fido ALLIANCE

December 11, 2024

Dear Madams,
Dear Sirs,

We are writing regarding the Reserve Bank of India's (RBI) recent Draft Framework for Comments on Alternative Authentication Mechanisms for Digital Payment Transactions. We understand that the formal comment period has closed and that our submission is late; we were unfortunately unaware of this draft until recently, and hope that, despite its tardiness, RBI is willing to consider our inputs.

Our concern is that, as currently written, the draft Framework may inadvertently preclude the use of the FIDO authentication standards – which are recognized across the globe as the "gold standard" for authentication – thus precluding Indian financial services firms and consumers from being able to use one of the most secure and user-friendly authentication standards.

We request that RBI consider allowing FIDO authentication to be used as an alternative to one-time passwords (OTPs), and outline our rationale below.

As background, the Fast Identity Online (FIDO) Alliance is a multi-stakeholder, public-private, industry standards development organization comprised of more than 300 companies and government agencies from around the world dedicated to the creation of standards and certification programs for Multi-Factor Authentication (MFA) and passwordless authentication, as well as remote identity verification.

Our 40+ board members, whose logos are included below, demonstrate the strength of the FIDO Alliance's leadership, as well as the diversity of its membership. Our members include leading firms in banking, payments, telecommunications, and fintech, as well as those in security, health care, and information technology.

The launch of the FIDO Alliance in 2012 – and the subsequent creation and mass adoption of FIDO authentication standards over the twelve years that have followed – has helped to transform the authentication landscape, addressing concerns about the problems with passwords, as well as the increasing phishability of legacy, first-generation MFA tools like OTPs while also enabling significant improvements in the usability of MFA.

Today, the FIDO standards have emerged as the de-facto best choice for implementers seeking to deploy phishing-resistant authentication that is both more secure and also easier to use than legacy authentication tools. They are supported by a broad ecosystem of more than 1000 products that have been certified as meeting the FIDO standards, ensuring that enterprises of all sizes are able to choose from a variety of interoperable, standards-based products to meet their authentication needs. Moreover, with the FIDO Web Authentication protocol being a W3C standard, ever major browser and platform ships with native support for FIDO, making phishing resistant authentication as easy (or often easier) to deploy as legacy authentication tools.

FIDO standards are recognized by governments across the globe

- The Financial Action Task Force (FATF) highlighted the importance of the FIDO standards in its 2020 Digital Identity Guidelines,[1] noting:

  > *"Multi-factor authentication (MFA) solutions, such as SMS one-time codes texted to the subscriber's phone, add another layer of security to passwords/passcodes but they can also be vulnerable to phishing and other attacks. Phishing-resistant authenticators where at least one factor relies on public key encryption (e.g., authenticators built off PKI certificates or the FIDO standards) can help combat these vulnerabilities."*

- FIDO is widely used in other countries across Asia, including Singapore, Malaysia, Thailand, and Vietnam; also in APAC, Australia has highlighted the importance of FIDO authentication as part of its "Essential Eight cybersecurity practices; use of phishing-resistant FIDO authentication is part of achieving the highest level (Maturity Level Three) of their Essential Eight Maturity Model.[2] Per their FAQ:

  > *"Organisations are encouraged to use multi-factor authentication solutions that have been certified against the FIDO2 standard (preferably Level 2 over Level 1)."*

- In the US, the Cybersecurity and Infrastructure Security Agency (CISA) has called FIDO the "gold standard" for MFA; an August 11, 2022 circular[3] from the U.S. Consumer Financial Protection Bureau (CFPB) states:

  > *"MFA solutions that protect against credential phishing, such as those using the (FIDO) Web Authentication standard supported by web browsers, are especially important."*

[1] See https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html

[2] See https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model-faq and https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model

[3] See https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/

- ENISA and CERT-EU highlighted the importance of FIDO in a 2022 publication entitled "Boosting Your Organization's Cyber Resilience (JP-22-01),[4] noting:

  > *"If possible, avoid using SMS and voice calls to provide one-time codes and consider deploying phishing resistant tokens such as smart cards and FIDO2 (Fast IDentity Online) security keys."*

- Also in Europe, Banque de France and the Netherlands National Cyber Security Center (NCSC) have both highlighted the importance of FIDO authentication in publications.
  - The report "Annuel de l'Observatoire de la Sécurité des Moyens de Paiement 2021" from Banque de France highlights how FIDO authentication is being used to address banking authentication challenges in France[5].
  - The Netherlands NCSC's publication "Mature Authentication – Use of Secure Authentication Tools" states that FIDO is *the "Most secure type of authentication, phishing resistant and user friendly"* and notes *"Tokens that implement this standard provide the most comprehensive protection for authentication at this time."*

FIDO adoption across the globe

Consumer facing organizations are adopting FIDO as their preferred authentication standard at scale across the globe, in many cases replacing legacy methods such as password and OTP. This includes many organizations who have a footprint in India and thus may be of particular interest to RBI.

- Google: At FIDO's recent 2024 Authenticate Conference, Google shared that over 2.5 billion sign-ins and 800 million accounts have used passkeys, boasting a 30% higher sign-in success rate compared to passwords.
- Amazon: More than 175 million Amazon customers are using passkeys.[6]
- X (formerly Twitter) : X improved login success rate by 2x after adopting passkeys.

Concerns with the Draft Framework for Comments on Alternative Authentication Mechanisms for Digital Payment Transactions

A number of our members have flagged that this draft framework is written in a way that could preclude use of the FIDO standards – and potentially favor use of less secure authentication approaches such as OTP that do not align with FIDO or other global best practices in authentication. We request some minor changes to the draft which would allow FIDO authentication to be used as an alternative to one-time passwords (OTPs).

As written, there are a number of elements in the current draft that might be viewed as precluding use of FIDO:

1. The "something the user has" definition only refers to "card hardware" or "software tokens," which

[4] See https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience

[5] See https://www.banque-france.fr/fr/publications-et-statistiques/publications/rapport-annuel-de-lobservatoire-de-la-securite-des-moyens-de-paiement-2021 and https://english.ncsc.nl/publications/factsheets/2022/juni/9/factsheet-mature-authentication---use-of-secure-authentication-tools

[6] See https://www.aboutamazon.com/news/retail/amazon-passwordless-sign-in-passkey

might be viewed by some implementers as too narrow a definition to support FIDO authentication. We request this be amended to say: "such as card hardware, software token, security key, or cryptographic authenticator."

2. The "dynamically created" requirement (Principle 3b) might preclude use of FIDO authentication, as it seems to refer to the way OTPs are created. FIDO, while it does not support one-time passwords, is much more secure than an OTP and is also easier to use. We request that this be amended to make clear that this requirement only applies when the AFA is an OTP.

   The "dynamically created" requirement (Principle 3b) stipulates that one of the factors of authentication must be dynamically created at the moment of the payment transaction. However, the possible authentication factors (something the user has, knows or is) typically already exist before a transaction is initiated, and are usually not dynamically generated at the moment of the payment transaction. Instead the authentication factor(s) typically dynamically generate cryptographic output that is specific to the transaction. We therefore believe the current wording might preclude commonly used MFA solutions, including OTP and FIDO-based solutions. We request that this be amended to clarify that the authenticator's output is dynamically generated, rather than the authentication factor itself.

3. The "robust" requirement (Principle 3c) does not mention phishing-resistance. While we believe a mandate for phishing resistance might be too limiting, we believe it would make sense for RBI to note that AFA's should aspire to be phishing resistant. We believe the following language would be helpful:

   > "The first factor of authentication and the AFA shall be from different categories, as defined in para 2(e) of this framework, *and ideally be phishing-resistant*."

   With this change, it would also make sense to add a definition for phishing-resistance to the definitions section. We suggest the following, based on the definition created by the National Institute of Standards and Technology (NIST)[7] in the United States:

   > "i. Phishing Resistance: Phishing resistance is the ability of the authentication protocol to prevent the disclosure of authentication secrets and valid authenticator outputs to an impostor verifier without relying on the vigilance of the claimant."

We greatly appreciate RBI's consideration of our comments. We look forward to further discussion with RBI on this topic and would welcome the opportunity to answer any questions or collaborate on approaches to address some of the issues we raised in this letter.

Additionally, we are available to present an overview of FIDO standards and the FIDO Alliance, should RBI officials wish to learn more about how FIDO authentication and how its certification programs work.

[7] See https://pages.nist.gov/800-63-4/sp800-63b/authenticators/

Please contact our Executive Director, Andrew Shikiar, at andrew@fidoalliance.org, or our government engagement advisor, Jeremy Grant, at jeremy.grant@venable.com.

Additionally, you might wish to contact the FIDO members who serve as the leadership team of FIDO Alliance’s India Workgroup:

- Arjun Varghese, Chair, FIDO India working group, Infineon Technologies Arjun.Varghese@infineon.com
- Niharika Arora, Co Vice-Chair, FIDO India working group, Google aroraniharika@google.com
- Tapesh Bhatnagar, Co Vice-Chair, FIDO India working group, Giesecke & Devrient MS India Pvt. Ltd. tapesh.bhatnagar@gi-de.com