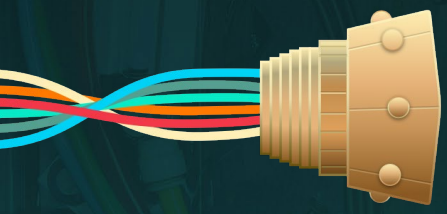
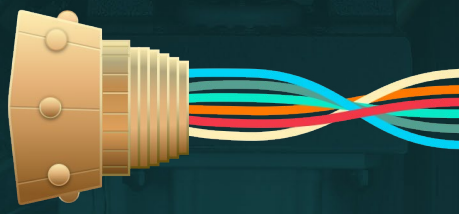
# 2024 identiverse
# TRENDS REPORT

identiverse®
A CRA Resource



THE
IDENTITY
ENGINE
Powering Our Online Lives



# 2024 Identity Trends Report

## A word from the Conference Chair Report

The digital identity industry traces its roots back to the very first days of shared computing and an effort to answer a simple question: how can multiple individuals easily use the same central resource and yet maintain the security and privacy of their data?

Today, on a global basis, billions of us use the descendants of these early shared systems multiple times every day. We stay in touch with friends and family. We read and watch current affairs, documentaries, sports, and entertainment. We learn. We teach. We buy and sell goods and services. All these capabilities, and more, are provided by governments and public services and businesses: places where we work and where, in turn, we use more online services to carry out our job functions.

The fundamental purpose of digital identity to provide convenient, secure, and privacy-respecting access to these online systems has not changed. The need for scale, pace, agility, and resilience across these areas, however, has grown almost beyond measure, and more change is on the horizon. National-level digital identity schemes, already well-established in some countries, are being adopted across many more. Cybersecurity threats against our identity systems are increasing. Risks to our privacy are becoming more widespread. All while users demand improved services with easier and safer experiences. In today's digital-first enterprises, digital identity is more than simply a line of defense: it is the cornerstone of customer enablement.

Seen in this light, the opportunity—the necessity—for the digital identity industry and its practitioners to play a leading role in shaping the future of our online world has never been more pressing or more present. Now more than ever, professionals within the industry need to share leading practices, collaborate in developing new ideas and solutions, and help leaders recognize the strategic value of digital identity projects.

This year, Identiverse celebrates 15 years of providing a platform for digital identity professionals to share their experiences and to collaborate in advancing the art and science of the industry. The Identiverse Call for Presentations, which informs the bulk of the conference agenda, provides an instructive window into the current interests and the future direction of the industry and the profession. This year's Identity Trends Report combines data from the Call for Presentations with additional industry analysis and insight and provides a valuable perspective for anyone involved in the critical field of digital identity.

Andrew Hindle
Conference Chair
**Identiverse®**

identiverse®
A CRA Resource

# THE IDENTITY ENGINE

## Powering Our Online Lives

The annual **Identiverse®** call for presentations provides a unique window into how the digital identity and security industry is responding to the shifting demands for business growth, cybersecurity posture, and regulatory compliance. Informed by a review of hundreds of call-for-presentation responses and refined by discussions with members of the Identiverse Advisory Board and other industry luminaries, we're delighted this year to release the second annual Identiverse Trends Report, providing insight into the priorities of leaders, executives, and digital identity professionals and informing your digital identity strategy for the next 12 months.

## To learn more:

VISIT THE IDENTIVERSE WEBSITE

REVIEW THE VIDEO ARCHIVE

ATTEND THE CONFERENCE

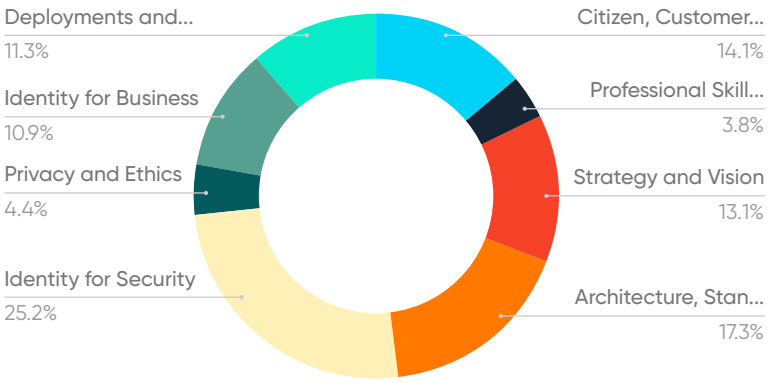
# ANALYSIS

## Identiverse 2024

Content at the 2024 Identiverse conference is broken out into 8 broad categories. Submitters are also encouraged to select from a set of subsidiary topics. You can read more about the categories and sub-topics **here**. Analysis of both the topics and the subtopics provides some interesting insight into the prevailing interests of the industry and its practitioners, a great complement to insights acquired from practitioners through the **IDPro® Skills, Programs & Diversity Survey**.

We typically see a healthy proportion of proposals for Identity for Security, Architecture & Standards, and Vision & Strategy, and this year is not different. However, it's interesting to note the increase in professionals wanting to share the specifics of their deployments and to discuss the business rationales supporting those projects. At Identiverse 2023 we spoke about the potential for C-level identity-specific role — a discussion subsequently examined in more detail by **Kuppinger Cole**.

The Identiverse 2024 CFP suggests that organizations are starting to pay more attention to the significant, even critical, role that digital identity plays not only in keeping organizations and their customers safe and ensuring appropriate levels of privacy, but in fundamentally facilitating excellent customer experiences in our increasingly digital economy.




For a look at how our larger CyberRisk Alliance audience is approaching the challenges around identity, download "**Navigating the identity security minefield**."

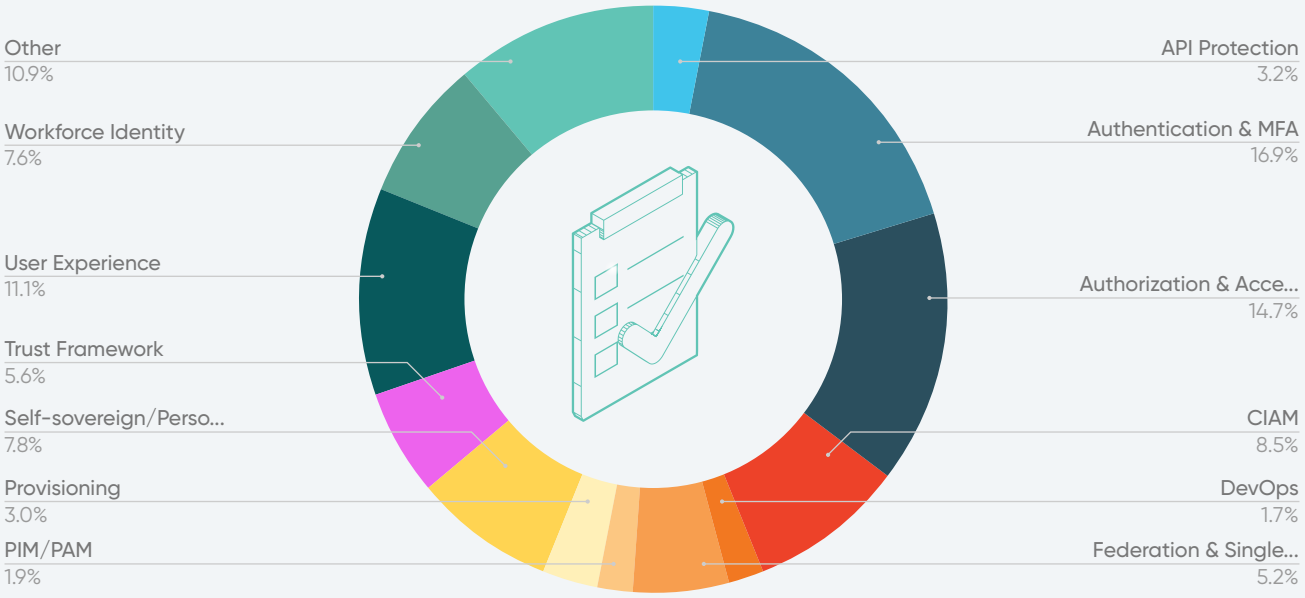
# ANALYSIS

## Identiverse 2024

Diving a little deeper and examining the sub-topics, it's unsurprising that Authentication & MFA takes the top spot. The 2023 IDPro Skills, Programs & Diversity Survey saw a significant focus by both practitioners and their organizations on the same area. Given the advent of passkeys, it is likely that we'll see this trend continue for another few years. Nearly half of the proposals in the Deployments category identified Authentication as a sub-topic: implementing standards-compliant MFA and/or passkey is clearly a priority.

It's equally interesting to note that Authorization & Access Control is a close second. During Identiverse 2023 we spoke about the need for the industry to turn its attention back to access control — an opinion also reflected in the IDPro Survey — and the industry is responding.

### TOTAL vs. SUBTOPIC

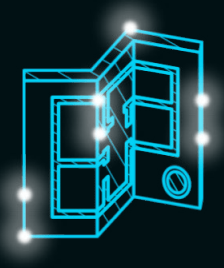


# OBSERVED TRENDS

There are other, less obvious, trends one can derive from the content review process, particularly when it comes to security, standards, and identity wallets.

## Identity and Cybersecurity

page 7



## Standards are still key

page 8

## Wallets on the Rise

page 9

## An Expanding Industry

page 10

# 1 IDENTITY AND CYBERSECURITY

As noted earlier, we see a significant proportion of proposals for talks orienting around the security aspects of digital identity — and specifically on the ways in which digital identity solutions are used as part of the overall cybersecurity design and response. In other words: architecting for identity as the security perimeter. MFA (and, increasingly, **passkey**) deployments, identity-based API protection with OAuth, and finer-grained access control with ABAC (and its cousins) generally take center stage here, with nods to **zero-trust architectures**. This year, however, we're seeing an increase in the use of digital identity orchestration (including low-code/no-code orchestration) to help co-ordinate multiple systems; and in techniques like ITDR to better instrument monitoring of threats to these identity systems.

The latter is an important point: as **identity systems become ever-more critical to business operations**, protecting those identity systems (and the data they rely on) becomes more pressing. Perhaps as a result, we see an acceleration this year in risk signaling with standards like CAEP and RISC increasingly becoming topics of discussion.

# 2 STANDARDS ARE STILL KEY

Modern digital identity is necessarily highly interoperable. Identity data is routinely exchanged between disparate systems within and across organizational boundaries; and, increasingly, between individual users and the online services they seek to use via digital wallets. Reassuringly, there's a lot of activity in the identity standards world in support of this; and it's crucial work. **Foundational standards** such as OAuth and OpenID Connect are being updated and advanced to respond to changing environments (particularly the deprecation of third-party cookies—and in this regard there's consideration of SAML, too: a much older standard but on which a large volume of large-scale deployments still rely) and to take advantage of newer approaches like verifiable credentials. We're also seeing advances in other infrastructure standards like SCIM and CTAP. Perhaps most notably, a raft of authorization specifications are being actively developed in order to allow vendors and practitioners alike to meet new requirements.

# WALLETS ON THE RISE

With the increasing adoption of user-held digital identity data such as Mobile Drivers' License (mDL), and active progress on citizen-scale digital identity projects in Europe, Australia, and several others, it's no surprise that we're seeing more interest in supporting technologies such as verifiable credentials and digital wallets. The majority of proposals received, however, are still relatively theoretical in nature: large-scale deployments are still some way off, and for every proposal exploring the potential benefits of wallet approaches, there is another one discussing challenges to navigate and risks to mitigate. The impact both on existing systems and processes will be significant; but with the levels of interest and investment across the industry is high and the tangible progress at national scale in several regions around the world, it's clear that practitioners need to start considering how to adapt to these new constructs.

# AN EXPANDING INDUSTRY

Modern digital identity is necessarily highly interoperable. Identity data is routinely exchanged between disparate systems within and across organizational boundaries; and, increasingly, between individual users and the online services they seek to use via digital wallets. Reassuringly, there's a lot of activity in the identity standards world in support of this; and it's crucial work. Foundational standards such as OAuth and OpenID Connect are being updated and advanced to respond to changing environments (particularly the deprecation of third-party cookies—and in this regard there's consideration of SAML, too: a much older standard but on which a large volume of large-scale deployments still rely) and to take advantage of newer approaches like verifiable credentials. We're also seeing advances in other infrastructure standards like SCIM and CTAP. Perhaps most notably, a raft of authorization specifications are being actively developed in order to allow vendors and practitioners alike to meet new requirements.


# IN SUMMARY

Whilst it is the Conference Chair's responsibility, with support from the Advisory Committee, to set the conference theme each year, it is the practitioners that take the time to submit proposals that make clear where the industry is going. And it is going both broader and deeper into the fabric of our digital lives, in our security and threat models, and in our services than ever before.

Identiverse 2024 will not only expand upon topics that will drive and guide the identity industry for the next 12 months; it will also provide hints for years to come. We hope to see you there, tracking the industry trends and being a part of guiding that future.

identiverse®
A CRA Resource

# THE IDENTITY ENGINE

Powering Our Online Lives

Learn more about Identiverse

Visit Identiverse.com