January 31, 2024

Dear Madams,
Dear Sirs,

We are writing to express our concerns about the Turkish Banking Regulation and Supervision Agency's (BRSA) Circular 2023/1, which governs Identity Authentication and Transaction Security in the Establishment of Contract Relations in Electronic Banking Services.

Specifically, we are concerned that BRSA may have inadvertently written the Circular in a way that would preclude the use of the FIDO authentication standards – which are recognized across the globe as the "gold standard" for authentication – and lock Turkish banks into a non-standard, proprietary solution.

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 eleven years that have followed – has helped to transform the authentication market, addressing concerns about the problems with passwords, as well as the increasing phishability of legacy, first-generation MFA tools like One Time Passwords (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.

FIDO standards are recognized 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.*

- ENISA and CERT-EU highlighted the importance of FIDO in a 2022 publication entitled "Boosting Your Organization's Cyber Resilience (JP-22-01),[2] 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[3].

  - 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 "T*okens that implement this standard provide the most comprehensive protection for authentication at this time."*

- In the US, the Cybersecurity and Infrastructure Security Agency (CISA) has called FIDO the "gold standard" for MFA; an August 11, 2022 circular[4] 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.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience

[3] See https://www.banque-france.fr/fr/publications-et-statistiques/publications/rapport-annuel-de-lobservatoire-de-la-securite-des-moyens-de-paiement-2021

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

Concerns with BRSA Circular 2023/1

A number of our members have flagged that this Circular is written in a way that would 1) preclude use of the FIDO standards, and 2) require the use of a proprietary authentication approach that does not align with FIDO or other global standards.

Specifically, there are a number of elements in the Circular that are of concern:

1) By requiring that Turkish financial institutions use not one but two public/private key pairs – and by requiring that the public key of the authentication key pair is used to encrypt signing requests intended for a certain user or authenticator, the Circular effectively precludes use of FIDO standards.

2) FIDO standards support verification of a knowledge factor (PIN) on the device (such as a smartphone) being used for authentication, but do not support server-side matching of these factors as a way to unlock the private key used to facilitate secure authentication; this is designed to provide security and privacy to the owner of the private key. In contrast, a requirement that the PIN that is used to unlock an authenticator be stored centrally will lead to multiple counter-parties that have knowledge of the PIN, and that can lead to increased risk for the compromise of credentials.

3) The FIDO standards do not allow sending a hash of the PIN, used by the user to authenticate to the FIDO authenticator, to the authentication server, for security reasons. If a hash of the PIN would be communicated to the server, it could be intercepted and be used to perform a brute force attack on the PIN. With the FIDO standards, information about the local authentication method never leaves the authenticator.

The net impact of this language is notable: by locking Turkish financial institutions into a proprietary solution, it limits competition and drives up the cost of authentication solutions. Additionally, it precludes Turkish financial institutions from taking advantage of an authentication standard that has been globally recognized as “best in class.”

We greatly appreciate BRSA’s consideration of our comments. We look forward to further discussion with BRSA 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 BRSA officials desire to learn more about how FIDO authentication and how its certification programs work.

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