German/US Expert Meeting

IT Security Association Germany (TeleTrusT) in cooperation with FIDO Alliance

San Francisco, 25.03.2026

Securing the Account Lifecycle

Andrew Shikiar, CEO and Executive Director, FIDO Alliance

Diverse Membership / Global Perspectives

1Password, amazon, AMERICAN EXPRESS, Bank of America, CHASE, CISCO

CVSHealth, Daon, DASHLANE, DELL, egis Technology, FEITIAN WE BUILD SECURITY, Google

HYPR, IDEMIA, infineon, INTUIT, LastPass, Lenovo, LINEヤフー

mastercard, mercari, Meta, Microsoft, NTT docomo, OneSpan, okta

PayPal, PNCBANK, Prove, RAON, RSA, SAMSUNG, SK telecom

sto, swissbit®, THALES, TikTok, usbank, VISA, WELLS FARGO, yubico

+ Sponsor members | + Associate members | + Liaison members | + Government members

The FIDO Alliance model for success

Technical Specifications

Market Adoption Programs

Industry Certification Programs

Engaged, Committed Community

Account lifecycle risks

Account Lifecycle: Risks today

Account Enrollment & Identity Verification

- Knowledge-based authentication
- Synthetic IDs
- Fabricated biometrics
- Injection attacks
- Presentation attacks
- Biased face verification results

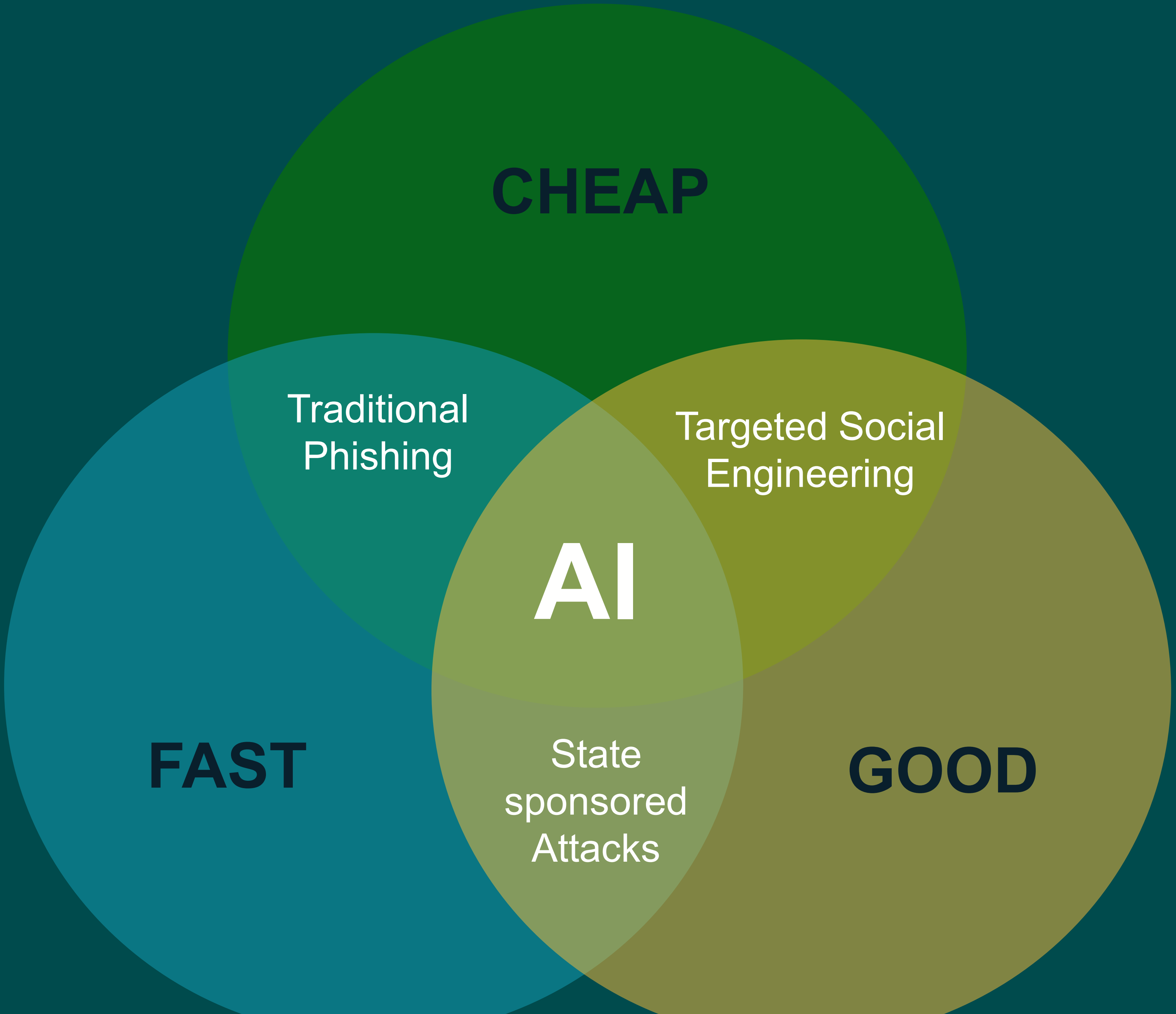
User Authentication

- Phishing
- Credential stuffing
- Man in the Middle
- Spear-phishing
- SIM swapping
- Social engineering

Account Recovery & Identity Re-verification

- Account take over
- Consumer and business fraud
- Stolen identities
- Business Email Compromise


FAST
CHEAP
GOOD



DARKTRACE

Phishing attacks surge by 620% in the lead-up to Black Friday

CNN

Finance Worker Pays out $25 million after video call with deepfake 'CFO'

Office of Information Security
Securing One HHS

New Spear Phishing Campaign by Midnight Blizzard

Generative AI Is..

Fast

200x

increase in personalization. AI-powered attacks can generate 10k personalized emails compared to 50 from a human in the same time.

(Brightside)

Cheap

95%

reduction in costs when using LLMs to automate entire phishing campaigns.

(Harvard Business Review)

Scalable

4151%

rise in malicious phishing emails since Q4 2022 & ChatGPT.

(Slashnext)

And highly effective

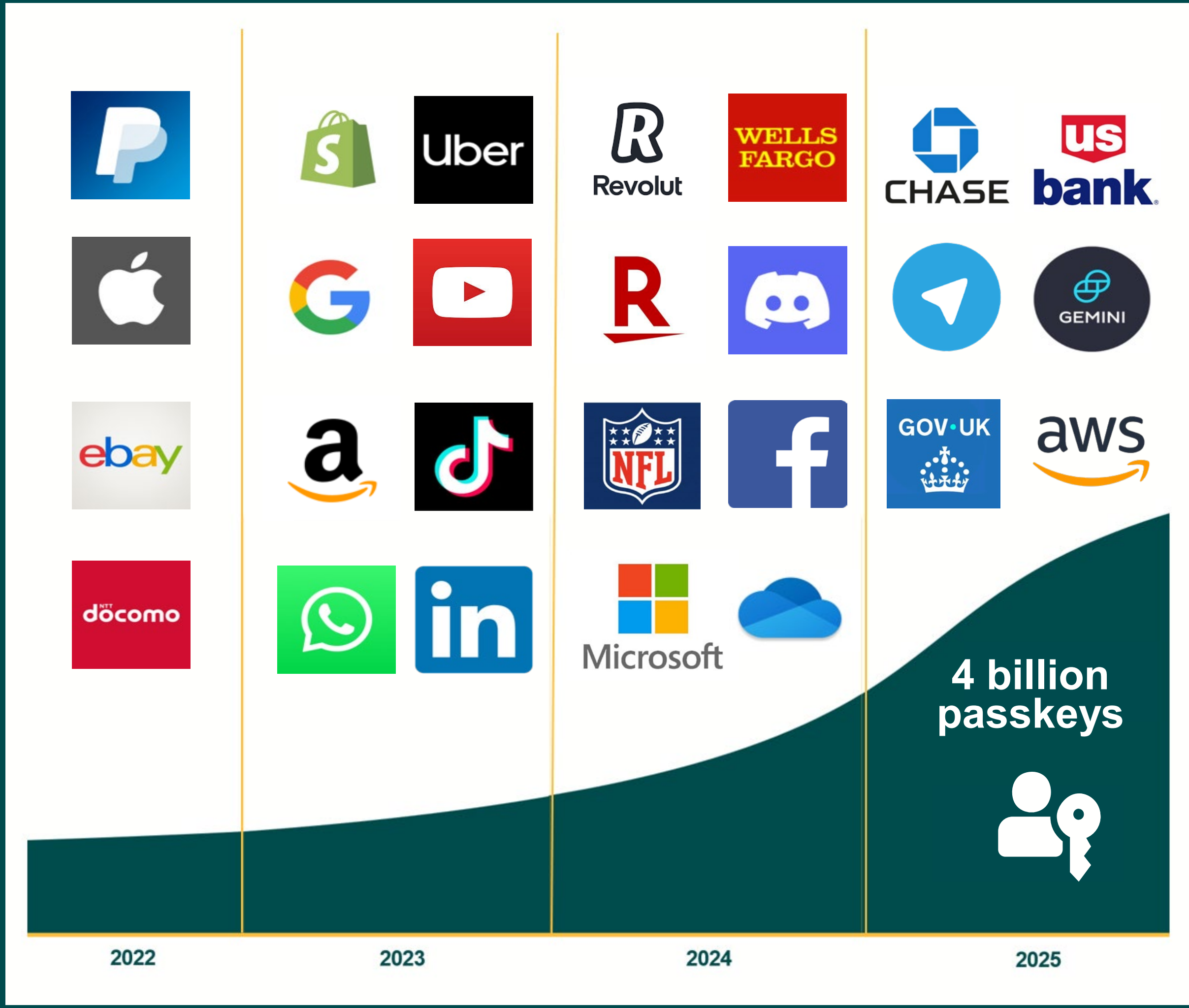
47%

success rate from AI-powered spear phishing attacks specifically when targeting trained security professionals.

(IBM)

Passkeys are improving and securing user sign-in

Passkey Success



- 93% login success rate *(Passkey Index)*
- 81% reduction in login-related help desk incidents *(Passkey Index)*
- Over 11m high-risk transactions protected without incident
- 32% fewer password recovery requests, and 30k fewer monthly ID-related calls
- The more passkeys are utilized, the more revenue increases
- 200m users registered and 3% reduction in SMS OTPs

ABANCA
ANZ
CHASE
DCU
FIRST
mastercard
nab
Revolut
:ubank
us bank
WELLS FARGO
first credit union

Global Government and Regulatory Engagement

NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PUBLICATIONS

NIST SP 800-63-4

Digital Identity Guidelines

Date Published: July 2025

Supersedes: SP 800-63-3 (03/02/2020)

Author(s)

David Temoshok (NIST), Diana Proud-Madruga (Electrosoft), Yee-Yin Choong (NIST), Ryan Galluzzo (NIST), Sarbari Gupta (Electrosoft), Connie LaSalle (NIST), Naomi Lefkovitz (NIST), Andrew Regenscheid (NIST)

Abstract

These guidelines cover the identity proofing, authentication, and federation of users (e.g., employees, contractors, or private individuals) who interact with government information systems over networks. They define technical requirements in each of the areas of identity proofing, enrollment, authenticators, management processes, authentication protocols, federation, and related assertions. They also offer technical recommendations and other informative text as helpful suggestions. The guidelines are not intended to constrain the development or use of standards outside of this purpose. This publication supersedes NIST Special Publication (SP) 800-63-3.

Keywords

assertions; authentication; authentication assurance; authenticator; credential service provider; digital authentication; identity proofing; federation; passwords; PKI

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

NIS2

TECHNICAL IMPLEMENTATION GUIDANCE

Business | Press Room Language Search

Digital Agency

This page has been translated using TexTra by NICT. Please note that the translation may not be completely accurate.If you find any mistranslations, we appreciate your feedback on the " Request form for improving the automatic translation ".

Current page： Home › Policy › My Number (Individual Number) Scheme / My Number Card › My Number Card utilization information for private sector › Japanese Public Key Infrastructure (JPKI)

Japanese Public Key Infrastructure (JPKI)

Last Updated:Feb 13, 2026

This section introduces basic information (service features and certification mechanism), service introduction examples, and useful information for service introduction (introduction method, procedure for introduction, Japanese Public Key Infrastructure usage fee, etc.) required for local governments and private sector residents to introduce Japanese Public Key Infrastructure (JPKI * 1).

* 1 Japanese Public Key Infrastructure

Financial Services Agency

○ Given the vulnerabilities of ID and password-only authentication, and the limited effectiveness of one-time passwords sent via email or SMS against modern phishing attacks, it is essential to mandate robust multi-factor authentication methods, such as passkeys. As attack techniques continue to evolve, countermeasures must be developed with the assumption that new methods will surpass existing defenses. Continuous monitoring of technological trends in both attack vectors and security solutions is necessary.

○ If adequate security cannot be ensured, financial institutions should consider suspending services proactively rather than reacting after damage occurs. Protecting customer assets is fundamental to customer-centric management, and we urge management to treat this as a critical issue requiring direct involvement.

Phishing-resistant authentication and passkeys are required or recommended by these governments

United States	Europe	Brazil	Japan	Malaysia	Singapore	Taiwan
Canada	United Kingdom	Honk Kong	Israel	New Zealand	South Korea	

FIDO In The Workplace

High Adoption & Priority

87% have successfully deployed or are currently deploying passkeys.

68% of all respondents said passkey deployment is a high or critical priority in their organization, rising to 71% among those who have already deployed.

Strategic Deployment

The top user groups targeted for passkey rollout were those requiring access to intellectual property (39%), users with admin accounts (39%), and users at the executive level (34%)

Only 21% targeting all users organisation-wide.

Measurable ROI

Security and efficiency gains are immediate.

90% of deployers report a moderate to strong impact on security, 82% on user experience, 77% on help desk call reduction, 73% on employee productivity, and 83% on digital transformation goals.

FIDO is securing trust across the account lifecycle

Securing the Account Lifecycle: The FIDO Approach

Secure Account Enrollment

Certified Remote Identity Verification

Phishing-resistant User Authentication

Passkeys

Secure Account Recovery

fido CERTIFIED IDV

fido CERTIFIED IDV

fido CERTIFIED UAF U2F FIDO2

fido CERTIFIED Biometric

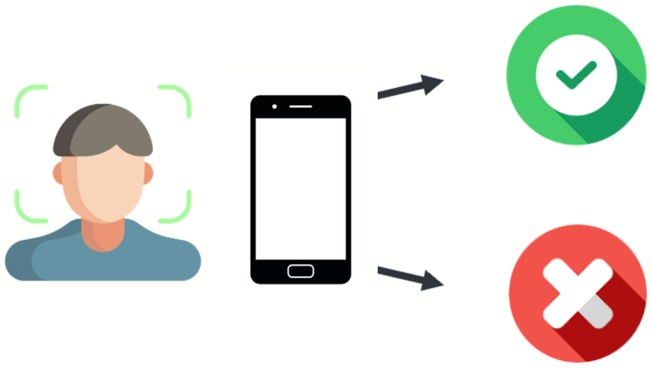
Securing Account Enrollment

IDV for Remote Identity Verification

- The process of providing sufficient information to establish an identity
- Document Authenticity Program
  - Determine the authenticity of a trusted ID document
- Face Verification Program
  - Comparison of face image on ID document with a selfie

Biometric Component Certification for Authentication

- The process of ensuring same person as enrolled
- Consumer device used for biometric enrollment
- Same device used for authentication



FIDO’s Next Frontier: Digital Credentials

Verifiable Digital Credentials Vision

A world where individuals can securely control, present, and delegate their digital credentials with the same **simplicity, trust & interoperability** that passkeys do for authentication.

Challenge: fragmented ecosystem impacting ecosystem buildup & adoption

Multiple standards available, making developer story overly complex

Multiple stakeholders (issuers, holders, verifiers) involved

Issuance and consumption of credentials impacted by lack of relevant certification programs

Applying the FIDO Alliance model for success to Digital Credentials

Technical Specifications

- CTAP / PXP
- OIDF / ISO / W3C

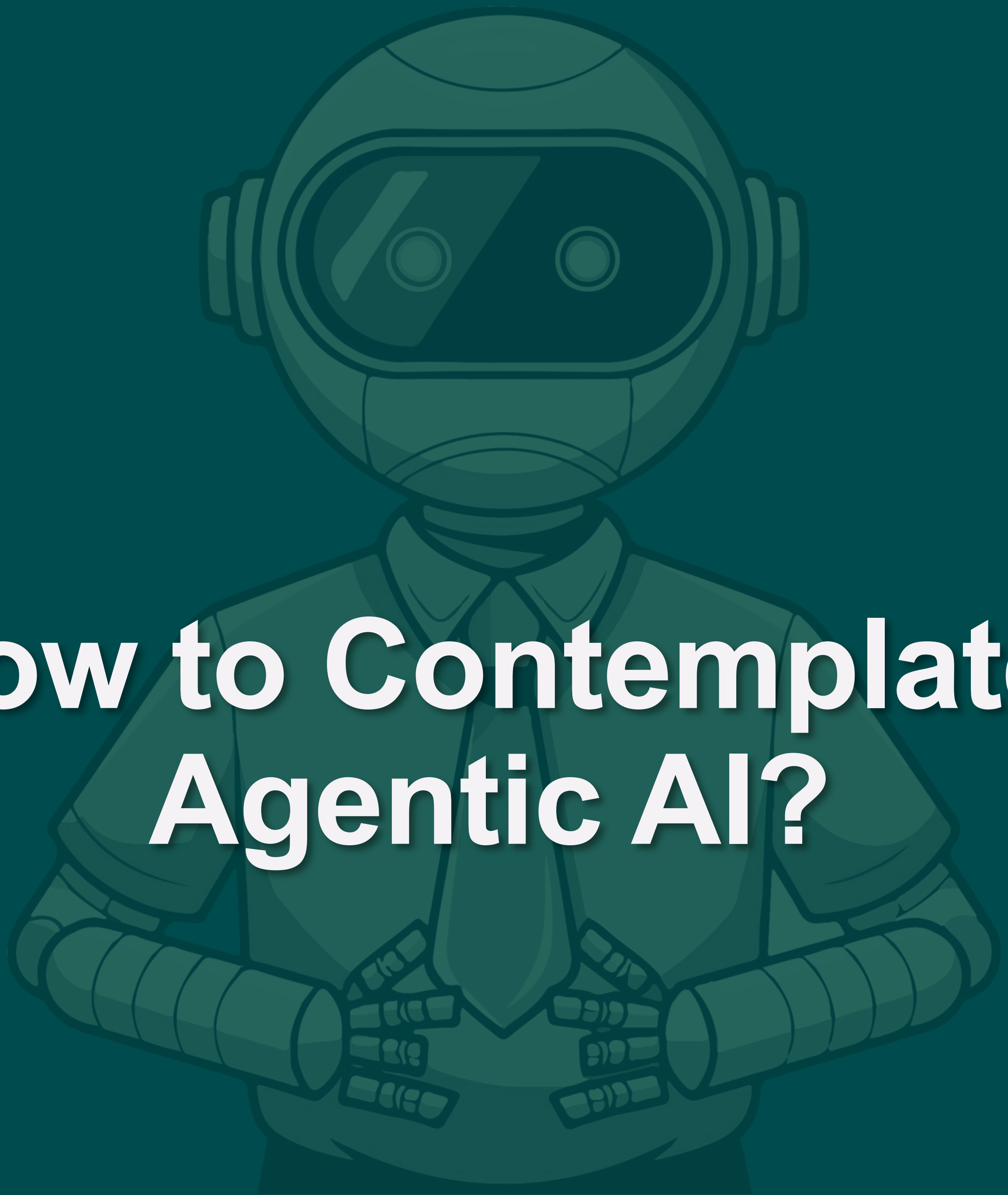
Market Adoption Programs

- UX guidance
- RP support

Industry Certification Programs

- Baseline Wallet Profile ++

Engaged, Committed Community



How to Contemplate Agentic AI?

Wrapping Up..

Passkeys are securing and improving user sign-in

Agentic AI introduces added use cases and imperatives for modern authentication

Verifiable Digital Credentials promise to establish trust across the account lifecycle

Thank you