authenticate 2024

THE FIDO CONFERENCE

October 14-16, 2024
Carlsbad, CA

Session Guide

Mainstage	2
Technical Fundamentals and Features	3
Business Case and ROI for Passkeys	4
IAM Fundamentals	6
UX Fundamentals	7
IDV Fundamentals	8
Passkeys for Consumers	9
Passkeys in the Enterprise	11
Passkeys, Government & Policy	15
Passkeys for Payments	16
Complementary Technologies & Standards	17
Vision and Future	19

authenticate 2024
THE FIDO CONFERENCE

Agenda

Mainstage

Opening Keynote: Accelerating the Journey Towards Passkey Utopia

Two years since passkeys were first introduced, Andrew Shikiar will look at the state of user authentication and the role that FIDO Alliance and passkeys are playing therein -- including steps that the Alliance is taking to catalyze the industry towards a future free from the burdens associated with depending on passwords.

Andrew Shikiar
Executive Director and CEO, FIDO Alliance

Achieving strategic outcomes with FIDO: The phishing-resistant user

Phishing-resistant authentication is the latest authentication method that many organizations are looking to implement. These organizations are investing in phishing-resistant authentication solutions to prevent phishing attacks on their organization. To meet the business objective of preventing phishing, organizations must invest in more than just phishing-resistant authentication, they must deliver phishing-resistant users.This session will dive into how you can create a strategy for making phishing-resistant users a part of your organization. We examine the intersection of passkeys and account lifecycle to provide enterprises with the tools to build the specific strategies to remove the perils of phishing for employees, external identities and even customers.

Derek Hanson
VP Standards and Alliances, Yubico

Game On: The Journey of Passkey Launch on PlayStation

Embark on a journey through the inception and execution of the revolutionary passkey launch on PlayStation and Sony services. In this session, we delve into the intricacies of building passkey experiences across a multitude of devices, clients, apps, and consoles. From securing stakeholder buy-in to leveraging passkeys as a comprehensive password replacement solution, discover the strategies that drove success in this groundbreaking initiative. Learn how we navigated the dynamic landscape of authentication, adapting to the emergence of passkeys and delivering a seamless user experience. Join us as we explore the innovative solutions that set new standards for security and user convenience in the gaming industry.

Cam Champeau
Product Manager, Sony Interactive Entertainment (PlayStation)

The two simple rules for creating passwordless authentication for consumers

The move to passwordless authentication has started and while some are well along the path, there are many who are yet to get started. In this session you will focus on two simple rules to follow as you start your passwordless journey. Whether you're a seasoned authentication professional or just an enthusiast, this session will provide invaluable insights into the future of authentication and how you can get there.

Mike Slaugh
Principal Security Engineer, Amazon

We love passkeys - but how can we convince a billion users?

It's clear that passkeys will be core component of a passwordless future. The useability and security advantages are clear. What isn't as clear is how we actually convince billions of users to step away from a decades-long relationship with passwords and move to something new. Join us as we share insights on how to accelerate adoption when users, platforms, and applications needs are constantly evolving. We will share practical UX patterns and practices, including messaging, security implications, and how going passwordless changes the concept of account recovery.

Scott Bingham
Principal Product Manager, Microsoft

Sangeeta Ranjit
Principal Product Manager Lead, Microsoft

Agenda

Technical Fundamentals and Features

Passkeys 101: Technical Principles of FIDO

Hear a deep dive on passkeys, including what they are, how they work, why the FIDO Alliance has introduced them, and how you should be thinking about them in your authentication strategy

David Turner
Sr. Technical Director, FIDO Alliance

CTAP 2.1: FIDO's new tricks for passkeys on security keys

A lot has happened in the world of passkeys over the past year, with a particular focus on improving usability – including FIDO CTAP. Now that CTAP 2.1 devices are hitting the market, and support is arriving in browsers and operating systems, it's a great time to take a look at what's available (and what's coming soon) for passkeys on security keys. The FIDO Alliance published the newest revision of the CTAP standard in June of 2022. Since then, hardware manufacturers, operating system and browser vendors, and identity providers have been adding new capabilities to security keys. This session will cover the new features that are included in CTAP 2.1, like the various types of blob storage, PIN related enhancements, and enterprise attestation, as well as the finalized features from the CTAP 2.1 preview, like credential management and biometric enrollment. We'll touch on the current platform support landscape for desktop and mobile, and some practical use cases. By the end of the session, attendees will have a better idea of the features that are right around the corner for passkeys on security keys.

Will Smart
Sr. Solutions Architect, Yubico

"How do I...?" Answering common questions from RP devs

Come hear answers to five common "how do I..." questions that Relying Party developers ask when adopting FIDO2-based authentication. I'll walk you through why people are asking these questions, and provide context for answers that might just surprise you.

Matthew Miller
Technical Lead, Cisco

Passkeys on Windows: New Platform Features

This is an exciting year for us as we are bringing some great passkey features to Windows users. In this session, I will discuss our new capabilities for synced passkeys protected by Windows Hello, and I'll walk through a plugin model for third-party passkey providers to integrate with our Windows experience. Taken together, these features make passkeys more readily available wherever users need them, with the experience, flexibility, and durability that users should expect when using their passkeys on Windows.

Bob Gilbert
Software Engineering Manager, Microsoft

Peeling back the passkeys onion

"What is this new UI?" "Why is there a browser UI and one from my OS?" "Why do I see this only on my laptop and not my phone?" "Do I have to use my device's vendor for all my passkeys?" "Where did the FIDO token option go???" "Can I use my passkeys across ecosystems?" Passkeys support started popping up on billions of devices around the globe in 2023 and the questions exploded as they brought new user experiences, behavior changes, and new options for users and organizations. We'll dive into the intricate relationships between websites, browsers, apps, operating systems, passkey providers, and security keys, and each party's role and impact on user experience and functionality.

Tim Cappalli
Sr. Architect, Identity Standards, Okta

authenticate 2024
THE FIDO CONFERENCE

Agenda

Technical Fundamentals and Features

Shift into high gear: Answering common questions to help you get off the starting line

Have you wondered about where to start with implementing FIDO for your web sites and services? Maybe you've done some research but phrases like "MDS", "attestation", and "challenge" make things confusing. Let us help you lift the fog of confusion as we go through the top 5 questions about implementing FIDO2. We've scientifically pulled these questions as the most asked by looking at Stack Overflow, reading too many Reddit posts, and personal experience. At the end of this session you'll have the tools and understanding you need to start the path to become an expert FIDO developer.

Karen Larson
Senior Director of Product Management, Uniken

Matthew Miller
Technical Lead, Cisco

Understanding Passkey UserVerification and its Impact on Authentication Experiences in your Products

Passkeys are an incredible advancement of phishing resistant credentials which improve user experience as well security for everyone; from individual users up through our critical infrastructure. But under the hood, Passkeys are complex and offer an array of optional parameters which impact how the authentication is performed. UserVerification (UV) is one of those parameters and it controls whether or not a user has to verify themselves with the FIDO credential before that credential can be used to authenticate with a relying party. Its simplicity of only having 3 values (+ null) makes it easy to confidently choose a one-size fits all solution which could end up having a negative impact on your security posture, overall UX, and/or customer satisfaction with your products. In this session we will discuss the WebAuthN/Passkey UserVerification authentication parameter and how its options function during Passkey registration and authentication events. We'll build on that knowledge and apply it to real world scenarios which demonstrate some things to consider as you apply the UV parameter in your authentication flows. We'll also highlight examples where a friction-first approach may be appropriate and what could possibly happen if you chose the wrong option for the use case.

Jeff Corrigan
Senior Product Manager - Identity Platforms, Yahoo

Business Case and ROI for Passkeys

Bridging the Trust Gap: Strategies for Overcoming Skepticism in Biometrics Adoption

Biometric authentication is recognized as a promising technology for enhancing security and convenience, however, despite its potential, widespread adoption of biometrics is hindered by persistent concerns surrounding privacy, security vulnerabilities, and the overall impact of generative AI on the reliability of biometrics overall. Consequently, building trust among users and stakeholders is imperative for the successful integration of biometric solutions into everyday applications. This presentation will address ways to overcome these barriers, including technological advancements and security protocols to safeguard biometrics, system design considerations for managing identity across different use cases in the user journey, the establishment of transparent policies, and proactive engagement with end-users.

Frances Zelazny
CEO, Anonybit

Agenda

Business Case and ROI for Passkeys

Building a cost-benefit analysis for passwordless solutions

Switching to a new identity technology has its challenges, apart from retrofitting sea of known use cases for conducting business as usual, there are risks related to technology feasibility, viability, usability and external threats from bad actors. This talk will help you build a case for passwordless. As a veteran and a practitioner in this space, you will be more confident to create the right financial metrics to be a champion for your organization or your customer to adopt a cutting-edge identity tech product or a service. Furthermore, as an Identity leader, you can now confidently make those build vs buy decisions and have your own personal compass for adopting new technologies in Identity and Access Management.

Rohit Nayak
Director of Product, Scrut

Creating a Compelling Business Case & Organizational buy-in for a "Passwordless Customer Experience"

"Why and How to transition to a passwordless organization" is a pivotal milestone in an enterprise's digital transformation journey. It encompasses a bigger shift in the mindset - embracing new security measures and shift in user behavior with focus a seamless customer experience. Technology is the enabler but focusing on user experience and being agile in adapting and learning is the key to success.

Ruchira Ghosh
Head of Enterprise Customer Authentication (CIAM), TD Bank

How to make your Security Team your best Engineering Partner

This session explores how security and engineering teams, often driven by different goals, can collaborate effectively. It addresses the friction caused by their differing focuses - innovation versus security - and offers strategies for aligning their objectives. Attendees will learn how to transform these teams into collaborative forces that enhance each other's work, promoting a culture of cooperation rather than opposition.

Aviad Mizrachi
CTO, Frontegg

How to win the four boss battles of your passkey product development quest

There are four product risks to tackle, or four boss battles to win, to triumph in any product development quest: value risk, usability risk, feasibility risk, and business viability risk. Our adventurer party, or product development team, battled each of these risks in our quest to implement passkey support as a credential provider. In this session, we'll apply our lessons learned to help relying parties emerge victorious from their own quests, and unlock the achievement of better security and convenience for customers thanks to passkey support.

Ting Zhuo
Lead Product Manager, Dashlane

Jumping Into the Deep End: Best practices for phased passkey rollouts

The majority of early passkey adopters over the last year have been large consumer brands. However, every major rollout of passkeys has varied widely, and there's been minimal strategic guidance for those implementing passkeys to know with enough certainty what will work best for their user base and support their larger business goals. Anna Pobletts, Head of Passwordless at 1Password, will provide the audience with strategic guidance on how to choose and execute a passkey rollout strategy that positively impacts business goals. She will leverage research, customer feedback, and firsthand observations on how to best rollout passkeys, measure their efficacy, and more in her discussion.

Anna Pobletts
Director of Engineering, Identity, 1Password

Agenda

IAM Fundamentals

Four Components of Modern Identity

There is change in the air; people are willing to consider new solutions and new architectures. What follows is a reframing of the enterprise identity space, one not based on “”classical”” market definitions, instead one based on capabilities. Join this session to learn about the four major components to new world of identity:Policy; Orchestration; Execution and Data.

Ian Glazer
Founder and President, Weave Identity

Harnessing Passkeys in the Battle Against AI-Powered Cyber Threats

In ‘Harnessing Passkeys in the Battle Against AI-Powered Cyber Threats,’ we shine a spotlight on the pivotal role of passkeys at the early stages of the authentication kill chain, setting the stage for a preemptive defense against AI-driven cyber attacks. This talk delves into how passkeys, when implemented at critical junctures of the kill chain, can effectively derail cyber threats before they gain momentum. By dissecting the mechanics of passkeys within these initial phases, we illuminate their capacity to disrupt the sophisticated tactics employed by AI adversaries, thereby neutralizing potential breaches early on. Attendees will emerge with a deep understanding of how to strategically integrate passkeys into their security arsenals, fortifying their cyber defenses against the ever-evolving challenge of AI-powered threats.

Ryan Rowcliffe
Field CTO, HYPR

Navigating the Identity Security Road with Confidence

As most enterprises continue their journey into bringing the best digital experiences to their customers, security remains a top priority. Security in the Enterprise is at a point where Identity is at the “Center of Everything”, which means not only do we get it, but the bad guys understand it also. IAM infrastructure is the new “keys to the kingdom” and its simply not enough that strong authentication services are in place. Awareness of the sophistication of identity-based threats and how to address them is needed. With new breaches happening almost weekly, Identity Threat Detection and Response (ITDR) is an attempt to formalize a discipline around protecting identity assets in the enterprise. This session will dive into the key decisions that should be addressed when implementing a foundation of Identity Threat Detection. Additionally, we’ll review key architectural considerations and guidance for implementing these critical detect and response controls. With a key principle of Zero Trust being “Assume Breach”, we’ll review proactive measures that can be taken for protecting human and non-human identities across the enterprise. While our focus will be on B2C architectures, there will be plenty of valuable guidance for B2B/B2E identity practitioners as well.

Andrew Cameron
Technical Fellow, General Motors

IAM Stacks Under Attack! Why Authentication is Key to Cyber-Resiliency

Last year’s MGM breach demonstrated that identities and IAM infrastructure are under attack. We have crossed the chasm, identity is no longer productivity-centric, because identity is the new attack surface. Gartner predicted this a few years back, and now we are seeing IAM vulnerabilities become weaponized. Identities themselves, protocols, cloud infrastructure, or IAM vendors directly are all vulnerable. IAM must fuse with cybersecurity and fraud prevention to become threat aware and cyber-resilient. In this presentation we define cyber-resiliency for IAM and the critical role of authentication in this much needed evolution.

David Mahdi
Transmit Security

Simon Moffat
Cyberhut

Agenda

UX Fundamentals

Best Practices for Designing Passkey User Experiences on Mobile Devices

This presentation explores the best practices for designing seamless and intuitive passkey experiences specifically tailored for mobile devices. Attendees will gain insights into the unique challenges and opportunities presented by mobile platforms, learning how to optimize passkey flows for smaller screens, interactions, and diverse user contexts.

Yunji Ha
UX designer, Google

Passkeys on Windows: Paving the Way to a Frictionless Future!

Discover the future of passkey authentication on Windows. Explore our enhanced UX, powered by Microsoft AI and designed for seamless experiences across platforms. Join us as we pave the way towards a passwordless world.

Sushma K.
Principal Program Manager, Microsoft

Ritesh Kumar
Software Engineer, Microsoft

The 2F's of passwordless journey

The presenters Sarit Arora and Lovlesh Chhabra have a combined 10 years of experience building and growing passwordless solutions across consumer and enterprise offerings. In our experience across User experience design and Product, there are two Fs in a users' passwordless journey - Friction and Fear and sometimes it's both. Optimising on security leads to lower usability and more friction for the user in passwordless authentication scenarios. Many times products are built for tech savvy users and then it's hard for the average user on the internet to use these solutions. On the other hand reducing friction can lead to fear and anxiety among the users as the process feels like something that is too simple or too easy and the users do not understand how that can be secure. What's the optimum way to design a product experience that balances security and usability? In this talk we will explore the best practices that result in reducing friction and fear both in passwordless authentication. We will focus our talk around the following 6 powers: Power of Why - Context Power of Trust Power of Pause Power of Micro Interactions Power of owning the responsibility of security Power of optionality / choice.

Sarit Arora
User Experience Design Leader, Oracle Corp

Lovlesh Chhabra
Director of Product, Meta Platforms

What UX guidelines to ensure user convenience and ultimately reduce the abandonment rate?

"Design is the silent ambassador of your brand." - Paul Rand. How to ensure you have the best ambassador of your brand? It is key to provide the best-in class solution. What could be the UX guidelines for my product and my customer to locate and solve any unnecessary friction points? How to ensure compliance with regulation and alignment with practices? How to integrate a continuous UX evaluation on your product? In this talk we will cover: 1.What UX guidelines to implement for my product? 2.What are the main accessibility regulation roadmaps? 3.How to integrate continuous UX testing?

Jean DI MANNO
Architect – expert digital payment and authentication, Fime

authenticate 2024
THE FIDO CONFERENCE

Agenda

IDV Fundamentals

Identity Verification Compliance around the World

The global web of compliance requirements for Remote Identity Verification is growing. What used to be a simple document or liveness assessment now encompasses many trust, fraud and identity signals. In this session we review how to build the best performing verification experience for your customers that also meets the requirements for entering into the largest markets in the world.

Christopher Cortes
Product Manager, Onfido

Private organization and government perspectives in navigating the technological landscape of remote digital identity proofing

Remote identity proofing has become paramount for secure transactions and interactions with private entities or public government agencies. This panel discussion delves into the recent advances and the key technological considerations, with panelists representing various perspectives from both the public and private sectors. From robust document verification and biometric authentication to navigating digital ID standards and ensuring compliance with evolving regulations, our diverse panel will explore the intricate balance between security and user experience. The discussion will also spotlight innovation such as the rollout of mobile driver's licenses and the role of FIDO passkey in shaping the future of remote identity proofing.

Paul Grassi
Principal, Amazon

Teresa Wu
Vice President, Smart Credentials, IDEMIA

Passkeys 101: Technical Principles of FIDO

Hear a deep dive on passkeys, including what they are, how they work, why the FIDO Alliance has introduced them, and how you should be thinking about them in your authentication strategy

David Turner
Sr. Technical Director, FIDO Alliance

Passkeys for Consumers

Deployment Case Study: Tailoring Passkey Journeys for Different Users

Over the past two years, passkey adoption has been gaining ground for applications of all sizes. While the end goal of better UX and security is clear, the journey to get there differs based on the app's industry, existing user base, and several other factors.In this session, Descope Co-Founder Meir Wahnon will go through a deployment case study of a fast-growing InsurTech startup to share: Tips to run a passkeys pilot. How to customize the passkeys experience for different end user segments. Implementation do's and dont's. Join this session to learn from the high-points and challenges of a real-life passkey implementation project.

Meir Wahnon
Co-Founder, Descope

Agenda

Passkeys for Consumers

Future-Proofing Authentication: From Biometric Logins to Passkeys with WebAuthn

Chime is dedicated to providing our members with seamless access to their accounts, striving to minimize friction in the authentication process. Our commitment to this goal led us to explore passwordless authentication options, ultimately guiding us toward the adoption of biometric login as a secure and efficient solution. We made the decision to align with WebAuthn standards for biometric authentication, to not only enhance security but also lay the groundwork for the future implementation of passkeys. This strategic decision significantly reduced development time for passkeys and facilitated the adaptation of passwordless logins across various teams, including Product, Risk Analytics, and Data Science.

Nimit Shah
Senior Software Engineer, Chime Financial

Guarding the Gate: Strategies for High Security with Passkeys

In the ever-evolving landscape of cybersecurity threats, the necessity for authentication mechanisms that can withstand current threats while remaining adaptable has become paramount. The emergence of passkeys as a contemporary framework for authentication introduces a paradigm shift in how organizations secure their sensitive information. However, the adoption of passkeys is often met with a degree of confusion regarding their advantages and potential drawbacks. This talk aims to demystify the benefits of passkeys in high security markets by providing an exploration of their transformative potential.

Rolf Lindemann
VP Products, Nok Nok

Navigating Passkey Adoption Challenges - Mercari's Journey to Effectively Mitigate Phishing Risks

Mercari, inc. offers C2C marketplace, financial, and cryptocurrency services. We have been struggling significantly with phishing attacks. We mitigated the situation by introducing additional authentication for critical functions. However, this led to a decline in user experience and increased SMS authentication costs. Even with these disadvantages, phishing attacks remain a potential threat. To address these issues, we decided to adopt passkeys. This presentation will introduce the integration of passkeys as a countermeasure against phishing attacks. Fundamentally, to take advantage of the phishing resistance of passkeys in a service, we have to enforce the use of passkeys. However, strongly encouraging the use of passkeys does not always yield positive results due to the characteristics of the service and the users' awareness. This presentation will discuss how passkeys are generally introduced as an anti-phishing measure and the specific strategies Mercari's adoption. To capitalize on these countermeasures, it is essential to increase the number of registered passkey users in the service. By increasing the number of users protected by passkeys against phishing attacks, the overall service can reduce the damage received from phishing. Additionally, this can indirectly improve user experience. This presentation will explain the measures Mercari has taken to increase the number of registered users, as well as the effects of these measures.

Tatsuya Karino
Software Engineer, Mercari, inc.

Kotaro Oi
Product Manager, Mercari

Passkeys deployment at scale - our journey and best practices

This talk shares eBay's experience deploying FIDO-based passkey authentication across all its platforms. We discuss the implemented options, challenges encountered, and best practices followed for a large-scale rollout. We'll explore how our strategy evolved, benefiting millions of users globally. The talk aims to provide valuable insights for organizations considering passwordless authentication at scale.

Mahendar Madhavan
Product Lead, eBay

Agenda

Passkeys for Consumers

Passkeys on Google platforms: updates on latest features and real-world successes

In this talk, we will share updates on the latest features supported by Google platforms (Android & Chrome) regarding passkeys. We'll also share real-world examples of the impact that passkeys are creating.

Diego Zavala
Product Manager, Google

Passwordless Authentication at eBay

eBay has deployed FIDO based passwordless authentication mechanisms across all its sites. In this talk, I will go over various options implemented, challenges we faced and best practices we followed to deploy at scale. From biometric authentication on mobile apps to latest adoption of Passkeys, we will look at how our strategy has evolved benefitting millions of users globally. This talk aims at sharing our journey and experiences which one can leverage to effectively deploy simple and strong authentication at scale.

Anand Bahety
Software Engineering Manager, eBay

Real-World Passkey Implementation for financial institutions - Insights & Results

As the momentum around passkeys continues to build, this session highlights a success story from the Financial Services Market. Through it, we will present some key considerations for the deployment of passkeys, as well as insights and results from this customer passkey deployment project which enables passwordless login to digital banking services for millions of users in LATAM. This session structured as a fire chat intends to explore the thought process, the considerations and evolution of a nationwide latin american identity provider for financial institutions backed by some of the largest financial institutions in the country representing close to 80% of the market.

Pedro Martinez
Business Owner Authentication, Thales

Risk mitigation in the identity stack: Bringing FIDO passwordless innovation into regulated financial industry

Learn from the trenches real-world examples of bringing FIDO passwordless innovation into a large, regulated financial institution. Hear from Bill Wright, who served as Executive Director of USAA Bank and on the FIDO Alliance, and from Dr. Tina Srivastava, MIT Lecturer on Technology Roadmapping and Co-Founder of Badge, a leading passkey provider with authentication technology based on quantum-resistant cryptography. This talk will focus on risk mitigation in the identity stack, leveraging insights from real-world deployments in regulated industries. These insights will guide how to think systemically about risk and user friction. Do not reflexively add more factors to multi-factor authentication (MFA) – that is not security, instead focus on SMART MFA and phishing resistance. Building off Bill Wright's decades experience as a practitioner delivering global scale information security and identity, as well as his long-time service at FIDO in developing standards and integrations, Bill and Tina will share practical insights on how to action the best FIDO has to offer while also balancing the need for easy, flexible user experience. At some point, added friction actually decreases security, so it is necessary to be practical about finding the most efficient ways to reduce risk and improve security posture. This talk will also cover common architectural challenges to adopting passwordless authentication and how to overcome them. The talk will conclude with how to deal with the "long tail" of legacy applications: Don't let perfect be the enemy of good, and do not let legacy apps become attack vectors.

Tina Srivastava
Lecturer & Co-Founder, MIT & Badge Inc.

Bill Wright
Former Executive Director of USAA Bank

Agenda

Passkeys for Consumers

Step-by-step procedure and considerations for Passkey deployment

Various services have implemented passkeys, and there may be many people who want to implement passkeys. In this session, I will explain where to start when implementing passkeys, and what to consider during each phase from planning to implementation and operation.

Keiko Itakura
Head of Security, Medley

What I wish I knew about passkeys content design before I started this adventure

It's not easy explaining the inner-workings of passkeys to the average person. And it can be even harder to persuade them to let go of their precious passwords. Get a behind-the-scenes look at the tools and resources I used to make Intuit's passkeys content easy for my customers (and me!) to understand.

Elizabeth Beasley
Senior Content Designer, Intuit

Passkeys in the Enterprise

A journey of passwordless authentication on shared mobile devices

In this presentation, I'll discuss our journey in creating a passwordless authentication experience tailored for front-line workers, who commonly share their mobile devices for work purposes. I'll highlight the specific challenges we encountered when adopting biometric authentication for shared devices and offer insights and suggestions on simplifying the adoption of passwordless authentication for enterprises.

Xun Chen
Director of Engineering, Samsung Research America

Balancing enhanced security with excellent user experience in the enterprise

As the threat of sophisticated attacks like phishing continue to rise, enterprise users and cybersecurity teams are seeking solutions that offer robust security, reliable authentication and user-friendly functionality. With the increasing adoption of biometric logins, enterprises aim to marry strong security with user convenience to reduce friction, boost productivity and job satisfaction. A major trend among enterprises is the adoption of hardware security keys that leverage biometrics and provide portable, seamless functionality – all while providing the highest level of authentication by facilitating passwordless login through biometrics. This session focues on enhancing security for organizations and reducing friction of security adoption for the employee. This session will detail the proven impact of solutions like biometric-backed security keys on phishing attacks and highlight key use cases and real world examples. Attendees will walk away being empowered with the tools and knowledge to enhance their cybersecurity posture, amplify operational efficiencies and increase adoption of security tactics by removing roadblocks.

Ludwig Ward
Hardware Product Manager, Yubico

Beyond Passwords: A Journey to Seamless Authentication for Enterprise Software

In this session, we'll explore overcoming the challenges of introducing passwordless login in large enterprises. We'll share our journey, highlighting how it not only increased customer satisfaction and lowered password reset support costs but also paved the way for innovative solutions. Discover the post-implementation benefits as we showcase how DocuSign utilized passwordless login to introduce ID Wallet, meeting EU regulations. Additionally, we phased out outdated identity recovery methods like Security Question Security Answer. Join us for insights into the transformative impact of passwordless login on security, compliance, and identity management.

Sarah Zou
Lead Product Manager, DocuSign

Agenda

Passkeys in the Enterprise

Borderline : Examining the edge cases of FIDO

We all have those borderline edge cases - the ones that fall through the cracks and jeopardize even the best laid plans to go passwordless with FIDO. FIDO is amazing technology as it can keep you and your organization safe, secure, and reduce user friction and frustration. However, edge cases can make or break the best of FIDO implementations. Things like non-federated applications, legacy ERP systems,IoT, and (do we dare mention?) kiosks and shared workstations, can all get in the way of a successful FIDO deployment. During this session we'll examine some common edge cases and provide strategies for tackling these hard cases to pull your passwordless implementation back from the borderline.

Karen Larson
Senior Director of Product Management, Uniken

Bringing Passkeys into your Passwordless Journey

Most of our customers are either deploying some form of passwordless credential or are planning to in the next few years, however, the industry is all abuzz with excitement about passkeys. What are passkeys and what do they mean for your organization's passwordless journey? Join the Microsoft Entra product team as we walk you through the background of where passkeys came from, their impact on the passwordles ecosystem and the product features and roadmap bringing passkeys into the Microsoft Entra passwordless portfolio and phishing resistant strategy.

Jarred Boone
Identity Security Product Marketing Manager, Microsoft

Enterprise passkey deployment updates and learnings from Passkey managers

FIDO2/WebAuthn/Passkey has been protecting a large portion of employees of Alibaba Group for over two years. A colleague from our operations team will update the user stories, user incremental curve, and coverage data since the last Authenticate Con. Plus, we'll run some math on how much money passkey saved. Next, we'll share two tech approaches to sync credentials among multiple browsers limited inside one mac. Why? Out of data security, an employee is restricted to access only one computer. First, we come up with a creative and very cheap way to relay the authenticate process to passkey authenticators via a single browser inside (Electron-based) security agent, to delegate passkey authentication for unsupported browsers, in an OAUTH fashion. Unfortunately it will some sort of compromise the anti-phishing capability from passkey. This could be fixed, and we'll discuss how. Then we look into password managers (or passkey managers) which have been quite successful on this scenario. We evaluate the 'monkey-patch' technique used by serveral password managers, and discuss how it can help.

Wang Kang
Staff Engineer, Alibaba Group

Xin Ma
Senior Staff Engineer, Alibaba Cloud

Houjun Xu
Product Manager, Alibaba Group

Zhen Zeng
Staff Engineer, Alibaba Group

From Consumer Convenience to Enterprise Security: Demystifying Passkeys in the Workforce

This session explores the challenges of adopting passkeys (a consumer login method) for strong enterprise security. It covers integrating passkeys with existing systems, managing them within the organization, and deploying them for various applications (including offline ones). Finally, it presents a case study of one of our customer experiences transitioning to passkeys.

Allen Storey
Chief Product Officer, Intercede Ltd

Agenda

Passkeys in the Enterprise

Lessons from Passwordless rollout

Identity is the new perimeter and passwords are the Achilles heal of Access Security. MFA on top of passwords is a bandaid and is an intermediate step until we get rid of passwords which are inherently a weak form of authentication. We recently rolled out phishing resistant MFA (number matching, mandatory touch/face id for MFA mobile apps) in FY23. In FY24, we wanted to improve end user experience as well as security. These are usually contrary goals. However, Passwordless provides a rare opportunity to significantly improve both simultaneously. Hence, we decided to roll out Passwordless using a phased approach. In this session, we will discuss all the learnings from our password less rollout.

Amandeep Nagra
Director, Authentication and Zero Trust, Kenvue

Navigating the implementation and roll out of passwordless authentication within the workforce environment

This session will cover the challenges and the learning of Swiss Marketplace Group, a group of 15 brands (marketplaces which serve the majority of the Swiss population), to FIDO passwordless authentication for its workforce. In this session, we will go over our experience from the existing state analysis, the new passwordless authentication concept, ideation, its fitting to a risk-based approach to authentication, the implementation, the testing, the pilot group, etc. We will share our challenges and learnings from the internal dependencies to vendor rollouts that broke our implementations. The session will cover what has been done so far, where we stand and our future plans and vision.

Mikel Grabocka
Security Architect, Identity and TrustSMG Swiss Marketplace Group AG

Passkey Authentication for IBM Employees

Learn from IBM's experience of deploying passkey authentication for worldwide employee intranet access. Business and technical requirements, challenges and lessons learned will be shared in this engaging session from two of IBM's technical leaders. Attendees will leave with a thorough understanding of key considerations for passkey deployment in the enterprise.

Chris Dotson
Engineer and Executive Security Architect, IBM

Shane Weeden
Senior Technical Staff Member, IBM

Passkeys: A Breakthrough Step for Workforce Authentication on Shared Computer

Industries relying on shared computers, such as healthcare, hospitality, manufacturing, and call centers, encounter significant challenges in workforce authentication. Frontline, blue-collar, and factory workers, often not tech-savvy, face difficulty managing complex passwords and frequent changes. Time efficiency for the login process is critical in these sectors and leads to sacrificing security for productivity. Using generic accounts is a common workaround and will make workforce authentication more complex. Passkeys emerge as a secure and phishing-resistant solution, eliminating the need for a username and password, helping with frictionless authentication and enhancing login speed. Plus, synced passkeys will address the issue of generic accounts on shared computers. We will review a success story of passwordless authentication development for a manufacturing plant with 100 computers and 120 workers and considerations.

Bahram Piri
CEO, IDmelon

Agenda

Passkeys in the Enterprise

Securing the Enterprise: How to use Passkeys/WebAuthn to become phishing resistant today and how to enable Zero Trust tomorrow

As we mark the two-year anniversary of passkeys, the landscape of enterprise authentication continues to evolve with both challenges and opportunities. While some enterprises have made significant strides in adopting full phishing-resistance, many are still in the nascent stages of implementation. After starting why enterprises need to start adoption now, we will also cover some of the challenges that persist today, including phishing-resistant onboarding and recovery processes, navigating remote use cases, and establishing control over key provenance. Fragmentation across platforms remains a significant hurdle, leading to disparate user experiences and management complexities. And despite the attention Zero Trust frameworks have garnered, their full enablement through FIDO remains elusive, leaving enterprises largely responsible for crafting their own strategies. Looking ahead, the emergence of enterprise-grade software authenticators and managed passkey providers presents a promising avenue for streamlined authentication solutions. The integration of Zero Trust principles, particularly device posture, with evolving authenticator technologies suggests a convergence that could enhance security measures. Moreover, the potential for continuous authentication, facilitated by context via WebAuthn and frameworks like the Shared Signals Framework (SSF), offers opportunities for advanced security protocols such as Continuous Authentication Endpoint Posture (CAEP) and Risk and Incident Sharing and Coordination (RISC). As the identity landscape evolves, collaboration and innovation will be critical in addressing emerging challenges and maximizing the potential of authentication technologies.

Johannes Stockmann
Sr. Software Architect, Okta

Simplify enterprise adoption of passkeys: Best practices for implementation

Passkeys, touted as the next evolution in FIDO authentication, present a robust solution for enterprise authentication, delivering heightened security, convenience, and efficiency. But organizations are still confused on how to best implement them. Join Gregory Vigroux Product Line Manager from Thales to glean valuable insights and practical tips for successful passkey deployment, empowering your enterprise to fortify security measures and effectively meet regulatory standards.

Gregory Vigroux
Product Line Manager, Thales

The [pass] keys to success of FIDO2 Enterprise Adoption

The enterprise realm of FIDO2 is still relatively unchartered, but TikTok has been working on building out infrastructure and policies to make FIDO2 the primary method of authentication for employees. From developing a FIDO2 registration platform for onboarding new users, to creating migration paths from “traditional” 2FA methods & developing policies for enforcing FIDO2 during login, come listen to TikTok’s FIDO2 rollout journey to make the company phishing resistant (and learn how you can roll out FIDO2 as well!)

Sydney Ng
FIDO2 Engineer, TikTok

Workforce FIDO2 Orchestration - Lessons Learned From Millions of Issued Credentials

After working on extensive large and small credential rollout projects for the enterprise, Versasec has gathered a practical list of practices and strategies that can help any organization, industry, and technical or non-technical team to safeguard their most valuable assets, their identities. Get ready to step up your identity management for your organization! What can you expect from this session? Security best practices to ensure enterprise management of FIDO authenticators and its processes. Enhance FIDO’s enterprise security by applying valuable lessons from our PKI deployments. Leveraging these insights, we can fortify identity and access management plans, ensuring heightened protection for your enterprise.By implementing these lessons, you not only bolster FIDO’s security but also pave the way for a more resilient and comprehensive security strategy tailored to the dynamic challenges of today’s digital landscape. We look forward to meeting you and also learning from you!

William Houry
VP Sales, Versasec

Agenda

Passkeys, Government & Policy

A Shared Services Model to Promote Rapid Adoption of FIDO2 Within Federal Government!

This session will focus on the architecture, operations and benefits of a FIDO2 shared services model for federal government enterprise users. We will discuss the development of progressive iterations (for over a year) of the architecture and design options for a government-wide shared services model for issuance and lifecycle management of Derived FIDO2 Credentials (DFC).

Sarbari Gupta
Founder and CEO Electrosoft Services, Inc.

FIDO Alliance Support to US Government Deployment

In 2023, at the US Government's request, the FIDO Alliance established an effort to support the US Government's adoption of FIDO. During its first year, this effort has released a technical guidance paper and opened a dialogue with stakeholders. This session will provide an update on US Government deployment and a snapshot of ongoing work in the now-enduring USGDWG.

Tom Clancy
Engineer, MITRE

Joe Scalone
Senior Solutions Architect, Yubico

Teresa Wu
Vice President, Smart Credentials, IDEMIA

Passkeys for the public - How Login.gov implemented passkeys as an MFA method to make federal services easier and more secure to access

Login.gov is a secure sign in service used by the public to sign in to participating government agencies. Participating agencies ask users to create a Login.gov account to securely access information on their website or application. All accounts require some form of multi-factor-authentication (MFA), and Login is constantly exploring new options that are both secure and easy to use. Allison will discuss challenges and lessons learned that the Login.gov team faced in a new MFA capability recently launched: passkeys as an MFA method. Challenges that will be discussed include: accessing passkeys across devices and operating systems; ensuring that as many users as possible will be successful with passkeys; and understanding what's not working for users. The session will include an interactive component where attendees can also share insights from their experience with those challenges with the rest of the group.

Allison Rosenberg
Product Manager, GSA

Passwordless Authentication in the Regulatory MFA Landscape

This session explores the integration of passwordless methods into the existing Multi-Factor Authentication (MFA) frameworks mandated in the EU, UK, and US. It covers traditional MFA approaches, such as SMS OTPs and voice/email authentication, and discusses the classification and implementation of passwordless authentication, including the role of FIDO biometrics and passkeys. The presentation aims to inform and initiate discussions on the future of secure authentication technologies in regulated sectors.

Tola Dalton
Senior Director, Identity Engineering eBay, Inc.

Privacy Risk Management Fall Update

Privacy preserving authentication has been a cornerstone of FIDO since its inception. As authentication, verification, laws, regulations, and guidance evolve, privacy plays an important role. Session attendees will learn about NIST Privacy Guidance such as the new Privacy Framework and an overview of the changes to privacy requirements in considerations in the upcoming Rev 4 of the NIST Digital Identity Guidelines.

Jamie Danker
Senior Director Privacy Services, Venable LLP

Agenda

Passkeys, Government & Policy

The tech behind main Brazilian`s Government Digital Transformation: from gov.br to PIX and e-invoices

Brazil's journey in transforming its public sector through digitalization is a testament to the power of innovative technology and strategic foresight. This presentation aims to provide an in-depth analysis of the key technologies driving this change, with a focus on the GOV.BR portal, the PIX payment system, and electronic invoicing, while emphasizing the instrumental role of Hardware Security Modules (HSM) and the compliance with FIDO 2.0 standards. GOV.BR and ICP-Brasil: A Model for Digital Governance GOV.BR, an integrated platform for government services, represents a monumental shift from traditional methods to a unified, digital approach. The aim is to provide a holistic view of Brazil's digital transformation, inspiring and guiding global audiences at Fido.org, especially those involved in digital governance, fintech, and cybersecurity. By sharing these insights, we hope to contribute to a more secure and interconnected digital future.

Marcelo Buz
Director, Dinamo Networks

Improving authentication policy enforcement for government resources

US Government enterprises are integrating security functions to realize Zero Trust capabilities on an ambitious timeline. Although phishing resistant authentication is a well-established foundation of typical agency roadmaps, supporting least privilege and context-based access are not as well defined within Federal Identity, Credential, and Access Management (FICAM). This session will survey government requirements and open standards to highlight alignment opportunities for industry-government that would benefit stakeholders the most.

Tom Clancy
Engineer, MITRE

Passkeys for Payments

Can we use passkeys to authenticate consumers in online card transactions

Can we use passkeys to authenticate consumers in online card transactions? Attend this session to learn about the role that passkeys can play in e-commerce payments to reduce friction when authenticating consumers purchasing goods and services as well as how passkeys can be used to address fraud concerns and cater to regulatory requirements.

Jonathan Grossar
Vice President, Product Management, Mastercard

Henna Kapur
Director, Product Management, Visa Inc.

Secure Payment Confirmation

The goal of the presentation is to update/inform participants on how SPC satisfies payment authentication use cases, provides strong authentication, reduces shopping cart abandonment and provides an enhanced customer experience. The presentation will be an opportunity to gain exposure to Secure Payments Confirmation (SPC), which should be on everyone's radar.

Douglas Fisher
Senior Director, Visa

Agenda

Passkeys for Payments

The Case Against Passwords: Biometric Authentication for SCA and the Pathway Forward

In a divided world, there's one thing that almost everyone can agree on: —passwords are the worst. The online payments space demands a move away from dependence on one-time passwords (OTP) for security to instead focus on the future of frictionless and active authentication using biometrics. Mastercard's vision for authentication unlocks the full potential of Strong Consumer Authentication (SCA) regardless of geography Janine Lafond & Qing Cao will walk attendees through Mastercard's vision, key learnings and best practices, and what's next in integrating FIDO standards into payment authentication.

Jonathan Grossar
Vice President, Product Management, Mastercard

Use of FIDO Authentication data in 3-D Secure Messages

The presentation will kick off by providing a high-level summary of the payment authentication eco system and the different parties involved today, including some payment authentication statistics globally, how it helps prevent fraud. It will then move on to how FIDO authentication can plug into this flow and authentication evidence can be sent securely to the Issuer for additional validation and approval as considered necessary in their market. Finally, there will be a mention of some further enhancements EMVCo is making in their specification to support FIDO authentication method (for example, updates to the protocol 2.3.1 and bridging extension)

Henna Kapur
Director, Product Management, Visa Inc.

Complementary Technologies & Standards

AuthZEN: Standards for modern authorization

Authentication standards, such as SAML and OIDC, have paved the way for an interoperable identity fabric that has propelled the industry forward. It's time for authorization to have its "OIDC moment." After all, authorization is the natural next step in identity-based security. Over the past few years, we've seen the rise of a new architectural pattern - externalizing authorization logic out of applications, and treating it as a separate concern. Join us to discuss the current state of modern authorization, and the progress we've made defining patterns, documenting use-cases, and reviewing the interoperability standards

Alexandre Babeanu
3Edges

Omri Gazitt
Co-founder & CEO, Aserto

David Brossard
CTO, Axiomatics

Atul Tulshibagwale
CTO, SGNL

Do Passkeys Solve the Account Recovery Problem?

You've built login for your application—and even added 2FA—but what happens when a customer upgrades their phone, loses their device, or otherwise gets locked out of their account? With an increasing number of consumer applications adopting Passkeys, account recovery is still an consideration. This session will show how to accommodate account recovery for passwordless solutions while minimizing account takeover and support overhead. I've tracked dozens of account recovery procedures to learn how everyone from utility companies to crypto startups attempt to re-verify identity when life happens. This talk will look at that research and outline best practices you can use depending on your industry and customer risk profile. Since phone support is commonly used for account recovery, we'll highlight how to build guardrails for your call center agents to minimize costs and delight customers. You'll leave understanding the trade-offs of mechanisms for account recovery (like government ID verification, forced waiting periods, security questions) and debating the value of recovery tokens.

Kelley Robinson
Developer Advocate, Identity & Authentication, Twilio

Agenda

Complementary Technologies & Standards

No browser, no password, no problem

What if you could run OAuth and OpenID Connect flows natively in mobile apps without involving a browser? And what if this approach could also leverage passkeys natively so the user could go fully passwordless? It's all possible using a Hypermedia Authentication API (HAAPI) that takes care of logging in the user and provides app developers full control of the UI and UX. In this talk Jonas Iggbom will present the underlying technology of a Hypermedia API that acts as a state machine to facilitate user login and demo the end user experience.

Jonas Iggbom
Director of Sales Engineering, Curity

Prevent Catastrophe When Authentication Goes Wrong

The real question is, not "IF an identity is compromised", but "WHEN...". You are trying to rapidly transition to a phishing-resistant strong authentication, but in the meantime, what can you do so that an authentication compromise doesn't enable an attacker to steal your crown jewels? Even after you have deployed strong authentication, you may still be faced with malicious insiders or session hijacking attacks, which leaves your enterprise vulnerable. Compromising identities has become lucrative to attackers because it almost always enables them broad access to critical organizational systems and data. A critical cause of this is the standing privileges and the permissive environment that most enterprises operate in. One cannot have an identity perimeter if users have broad access. Standing access permissions collected over time as employees move through various job functions contribute to a permissions sprawl that is hard to review and restrict. Join this session and walk away with practical steps that you and your organization can take today to prevent catastrophe. And maybe more importantly, what not to do.

Atul Tulshibagwale
CTO, SGNL

We know who you are, now...what can you do? Expanding beyond authentication with emerging authorization standards.

Securely authenticating is the first fundamental step in a user's digital journey. However, once we know who you are, we need to determine what it is you can or cannot do. And we need to keep track of what you did. This is what authorization aims to solve. Historically, IAM practitioners have leveraged authentication frameworks to achieve some degree of identity-centric, coarse-grained authorization but this is no longer sufficient. Fortunately, there are a slew of new emerging patterns and standards that aim to solve the authorization conundrum. From OAuth's Rich Authorization Requests RFC9396 to OpenID's latest WG, AuthZEN, this presentation will aim to give the attendee a good understanding of current options, implications on current architecture, and means to bridge authentication and authorization. We will discuss ABAC, ReBAC, and Graph-based authorization as well as AuthZEN's aim to provide a standardized approach to delivering runtime authorization decisions.

David Brossard
CTO, Axiomatics

Reusable Identity for Improved Passkey Compliance

This presentation explores the integration of passkeys with decentralized identity standards as a solution to enhance security and streamline identity verification in regulated industries. Traditional passkeys, while offering improved security and phishing resistance, often fall short in industries requiring stringent identity proofing, such as healthcare. We discuss the limitations of current identity proofing methods, such as knowledge-based authentication and selfie+picture ID checks, which add friction and hinder onboarding success. By adopting a "reusable identity" model that ties passkeys to a user's digital identity through a decentralized framework, we aim to reduce onboarding friction and meet regulatory compliance more efficiently. The presentation will cover proof-of-concept work, the necessity for a governance and interoperability framework, and real-world applications in compliance-driven sectors, providing insights into enhancing passkey effectiveness and user identity verification processes.

Abbie Barbir
Advisor, CVS

Rolf Lindemann
VP Products, Nok Nok

Agenda

Complementary Technologies & Standards

Safeguarding Your Business Against OTP Frauds and Scams – Authentication Strategies to Protect Your Customers and Your Brand from Sophisticated Attacks

Businesses favor using one-time passcodes (OTPs) because they are accessible to a large portion of the customer base and easy to use, but unfortunately vulnerable to attack. SIM swaps and other mobile fraud are on the rise. Social engineering scams that dupe victims into revealing their OTPs are increasing in popularity. 60% of respondents to a recent TransUnion survey expressed concern about OTPs being intercepted by fraudsters for account takeover. What can businesses do to prevent fraudsters from spoofing their phone number to impersonate them on outbound calls to consumers? How can they ensure OTPs used to authenticate are safely going to legitimate customers and not to criminals? Join this session to discover how fraudsters successfully intercept OTPs and how phone intelligence mitigates this attack vector. Attendees will also learn other common fraud tactics and scams frequently used to victimize consumers.

Leslie Deniken
Director, Product Marketing Global Fraud Solutions, TransUnion

The Power of Combining Identity Wallets and Passkeys

Are identity wallets in competition with passkeys? Absolutely not! In the rapidly evolving landscape of digital authentication, the role of identity wallets and verified credentials is often misunderstood. Contrary to the belief that they compete with passkeys, mobile documents serve a complementary function by providing verified attributes to a user's digital identity.

This session will delve into the synergy between verifiable credentials and mobile documents, emphasizing the necessity of coupling them with passkey phishing-resistant authenticators. Attendees will gain insights into creating a seamless, secure, and privacy-preserving authentication experience by integrating these technologies. Join us to explore how this integration can enhance security protocols and drive the next wave of passwordless authentication solutions.

Christine Owen
Field CTO, 1Kosmos

Vision and Future

All the Things PQ -- End-to-End PQ-Secure Fido2 Protocol

While being a niche research topic only few experts were focusing on two decades ago, the development of cryptographic solutions that are secure even in the presence of quantum computers has been recognized as being necessary to ensure Internet security in the future by research, industry and government bodies. In particular, addressing the impact of the quantum threat has been the topic of the FIDO Alliance's recent white paper. Indeed, due to its wide usage also in high-risk security environments, the FIDO2 protocol is a key example (pun intended) of a protocol that urgently needs to be migrated to be post-quantum secure. In this presentation we will describe the first two steps we have recently been taken on the road to a quantum-resistant FIDO2 protocol.

Nina Bindel
Staff Research Scientist, SandboxAQ

Agenda

Vision and Future

"Verify but trust?" - Confidential Computing and the future of passkey synchronization

The FIDO Alliance, and especially the synced passkey fabric, is revolutionising authentication by joining the state of a user's physical device to all their many registrations. Instead of trusting that a user's knowledge shared secret proves who they are, synced passkeys allow a user to prove they are in control of a trusted endpoint. As passkey synchronisation fast becomes the norm, both between devices and across passkey managers, the need for cryptographically strong security and confidentiality across domains becomes paramount. This panel will discuss how Confidential Computing enables a new world of trust and security for cryptographic secret management, including passkey synchronization.

Mike Bursell
Executive Director, Confidential Computing Consortium

Manu Fontaine
Founder & CEO, Hushmesh Inc.

Stephen Wilson
Principal Consultant, Lockstep Consulting

Detecting Compromise of Synced Passkeys

FIDO2 represents a significant step forward in user authentication, aiming to replace traditional password authentication with increased security while remaining user-friendly. Despite its advantages, FIDO2's widespread adoption faces obstacles, particularly in terms of private key management and account recovery in the event of an authenticator loss, theft, or failure. While synced passkeys appear to be a viable solution for account recovery and cross-device authentication, the move to centralized passkey management offered by passkey providers introduces new security vulnerabilities. In this talk, we will present a novel framework for detecting passkey compromise at passkey providers while balancing security and usability in account recovery. This framework is compatible with current passkey syncing and management implementations and designs, requiring only minor changes to the existing FIDO2 authentication process.

Coby Wang
Staff Research Scientist, Visa

From Passkeys to Cloud Wallets and Beyond. A global synchronization fabric for verifiable data.

Over time, the locus of critical computing, including cryptography, swings from client to cloud and back again. In one era, we prefer to keep our important data and operations close; in the next, we are happy to let specialist providers do the hard work. Mobile digital wallets are likely to fast become indispensable; at the same time, the scale and velocity of wallet usage is driving us to shift key management to the cloud. There are great tensions between security and utility. The same story has played out in the FIDO Alliance community with the evolution of passkeys. This presentation explores how Synchronised Passkeys have established a new technology and business pattern, and a potentially global cryptographic fabric.

Stephen Wilson
Principal Consultant, Lockstep Consulting

Passwordless zero-knowledge services

Password managers, a.k.a credential providers, have long been hailed for simplifying the management of passwords and passkeys. However they come with a caveat: the need for a strong "master password". This master password serves as a crucial element in encrypting personal data, acting as a symmetric cryptographic key known only to the user, granting access to the stored information. Yet, no matter how complex a master password is, it is still a knowledge factor and comes with the inherent flaws of traditional passwords - flaws we're all too familiar with. In this session we'll look at the role the "master password" plays for zero-knowledge services that encrypt user data and how we can get rid of it so we can have a truly passwordless experience. We'll look at how to bootstrap new devices, use local device authentication and cover the challenges of account recovery, and all of this through the lens of a completely passwordless experience.

Rew Islam
Director of Product Engineering and Innovation, Dashlane

Agenda

Vision and Future

Solving the Final Roadblock to Passkeys: a Fractured Development Environment

The demand for passkeys is only accelerating, with Google, Apple and Microsoft spearheading a push towards passkey ubiquity. Moreover, the recent adoption surge by tech giants like Gmail, Robinhood, Coinbase, Shopify, and Amazon is a clear indicator of the impending shift in authentication paradigms. However, amidst this push lies a critical roadblock: a fractured development environment. In this session, Reed McGinley-Stempel CEO and co-founder of Stytch will delve into the evolving landscape of passkey adoption, focusing on the pivotal role of the developer experience. He'll discuss what it will look like for a developer building with passkeys in 2024 vs. 2023 and how the standards and ecosystem have evolved since last year. He'll also dive into the most common implementation challenges for developers, strategies for addressing these complex edge cases they need to build around, and what developers can look forward to as the tools and best practices evolve.

Reed McGinley-Stempel
CEO and Co-founder, Stytch

Stop Counting Factors... Start Describing Authentication Events

We began deploying multi-factor authentication because passwords provided insufficient security. More factors equals more security, right? Yes, but we continue to see authentication attacks such as credential stuffing and phishing! The identity industry needs to stop thinking in the quantity of authentication factors, and start thinking about the properties of the authentication event. As we transition into the era of passkeys, it is time to consider how we describe the properties of our authentication event. In this talk, we'll demonstrate how identity providers and relying parties can communicate a consistent, composable collection of authentication properties. To raise the security bar and provide accountability, these properties must communicate not only about the authentication event, but about the security primitives underlying the event itself. These properties can be used to drive authentication and authorization decisions in standalone and federated environments, enabling clear, consistent application of security controls.

Pamela Dingle
Director of Identity Standards, Microsoft

Dean H. Saxe
Principal Engineer, Office of the CTO, Beyond Identity

Unshackling Passkeys: Digital Strategies for Strong Identity Binding

Challenge: Document verification has, for a long time, been considered the "gold standard" for identity verification. This may remain true in the physical world (although that could be a hotly contested point), in the digital world there are too many challenges with document verification for it to be relied upon for a strong bind of an identity to a passkey. First of all, the means and methods of that verification are not inherently secure. Secondly, the user experience can be so difficult that even experienced users are likely to churn. How can that be addressed? Digital verification needs a digital-first approach. The history of the FIDO Alliance goes back to the original concept of using a piece of hardware to unlock digital experiences. The one piece of hardware that almost every user has is the mobile device. That is why the FIDO2 standard has started taking off. It's now possible for just about every user to securely authenticate without a password. That same principle applies to the initial identity verification as well.

Tim Brown
Global Identity Officer, Prove

Bill Fish
VP of Authentication, Prove

Agenda

Vision and Future

A FIDO web wallet for digital identity

Our work with digital identity, eID, in the EU has made it clear that hackers are not targeting the highly regulated HSMs in the backend. Instead, all the hacker action is in the front end, with sophisticated phishing attacks succeeding no matter the formal level of assurance of the eID. Still, there are no regulatory requirements to curb phishing. On the contrary, phishing-resistant solutions like passkeys are not allowed in our eIDAS-compliant systems because passkeys may be backed up. To illustrate the challenge, we will demonstrate a user-friendly and phishing-resistant web wallet, discuss wallet usability, and signing of Verifiable Credentials. Finally, while we point out that regulators may need a refresher on how fraud actually happens, we also suggest that FIDO should consider general encryption and signature capabilities as part of the core specifications. This would allow for building genuine digital wallets in the browser backed by trust modules in the platforms or external devices.

Niels Flensted-Jensen
Co-founder, CEO,Criipto

Web 3.0 Before It Was Cool: Why Decentralized Authentication is the Future and the Past

The benefits of a decentralized internet have long been touted and are well understood. With increased centralization over the past few decades the need for the internet to go back to it's decentralized roots are becoming more and more apparent. From high-profile attacks on centralized single sign-on (SSO) authentication services to accidental outages that result in wide-spread lockout. Systems with single points of failure are hitting a scalability wall. Sometimes the best way to go forward is to look in the rearview mirror. In this talk, I will explore the early days of the Internet where decentralization was the norm: folks shared their PGP keys at key sharing parties, bulletin boards and IRC servers ran in a fully-distributed fashion, and tracking and ads were relatively non-existent. Through this lens, I will paint a picture of a very realistic, and not-so-distance, future where privacy is the norm, authentication is simple and foolproof, and most of the cyber attacks that we know today are a thing of the past. Indeed, we already have all of the tools that we need. This is all possible with modern smartphones, protocols like FIDO and Verifiable Credentials, and a fully-decentralized identity and recovery ecosystem.

Chad Spensky
CEO, Allthenticate

 |