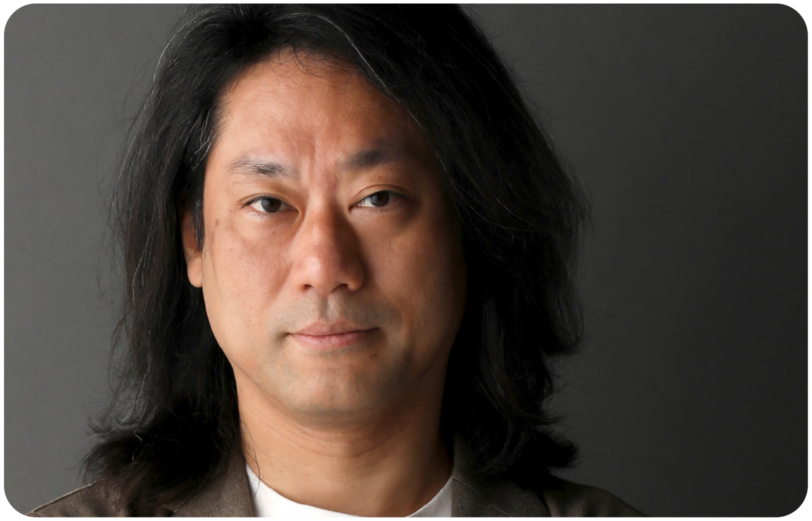
Heather Flanagan is undoubtedly the most prominent Identity hero with a master’s degree in library science. “I was supposed to be a librarian when I grew up,” she confesses. But the library’s loss is our gain, and Flanagan’s deep training in words, stories, and expression serve her and her clients well in her role as an organizational leader in the Identity space, and in side gigs as a brilliant technical writer, an enthusiastic presenter, and a prolific blogger who’s made many important contributions to standards and interoperability.

The motto of her Spherical Cow Consulting is “Translating geek to human,” an apt summation of Flanagan’s superpower. She has served executive and editorial roles in a variety of organizations and groups, including IDPro, the OpenID Foundation, ICANN, and several working groups. The common denominator of these enterprises: Flanagan bridges communications gaps, bringing together people and organizations that might not otherwise interact, enabling richer and more productive discussions about the complex Identity problems people are really trying to solve.

“The engineers and the architects – they’re brilliant, they’re wonderfully brilliant,” she acknowledges. “I rarely tell anyone this is the technical direction to take.” Flanagan’s role, rather, is to help translate what those brilliant minds do into something mere mortals can understand, so the information is truly grasped by end users and collaborators. She’s passionate about the responsibility of tech leaders to commit to communicating, rather than throwing information at end users. “Relying on user education for your service’s Identity security needs will not work,” she declares. “If users have to read something, it’s not going to happen. If you say, ‘It’s not our fault; it was in the consent banner,’ you are not making the difference you’re aiming for.”

It’s clear from her prolific writing that Flanagan’s varied background – which includes stints in systems administration and academia – allows her to see things through a wider lens than most. It’s also built in her a great appreciation of the value of collaboration and consensus, and her vision for Identity’s future includes public and private sector organizations recognizing the need for strong Identity management and providing IAM practitioners with training, career development, and other support. “I would see Identity becoming as recognized and ubiquitous as cybersecurity,” says Flanagan. “If we’re fortunate, funding will ramp up for academics to focus on Identity as its own discipline.”

Her long experience in Identity standards development has given Flanagan a deep understanding of the value of shared structure and interoperability. And she has the tools to explain the complex chaos of what’s happening today – shifting Identity frameworks, digital wallets, etc. – to laypeople in ways that make better-informed decisions more likely. “All of this is driving change faster than humans can keep up with,” she warns. “We’re definitely seeing the beginnings of what AI is bringing to the table. The next ten years will see a need for a breadth and depth of understanding to keep up with the promised efficiencies and threats in the Identity space.”



IDENTITY 25 HONOREE

Naohiro Fujie

General Manager, ITOCHU Techno-Solutions Corporation and Chair, OpenID Foundation Japan

> “Digital Identity and trust are a mixed martial art that involves a complex combination of philosophy, cognitive science, sociology, and more.”

Naohiro Fujie’s approach to Identity goes beyond its mechanisms and is informed, in part, by a humanities-based course of study unusual among his peers. Fujie studied the folklore of Arabia and the religion of pre-Islam as an undergraduate, choices that may help explain his standpoint. “Digital Identity and trust are not just about technology,” he says. “They are a mixed martial art that involves a complex combination of philosophy, cognitive science, sociology, and more.”

Fujie’s tenure at the Japanese IT services and consulting company ITOCHU Techno-Solutions Corporation began nearly a quarter century ago. His early work in active directory design and Identity lifecycle management within enterprises revealed the need for a standard interface to connect multiple systems. At the same time, the ideas of Microsoft’s Kim Cameron on the Identity Metasystem and the Laws of Identity impressed Fujie as they were gaining traction globally. Fujie began advising clients on how to apply various standards like SAML, OpenID Connect, and SCIM to enterprise and consumer Identity systems.

Fujie understands the challenge of establishing flexible standards and new practices to respond to constant changes in system architecture. “Standard technologies are essential for safety and scalability,” he acknowledges, but innovations like digital wallets can make standard technologies insufficient or even obsolete while the paint has yet to dry. The key to success, he says, is democratize standards-writing and modifications, not concentrate that responsibility with just a few. “To develop and spread standard technologies, it is essential to establish practices that involve more implementers,” he says.

From his high-visibility platform as the chair of the OpenID Foundation Japan, Fujie plans to continue raising awareness and encouraging new engineering talent to come aboard. “Credentials such as diplomas and degree certificates exist in every country,” he says. “Through joint research with academic institutions, we have learned that achieving technological and trust framework interoperability is essential.” He sees academic partnerships as essential to building a global Identity ecosystem with use cases that are grounded in reality and easy to understand.

Fujie sees his Identity work as helping move us all toward a better future, and he is enthusiastic about discussing these issues with as large an audience as possible. “Digital Identity forms the basis of our lives in digital society,” he says. “Humanity cannot live in the real world without the Internet, so we engineers must continue to develop necessary technologies and to promote awareness of Identity and trust technologies.”

IDENTITY 25 HONOREE

Ryan Galluzzo

Identity Program Lead, Applied Cybersecurity Division, NIST

“Identity is going to have to become better integrated across organizations and more multi-disciplinary. It’s going to have to become more of a team sport.”

“I really like my job … a lot.” So says Ryan Galluzzo, the Identity Program Lead at the National Institute of Standards and Technology, an agency of the Department of Commerce tasked with driving American innovation and competitiveness. And like many of his colleagues at NIST, he’s channeled this inspiration into a mission to leverage strong Identity to improve lives. “The breadth of people and ideas I am exposed to is really, really cool,” he says. “Agencies and partners who are implementing technology to make critical services available to people who are in desperate need of support. I love my job because our guidelines help agencies create real impact for real people every day.”

Galluzzo’s experience with strategies, systems, and standards – he was an officer in the US Army for nearly five years and a cyber risk expert at Deloitte for over a decade – informs his views on America’s challenges in creating a coherent digital Identity strategy. “There is a lot of excellent work happening across government,” he points out, “but it is driven by mission needs more than by an approach to achieving national level outcomes.” He believes that a consolidated approach for Identity is critical to modernizing and optimizing how government and industry can function in a digital world.

Galluzzo is humble about his role in this worthy endeavor. “I just work on standards,” he says. But by staying focused on making sure the people and organizations implementing these technologies have well-considered standards, he’s leading the way toward reining in the chaos and building a more interoperable future for Identity initiatives. Proof points include the current project to demonstrate using mobile driver’s licenses and verifiable digital credentials to open a bank account online. Galluzzo is excited by the initial results, but also by the successful collaboration with NIST’s financial service and technology partners that are transitioning standards into practice.

Galluzzo is quick to point out that compliance with NIST’s non-regulatory technical guidelines or any other standards is not enough on its own to guarantee an outstanding Identity process. “You can have a fully compliant system that’s absolutely terrible,” he says. “Maybe your password reset is terrible. Your biometric might not be performing the way you thought it would. Maybe everyone is confused about the instructions.” He says that without a focus on UX, a system for inviting feedback, and a culture of continuous evaluation and improvement, digital Identity systems are likely to create unnecessary friction and to underperform when it comes to fraud prevention.

Emerging and proliferating challenges, including generative AI, social engineering, and insider threats, are growing in complexity, promising to make Galluzzo’s work indispensable for years to come, with standards enabling the kind of collaboration that’s increasingly required. “Identity is going to have to become better integrated across organizations and more multi-disciplinary,” he says. “It’s going to have to become more of a team sport.”

IDENTITY 25 HONOREE

Sasikumar Ganesan

Head of Engineering, MOSIP; Former Chief Security Architect, Aadhaar

> “At the heart of my work lies a commitment to making the digital world more inclusive. I firmly believe technology should be a bridge, not a barrier.”

Sasikumar Ganesan’s goals are big: “My vision is to leverage innovations in cryptography, decentralized Identity, and scalable architectures to create systems where everyone, regardless of geography or socioeconomic status, can access opportunities in the digital economy.”

He has the experience to realize big dreams. As the former security chief of Aadhaar, Ganesan was deeply involved in a biometrically secured identification program that today services well over a billion people in the world’s most populous country. For him, the stakes were personal. “My own mother did not have a single Identity proof before Aadhaar,” he says, “Such foundational credentials are essential to enable access to basic services and opportunities.”

Today, Ganesan is head of engineering at the Modular Open Source Identity Platform (MOSIP), a program that helps governments around the world build Identity systems. MOSIP’s innovations make Identity widely accessible; in fact, the platform allows 90% of registration to happen offline, so it can function in areas with limited connectivity. Other features, like digitally signed QR codes, allow people to create ID cards when supply chain snags disrupt the creation of physical credentials. And it’s efficient, too: Ganesan says MOSIP’s Rapid Deployment Model, launched first in Togo and now used in more than a dozen other countries, proves governments can execute an Identity system in as little as eight weeks…an incredible feat.

Government agencies are popular targets for threat actors, and countries looking to expand Identity services always face a difficult and volatile security environment. Ganesan says that transparent, open-source systems are precisely what’s needed to meet these challenging times. “Transparency strengthens the system,” he says, “by fostering collaboration and enabling the global community to audit, test, and improve the platform continuously.”

His experiences with MOSIP and Aadhaar have granted Ganesan unique insights into the global future of Identity. He predicts decentralized verification models, with individuals largely controlling their own credentials, will come to dominate the landscape. He sees advanced cryptographic features, like zero-knowledge proofs, homomorphic encryption and selective disclosure, becoming crucial for all systems. And he expects industries and government entities to use ever more sophisticated biometric technologies to fight Identity fraud and deliver services, while paper-based credentials still persist in places that lack digital infrastructure.

It’s all progress, and ultimately, Ganesan says he wants to help build digital Identity systems that empower everyone all over the world. “My journey continues, with the belief that the convergence of technology and humanity can unlock incredible potential,” he says. “And I am deeply committed to being part of this transformative movement.”

IDENTITY 25 HONOREE

Gail Hodges

Executive Director, OpenID Foundation

"There is a new era emerging in how to deliver robust digital Identity infrastructure globally… and to build out ecosystems that leverage existing standards."

From Gail Hodges' viewpoint as the Executive Director of the OpenID Foundation, creating a shared set of standards to verify Identity is crucial as the global economy struggles to confront unprecedented fraud challenges. "Have we finally gotten to the point where the amount of cybercrime, the 'businessification' of fraud, and the number of people harmed is sufficient to actually chart a path to addressing it?" she wonders.

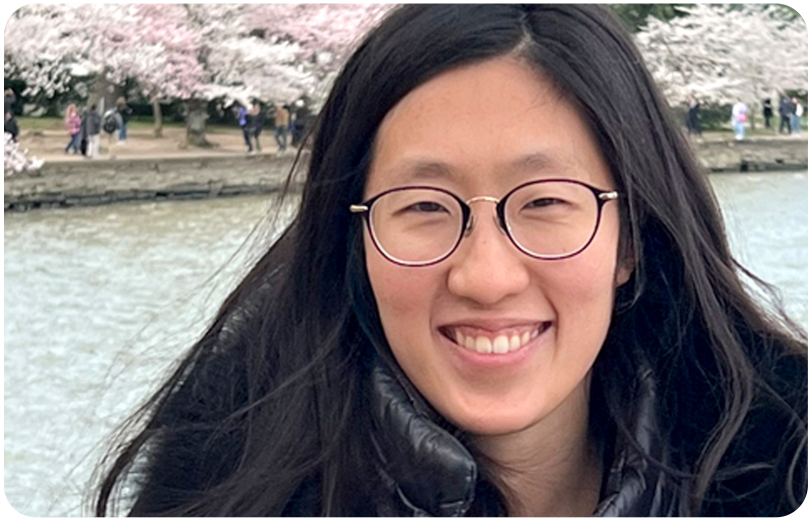
With a career that saw her leading Digital Payments at HSBC and then heading up Business Development at Apple Pay, Hodges has experienced firsthand how the uneven growth of digital Identity infrastructure creates unsustainable tensions. Private companies were far ahead of government entities, but it was these government groups that were primarily issuing credentials, and also using and regulating them. Part of the answer, she believes, is growing Identity solutions in the non-profit sector that everyone can implement.

Hodges got involved. In 2020 she launched the Future Identity Council, a global community group organized to help people obtain mobile Identity credentials. In May 2021, she joined OpenID and later became a senior advisor on Digital Identity for the California Department of Motor Vehicles. And she continues to try to help government agencies, nonprofits, and private companies develop interoperable standards that are usable by a wide range of consumers and citizens.

Building a suite of standards for all these players is needed to deliver the security and privacy users expect… but which standards? "The reality of the current standards marketplace," Hodges says, "is that there are a range of different digital Identity standards: some that are already at global scale, and some that are still in their infancy." Today, she says, different entities are engaged in "standards competition" in the global marketplace to see which protocols become widely – maybe universally – adopted. She predicts that markets backed by centralized government strategies will gain traction, and that agencies that don't adopt a strategic approach will fall behind. In the US, she's concerned that the lack of a national strategy creates liabilities for fraud prevention, national security, trust in the government and even GDP growth.

Building interoperability between the Global North and the Global South will also continue to be a challenge, according to Hodges, because in the North it's Identity stakeholders in the private sector leading development initiatives, while in the South, these are more likely to be government-led, supported by IGO and NGO funding.

But Hodges is an optimist about the regions' ability to coordinate. "I remain 'mission led' and committed to the belief that eight billion people need the option to have a digital Identity credential that they can use to assert their Identity and take part in the digital economy," she says. "And that no country should be left behind."



IDENTITY 25 HONOREE

Hanna Kim

Director, Login.gov

> “Like other forms of infrastructure, people often don’t realize how essential Identity is, or how well it’s working – until something goes wrong.”

As the director of Login.gov, which has more than 100 million user accounts, Hanna Kim often meets her customers by accident, like in a restaurant or taxi. “They tell me how surprised they were by how seamless their Login.gov experience was,” she says, and how that made them think more positively about government. It’s these small, happy moments that motivate her.

Login.gov is a portal of the US General Services Administration, and its mission is to allow people to leverage one account to access government agencies. Kim says one of her most important missions is to help foster trust in government agencies. “It’s essential we deliver secure, seamless and reliable experiences for the people we serve.”

A former principal product manager at Amazon, Kim’s well versed in working for organizations that connect directly with massive consumer bases. And with that individual connection comes a special understanding of the critical importance of Identity standards. After garnering IAL2 certification, Login.gov will build on its achievements, she says, enhancing fraud prevention and incorporating new forms of Identity evidence, like passports. IAL2 certification and a solid partnership with NIST will also allow Login.gov to partner with more agencies at the federal, state and local levels.

As Kim’s team helps millions of people access critical services, security continues to be a central concern. The rise of new sophisticated AI-powered fraud schemes poses a serious threat, Kim notes, with American adults losing $43 billion to Identity fraud in 2023. “As users and bad actors adapt to new technologies, so must we,” she says. “We need to meet users where they are while combating fraudulent schemes so that those who qualify for benefits are not excluded or unfairly delayed.”

To do so, Login.gov is partnering with private sector vendors and government agencies alike, in order to combine best-of-breed technologies and authoritative government data records. These intersecting goals have clarified Kim’s goals at Login.gov – to build trust and help millions navigate the digital space. “We’re not only proactive about strengthening our security and anti-fraud posture, but we also focus on delighting our users by introducing features and user experience improvements that make their experience with government seamless.”

IDENTITY 25 HONOREE

Gideon Lombard

Chief Operating Officer, DIDx

> “We try to stay vigilant by consistently asking, ‘Is this making someone’s life easier, safer, or more efficient?’”

Gideon Lombard is Chief Operating Officer at DIDx, a decentralized Identity company in Cape Town, Africa focused on providing reusable, verifiable digital Identity solutions. An experienced business strategist with a background in business development, project management, and digital transformation, Lombard was previously Business Development Manager at Pfortner, a provider of encrypted email, network, and messaging solutions, and drove strategic business planning, investor engagement, and software development roadmaps at MN8 Technology.

Lombard is also an accomplished actor, writer, and producer who has won over 20 awards for his creative work. His media career, he says “has equipped me with invaluable skills in storytelling, improvisation, and collaboration – qualities that have proven essential in entrepreneurship and the digital Identity space.”

Having managed large creative teams in more than 10 countries, Lombard is passionate about Africa’s vital role in generating Identity solutions that bring greater decentralization, interoperability, and user empowerment. The continent’s broad array of different demographics, with varying levels of connectivity and banking access, presents a complex challenge. But it also presents a unique proving ground for players keen to develop technology that’s interoperable across different systems, and that leverages the different strengths of businesses, governments, and regulatory agencies.

“The public sector’s ability to mandate digital Identity solutions is a crucial distinction,” Lombard says. “In contrast, in the private sector, the end user is a customer, where commercial objectives often take precedence.” He believes that, in the current landscape, perhaps a hybrid Identity strategy has the best potential to serve all constituents, with governments providing oversight while elements of Identity data are decentralized, giving individuals ownership of their data.

Furthermore, Lombard thinks companies and regulatory agencies must explain new tech in simple, compelling terms so all stakeholders can see its transformative potential. “Failure to do so risks creating a disconnect,” he warns, “where technologists build a sexy solution in search of a problem.” Instead, Lombard suggests focusing on an effective sequence of steps that allows business development to spot opportunities, which can then be capitalized upon by engineering and prototypes.

Helping unbanked and undocumented groups access healthcare, education, and financial services will demand creative problem-solving. And Lombard thinks the results could be revolutionary. “Tackling these challenges is a worthwhile endeavor,” he says. “The outcomes have the potential to transform lives and set a powerful precedent for global Identity systems.”

Most recently, Lombard organized and hosted the first-ever Internet Identity Workshop (IIW) in Africa, DID:UNCONF AFRICA, in collaboration with the IIW team. This landmark event brought together leading voices in digital Identity, fostering collaboration between the public and private sectors, startups, and regulators to advance the future of self-sovereign Identity in Africa. The event’s success underscored the continent’s potential as a global leader in decentralized Identity innovation and solidified Africa’s place in shaping the future of trust on the Internet.

IDENTITY 25 HONOREE

Nat Sakimura

Chairman, OpenID Foundation; CEO, NAT Consulting

> “The field’s ability to be inclusive and to adapt to emerging challenges will define the trajectory of digital trust in the coming decades.”

As the Chairman of the OpenID Foundation (OIDF), Nat Sakimura knows as well as anyone that helping billions of people assert their Identity wherever they choose requires building consensus. The Foundation’s stated mission is to lead the global community in creating Identity standards that are “secure, interoperable, and privacy-preserving.” But Sakimura believes that the right process is crucial, if standards are to be adopted widely in a competitive world. “Building consensus among diverse OIDF stakeholders requires a blend of structured collaboration, inclusivity, and transparency,” he says.

His passion for Identity work was born in a time of crisis. In 1999, Sakimura’s daughter underwent a failed surgery and had to be transferred to another hospital for a second attempt at the procedure. “I needed to get access to her medical records, but I couldn’t. There was no right for me to do so in Japan at the time,” he recalls. “So, I began the project to bring the right to gain access to our own data and to develop technical standardization and policymaking around digital Identity.”

Sakimura has been with OIDF for almost as long as it has existed, working tirelessly throughout his tenure to foster open, productive conversations that advance Identity ecosystems. “I often play the role of a neutral facilitator, which involves reframing contentious issues, finding common ground, and ensuring that debates remain constructive,” he says. “My focus is on guiding discussions towards practical, consensus-driven outcomes.”

The Foundation encourages participation by individuals and groups that share its vision and mission, says Sakimura, including private companies, government agencies, non-profits, and academia. The incentives to join include the opportunity to shape the evolution of open Identity specifications, to ensure that relevant scenarios are considered in protocols, and to add credibility to claims made to customers and citizens that they do, indeed, meet global standards. “Our diversity ensures that standards reflect real-world use cases across industries and geographies,” he asserts.

Sakimura recognizes the necessity of crafting technical Identity innovation within legal and policy frameworks. “Government requirements for digital Identity standards often differ significantly from those in the private sector,” he says. “In order to bridge this gap, we need to incorporate privacy-by-design principles and address regional regulatory requirements early in the process.” He points to solutions like the “Profiles” approach in OpenID Connect as an example of modularity that allows customization while maintaining interoperability within the broader Identity ecosystem.

“The evolution of Identity will be not just a technical journey, but also a societal one,” says Sakimura. “The field’s ability to be inclusive and to adapt to emerging challenges will define the trajectory of digital trust in the coming decades.”

IDENTITY 25 HONOREE

Eric Scouten

Identity Standards Architect, Adobe

> "Creators are losing contact with their audiences because the audience doesn't know what's really theirs and what's not."

Most of us typically think of individuals when we consider Identity. But Eric Scouten believes that content also has an Identity that ought to be subject to scrutiny and verification, so that it can be validated and earn our trust. Content producers in news, entertainment, sports, and government tell him that they are frustrated that their media is being manipulated to tell stories that are not authentically theirs. "Creators are losing contact with their audiences," he says, "because the audience doesn't know what's really theirs and what's not."

Scouten heads the Creator Assertions Working Group of Adobe's Content Authenticity Initiative, a coalition that helps content creators develop trust among content consumers through trust signals. He says that audiences are becoming more curious about where things are coming from, and this important work addresses what he sees as their "first layer of skepticism and a second layer of 'let's go make sure that this actually comes from where I thought it was coming from.'"

Scouten's vision is to give people clear, actionable paths to determine whether photos, videos, and other media deserve their trust. Functionally, this includes complementing C2PA's metadata standards. He explains: "The C2PA is really aimed at making metadata securely bound to content. There was no guarantee whatsoever that the attribution in the metadata is what was intended. We're actively working on defining a technical standard for taking credentials that have some attestation about an individual or an organization and binding that to the content." Such a content authenticity standard, says Scouten, will help differentiate those who merely claim to have created or modified content from those who did the actual creation or modification – a distinction consumers increasingly demand.

This intriguing initiative was born five years ago in an unlikely coalition. "The founding members in 2019 were a social media company, a news organization, and Adobe," Scouten recalls. While their businesses were vastly different, the founders shared a common vision of where generative AI was heading, and particularly its ability to misinform. They were convinced that if they didn't work quickly and proactively to meet consumers' emerging concerns, regulators might step in and try to address the problem in a way that would not preserve the creativity that content creators thrive on.

Scouten sees this project as one of the most rewarding in his long career. "I am a software engineer at heart, but I also have some skills at negotiating, at technical writing, and at building standards. This has been a happy meeting of skills and talents that are outside the normal Venn diagram of the typical software engineer."

IDENTITY 25 HONOREE

Andrew Shikiar

Executive Director and CEO, FIDO Alliance

> “Our children and grandchildren will look at passwords as my kids look at a rotary phone or a car without seatbelts —a quirky relic of history.”

“Time and time again, we’ll see enterprises suffer a major attack and only move to FIDO-based solutions as part of their remediation plan,” says Andrew Shikiar, executive director and CEO of the FIDO Alliance. When news of these cybercrime incidents spreads, it sometimes provides the push other companies need to take the leap, and reduce their reliance on weak authentication factors like passwords, and adopt better security to protect their staff, customers and assets.

The group that Shikiar leads promotes the development of passwordless authentication standards, and his role comes out of what he calls “a passion for bringing new technology concepts to market.” Before taking on the leadership of the FIDO Alliance, he worked at Sun Microsystems managing IAM products and its initial introduction of Java. It was on the Java marketing team at Sun where he was inspired by those he characterizes as some of the smartest people in Silicon Valley.

The adoption of FIDO-based solutions by giants like Amazon, Bank of America, and Target, and their growing adoption more generally across ecommerce, financial services and travel sectors, excites Shikiar. He notes that multiple case studies have shown these solutions have helped boost workforce productivity and eliminated social engineering attacks on employees and consumers alike. “Looking a bit further ahead, we can envision a future where passkeys become to user authentication what SSL is for secure websites – part of the fabric of the web itself,” he says.

Continuously updating Identity security protocols is crucial, he explains, because attack techniques are constantly evolving. For years, fraudsters have targeted user authentication as the weak spot in the Identity lifecycle. As defenses have hardened around authentication, sophisticated criminals have shifted tactics to find new ways to infiltrate protected systems. He cites recent examples including the $100 million ransomware attack against MGM Resorts that surfaced in 2023, and a 2024 report from Google that revealed that dozens of the world’s largest companies have mistakenly onboarded North Korean workers using stolen or fake identities.

“Such attacks speak to the imperative of stronger Identity verification systems that have proven biometric capabilities, certified against industry performance and security benchmarks,” says Shikiar. Securing the Identity lifecycle also requires authentication that is both difficult to compromise *and* is easy to use, to ensure it will actually be adopted. “There’s a dustbin full of strong authentication technologies that preceded passkeys that failed the usability test,” he says. Complicated, awkward authentication will tempt staff to find workarounds and customers to stop doing business with a company.

And it’s the convenience of passkeys that makes Shikiar particularly optimistic about achieving the FIDO Alliance’s goals. “More and more we’re seeing usability as a core driver for adoption,” he says. “More usable authentication leads not only to cost savings … but also to revenue expansion through increased sign-in success rates and reduced cart abandonment.”

IDENTITY 25 HONOREE

Teresa Wu

Vice President, Smart Credentials and Digital, IDEMIA Public Security North America

> “As soon as the innovation is known or done or developed – even if it’s just proof of concept – the market expects that availability is almost immediate.”

Teresa Wu, the VP of Smart Credentials at IDEMIA, is convinced that a game-changer in Identity is upon us. “Government-issued digital Identity that is cryptographically secure and verifiable is going to be a big leap forward, empowering the entire Identity ecosystem,” she says. As the lead for IDEMIA’s mobile driver’s license program, she has good reason to be excited about the moment. “There are 14-16 US states issuing mobile driver’s licenses one way or another. We are hitting critical mass, and the beauty is that they’re already interoperable because they are ISO-based. There’s no going back.”

Wu is pleased by the convergence approaches to Identity underway between government and enterprise. It occurred to her at Identiverse 2019 that these different spheres could not continue to be separate. “The two digital Identity spaces barely overlapped,” she remembers. “For government, Identity is critical infrastructure. That’s where I came from – Identity as a credential that a citizen can be recognized by so they can receive benefits from the government,” she explains. Wu says the private sector’s view was different, more like: “‘No, we’re in this bubble. For us, digital Identity is just who you need to deal with, whether it’s a customer or an employee. We are self-sufficient.’”

What changed to bring the two worlds together? Wu says that the Zero Trust mindset caused enterprise to reevaluate their willingness to accept endorsements. “They started to say, ‘Actually, we really do want to know whether we can trust those attributes and credentials. Now, government Identity has become an anchor for enterprise Identity.” She cites COVID-19, the sharp increase in digital fraud, and the emergence of AI as drivers of this fortunate convergence.

Wu has spent over two decades in biometrics and Identity, and understands that broad adoption of big changes usually takes time. “With fingerprints, it took over 15 years to become a viable biometric technology,” she says. “Same thing with facial recognition – 20 years ago, it was like flipping a coin, but now it’s this incredibly accurate thing.” Today, she says, there’s an expectation of faster market turnaround. “As soon as the innovation is known or done or developed – even if it’s just proof of concept – the market expects that availability is almost immediate.”

Wu co-founded the Women in IDEMIA Network and volunteered to be one of the 2025 AmbassadHERs of Women in Security Forum, not strictly for gender equality (“I don’t like to do diversity for diversity’s sake,” she says) but to help get more women’s voices into the Identity conversation. She’s not naturally drawn to the stage, but has made it a point to “flex [her] public speaking muscle,” as she puts it. Microsoft’s Pam Dingle was and continues to be an inspiration, and Wu explains: “Pam said to me, ‘If you’re not visible, then how can we help the next person be visible?’”

IDENTITY 25 HONOREE

Yang Xie

CEO, Authing

> “I want to use Identity to make every person, every business, and every developer more productive and reshape the way they spend their time.”

Yang Xie, founder and CEO of Beijing-based Authing, is as serious about Identity as anybody, and he holds strong views on the consequences of not giving it its proper due. “Every person needs an Identity,” he says simply, “and if not done well, there will be security issues.” Authing is a security and IAM service provider, and Xie’s goal is to build it into a global-scale computing ecosystem. “I want to use Identity to make every person, every business, and every developer more productive and reshape the way they spend their time.”

Xie says that Authing was created with developers in mind, as a reliable authentication infrastructure that can deliver security and enable high productivity and performance. “I have rich experience as a developer,” he says, “and I know what good programming languages and frameworks look like.” Authing’s Identity automation engine reduces cost and errors relative to existing manual processes, and Xie says developers appreciate the development-style logic of his platform’s approach. “It’s just like what can be done using programming languages and algorithms,” he says. “Same as any application.”

Xie, a recent Forbes 30 Under 30 honoree, thinks this developer-first approach puts Authing on a promising track for global success. “I hope Authing can become a company that serves the world, starting from developers and gradually serving everyone,” he says. “Everyone needs AI, and quantum computing is obviously a more economical method than the existing GPU solution.” Xie hopes that his understanding of what developers and enterprises want and what AI and quantum computing can do will eventually turn Authing into a global leader in productivity solutions. “Although it is far away, I am very confident,” he says.

Authing isn’t Xie’s first rodeo. He describes himself as a serial entrepreneur, having launched this business while still a college student after cutting his developer chops during a stint as an in-house hacker at TikTok parent ByteDance. He is in a group of Alibaba Cloud MVPs who work to share their expertise about the tech giant, and his work attracted the attention of Sir Tim Berners-Lee, the inventor of the World Wide Web, and Yang is now backing Berners-Lee’s Solid web project. Xie explains: “Solid is a decentralized digital Identity project. It wants everyone to have their own Identity, to control their own Identity, and to own their data. This is a very beautiful vision,” he says. “I am fascinated by it.”

Xie admits that outside of the space, Identity often takes a backseat. “People are more concerned about productivity and functions,” he says, “but Identity is everywhere.” He thinks that eventually, people will come to think of Identity like a utility – always available, and functionally indispensable. Authing, he predicts, will “make Identity management available on demand like water and electricity.”

IDENTITY 25 HONOREE

Yodahe Zemichael

Executive Director, National ID Ethiopia

“Issuing digital identification to everyone in Ethiopia has the potential to reach every household, transform lives, and pave the way for a more inclusive future.”

National digital identification system projects often set ambitious goals, and Ethiopia’s vision is no different. The program has already registered 12 million residents under its current digital Identity initiative and aims to enroll over half of its target of 90 million people by the end of 2025. But according to Yodahe Zemichael, who is leading the program, enrollment is only part of the story. “Our key performance indicators focus equally on the number of IDs issued and the number of authentications that unlock usage for service delivery,” he says. “That’s what makes our rollout of digital ID here in Ethiopia stand out.”

Ethiopia in many ways has been an ideal proving ground for a modern digital Identity case study. Before Fayda, the national digital ID system backed by biometrics which began as a pilot program in 2023, most adults in Ethiopia already had some form of functional identification, sufficient for opening a bank account, securing a passport, or enrolling in school. Once full coverage and adoption is achieved, Fayda ID will offer real-time digital Identity verification across sectors such as finance, education, health, social safety nets, agriculture, tax, and telecom. This will enable seamless service delivery through proper eKYC (electronic “know-your-customer”) protocols, empowering sector capabilities by transforming processes, reducing fraud and leakages, cutting service time, and improving overall inclusion and coverage of the population.

According to Zemichael, one of the initial challenges was building trust. “Creating public awareness—both among the general public and institutions—was critical,” he explains. “Additionally, procurement-related long lead times delayed the acquisition of biometric kits.” However, despite these hurdles, Zemichael believes the progress so far has been remarkable. “Customizing Fayda, from both legal and technological aspects, to align with our unique context has been a defining achievement,” he says proudly.

High-quality forms of identification are crucial for a government to serve its people effectively and for citizens to safely exercise their rights. “Seeing digital IDs enable access to essential services, increase inclusion, and open up opportunities—even at this early stage—has been deeply rewarding,” says Zemichael. “We believe in the power of this initiative to reach every household, transform lives, and pave the way for a more inclusive future that continues to drive the Ethiopian digital forward.”

A bold new Identity future

Our Methodology
Each year, Okta assembles an all-star selection committee of Identity experts to help determine the honorees in the year's Identity 25 initiative. This anonymous committee nominates a few dozen carefully considered candidates, including open source contributors, founders, IT specialists, technologists, academics, operators, policy makers, and more. They then meet on multiple occasions to discuss the merits of potential candidates, ultimately winnowing down the broader list to just 25 selectees. Outreach to selectees includes general and specific questions designed to elicit details to add detail to their bios and clarify their approaches to Identity. If you have someone you'd like to nominate for next year's Identity 25, please see the instructions at the lower right of this page.

.

The pioneers of Identity celebrated in this year's Identity 25 are part of a long-term, concerted effort to secure our digital world, so that global collaboration, ecommerce, online transactions, and other digital functions can be safer and easier for all the world's citizens. As you've seen in these pages, these heroes are passionate about security and usability, about maintaining consumer privacy while expanding government and enterprise services, and about thwarting fraudsters from exploiting security weaknesses to gain access to our assets and identities.

Whether it's expanding the use of digital IDs in Australia or America, helping developers log in securely in China, or strengthening the national ID system in Ethiopia, we can count on the tireless efforts of the Identity 25 to keep us moving ever closer to the secure and seamless digital future we all hope for. Individually and in collaboration, they're always hard at work behind the scenes: developing ever-smarter standards, chopping through governmental bureaucracy and enterprise competition, delivering big Identity breakthroughs and small gradual improvements. Yes, professionalized fraud groups are presenting increasingly sophisticated threats, like leveraging generative AI to create deepfake IDs that test our security controls at scale. But we're not alone, and we're lucky we've got these folks watching our back.

Thanks for joining us in celebrating this year's incredible visionaries… We'll see you in 2026!

Know an Identity pioneer you'd like to nominate for next year's Identity 25? Send your nomination, including a short paragraph describing why you think this nominee is deserving, to Identity25nominations@okta.com on or before July 1, 2025. Include any relevant links to support your case. Okta's Identity 25 Selection Committee will consider your nomination and reach out on or before October 1 informing you of their decision. Good luck!

okta
Ventures

okta

About Okta

Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology—anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at okta.com.