FIDO Authentication in Digital Payment Security
: In line with the Reserve Bank of India's Master Directions

August 2022

Editors:
Deb Jyoti Ghosh, Visa
Tapesh Bhatnagar, Giesecke + Devrient
Amit Mathur, Ensurity
Shankar Ramaswamy, Individual Contributor

Abstract

The Indian Payments ecosystem is going through rapid change and advancement. The Reserve Bank of India (Digital Payment Security Controls) Directions 2020 were issued for regulated entities to set up a robust governance structure for such systems and implement common minimum standards of security controls for channels like internet, mobile banking, and card payments, among others. In this paper, we demonstrate how FIDO Authentication represents the best way for organizations to implement simpler, stronger authentication that meets Reserve Bank of India's Master Direction on Digital Payment Control requirements, while also enhancing the user experience.

Audience

This paper is aimed at banking industries and regulators in India.

Contents

1. Introduction

The Indian Payments ecosystem has seen rapid change in the recent past. Frequent innovation and brisk implementation of new payments technologies have renewed focus towards safety, security, and ease of payments. In the past two decades, the role of the Reserve Bank of India (RBI) has transformed from regulator, operator, and facilitator to creator of an environment for the structured development of the India payment ecosystem system. Based on the 2019-2021 payment vision document from RBI, organizations have worked towards enhanced outreach, customer centricity, cyber security, and digital deepening and are further expected to consolidate the outcomes and realize the next 2025 payment vision, which is based on integrity, inclusion, innovation, institutionalization, and internationalization. Further, RBI has acknowledged the need to weave in alternate authentication mechanism(s) for digital payment transactions [1].

1.1 Reserve Bank of India – Digital Payment Index (RBI-DPI)

In 2021, RBI announced a composite Reserve Bank of India – Digital Payments Index (RBI-DPI), using March 2018 as the reference point, to document the degree of payment digitization across India. The DPI for September 2021 stood at 304.06 as against 270.59 for March 2021. The numbers were an indicator of several factors with reference to digital payments [2] :

a. rapid awareness and knowledge of the digital payment system
b. swift adoption of the system
c. expansion of infrastructure by service providers to accommodate the swell of digital payments
d. innovative technologies adopted by select service providers to improve costumer experience
e. development of new systems of digital payments other than banks.

The role of digital payments has thus gained importance in the economic activity of the country. Therefore, to provide security and regulation to India's financial environment, RBI issued "The Reserve Bank of India (Digital Payment Security Controls) Directions 2020." The main aim of the controls and guidelines are

a. to establish a governance structure for such systems
b. to define minimum security control standards for channels like internet, mobile banking, and card payments, among others
c. to be technology and platform agnostic
d. to create an enhanced and enabling environment for customers to use digital payment products in a more safe and secure manner.

1.2 Regulated Entities

The provisions of these directions apply to the following Regulated Entities (REs):

a) scheduled commercial banks (not including regional rural banks)
b) small finance banks
c) payments banks
d) credit card issuing NBFCs. [3]

2. Impact on Authentication

Within the directions, there are several guidelines specifically impacting authentication. These are as follows:

2.1 Authentication Framework – Guideline No. 34E

"At least one of the authentication methodologies should be generally dynamic or non-replicable. [e.g., Use of One Time Password, mobile devices (device binding and SIM), biometric/ PKI/ hardware tokens, EMV chip card (for Card Present Transactions) with server-side verification could be termed either in dynamic or non-replicable methodologies." [1]

⇨ This guideline opens a path for alternative forms of authentication, including biometric. The guideline, along with guideline 60, mandates the binding of devices with the identity of the consumer.

2.2 Authentication Framework – Guideline No. 34E

"As a key component of multi-factor authentication (MFA) architecture, REs "should also implement appropriate measures to minimize exposure to a middleman attack. . . more commonly known as a man-in-the-middle attack (MITM), man-in-the browser (MITB) attack, or man-in-the application attack ("Internet Banking Facility for Customers of Cooperative Banks")." [1]

⇨ This process is to ensure, among other things, that the data in transit is secured and the transactions are authenticated only by a genuine/authorized source/process.

2.3 Mobile Payments Application Security Controls – Guideline No. 60

"REs shall ensure device binding of mobile applications." [1]

2.4 Mobile Payments Application Security Controls – Guideline No. 61

"Considering that the additional factor of authentication and mobile application may reside on the same mobile device in the case of mobile banking, mobile payments, REs may consider implementing alternatives to SMS-based OTP authentication mechanisms." [1]

⇨ This guideline, in conjunction with guideline 60, allows third-party authenticator apps and platform authenticators to participate in the transaction authentication process.

The requirements around authentication can thus be summarized as follows:

a) strong device identity

b) identity bound to device

c) multiple alternatives to MFA, including biometrics

d) participation of platform authenticators.

2.5 Industry View

Major fintech companies are petitioning with RBI to implement an alternate to SMS-OTP based authentication [3]. Security and operational costs have been cited as major reasons for this change. An in-app authentication would also limit consumer exposure to external fraud and data sharing between different parties.

In the next sections, we investigate how FIDO can meet all the specifications set forth by RBI.

3. Introduction to FIDO

FIDO (Fast IDentity Online) is the industry's answer to secure and fast authentication. It is based on binding the device with the user and consequently using the device to authenticate the user action. It addresses a variety of use cases including MFA.

FIDO Alliance is a 250+ strong member body. The members include government agencies who are active in authentication. FIDO standards are built in almost all browsers, operating systems, and consumer devices used in online transactions (laptops, phones, tablets). Apart from platform authenticators, (e.g., authenticators built in the device), FIDO works seamlessly with roaming authenticators. In India, field studies conducted with MoF using roaming FIDO devices have produced great results (see "FIDO Adoptions and Case Studies in India").

3.1 What is FIDO Authentication

FIDO Authentication is based on free and open standards developed by the FIDO Alliance. It encompasses a set of authentication techniques other than passwords and SMS OTPs. Instead of passwords, it enables logins to be replaced by a secured and stronger user authentication mechanism employing biometrics, tokens, smart cards, near field communication devices, and many more authentication methods across the web and mobile applications.[1]

To achieve its mission, the FIDO Alliance has primarily involved in three areas of work:

3.1.1 User authentication

FIDO standards-based authentication eliminates many of the vulnerabilities and problems that arise from password-based authentication, one-time-passwords through SMS. FIDO Authentication is strong, secure, and simple simply because it is based on public key cryptography.

The standards are designed such that it offers

a. strong and strong authentication (more than passwords and SMS OTPs)
b. simple and easy to implement, deploy and manage
c. ease of use for consumers.

3.1.2 Identity verification and binding

FIDO standards-based authentication perfectly attacks authentication problems by providing strong user identity verification and device binding protocols. The Identity Verification and Binding Working Group (IDWG) and the FIDO Alliance have created and developed newer

[1] To know more about how FIDO works, visit https://fidoalliance.org/how-fido-works

methods of capturing user credentials and protecting them. Subsequently, the group has established stricter account recovery processes when the user's device is manipulated or lost. The accounts created with FIDO Authentication in place meet the Know Your Customer (KYC) and Anti-Money Laundering (AML) guidelines while giving the user

a. strong and simple account onboarding processes
b. strong protection against account takeover attacks (phishing)
c. strong identity verification and assurance
d. secured and smooth account recovery.

3.1.3 Internet of Things

The FIDO Alliance IoT Technical Working Group has been working towards making FIDO standards-based authentication able to keep pace with the billions of connected things as forecasted by Gartner. It aims to provide a comprehensive authentication framework for IoT devices. The idea is to eliminate the vulnerabilities due to obsolete security standards and the desire for stronger IoT security standards. [4]

4. FIDO Authentication Compliant with RBI's Master Direction on Digital Payment Security

Strong consumer authentication works on three basic principles:

a. who you are
b. what you have
c. what you know

While SMS OTP only covers one of the criteria (b), traditional PINs/passwords also covers "What you know." FIDO encompasses both "a "who you are" and "what you know." In the sections below, we investigate how FIDO is compliant with the criteria mentioned in section 2.4.

The following table provides a comparison of current SMS-OTP as AFA and how FIDO is compliant with RBI guidelines on Digital Payment Security controls:

Guidelines	PW/SMS-OTP	FIDO	Comment
Multi-factor Authentication	√	√	Possession + Biometric or PIN
Dynamic Authentication	√	√	Challenge-Response, Dynamic Signature
Non-Replicable	√	√	Private Key in Key Store, EMV Card or HW Token
Adaptive Authentication	×	√	Policies, Scalable Security
Confidentiality Protection	×	√	End-to-End Protocol Security + TLS
Resistance against Phishing, Key Logging	×	√	No Shared Secrets, Passwordless

MITM Resistance	×	√	No Shared Secrets, proven protocol security
Ease of Use	×	√	Single Factor Feeling to End-User
Interoperability	×	√	FIDO, W3C standard, Integrated into EMVCo 3DSecure

Table 1 - SMS-PTP as AFA and FIDO Compliance with RBI Guidelines

4.1 Strong Device Identity

Man-in-the-Middle Attacks aim to steal personal information of a user, such as usernames, passwords, account information, and more. This information is used by malicious entities to access accounts and conduct unauthorized transactions. The aftermath of such activities creates heavy losses for both the organization and the customer. Traditional authentication mechanisms are vulnerable to MITM attacks even though multi-factor authentication is employed.

FIDO security keys based on FIDO Alliance standards are easier to use and more secure than other forms of MFA and solve the problem of MITM attacks by providing cryptographic proof the user is in possession of the second factor, and that they are interacting with a legitimate service.

FIDO protocols are designed from the key idea of providing user privacy and security from the ground up. These protocols are device-specific and therefore do not provide information that could be easily tracked by online services.

The FIDO protocols may be used independently in three ways in authentication, or in a combination of ways, depending on the device and use application:

a. complete passwordless or without a token
b. with a hardware security key, and/or
c. with near-field communication (NFC) devices with a security key (for mobiles).

4.2 Device Binding

The process of binding (linking) a token to a trusted device is called “device binding.” In other words, it is a process to register a device as a trusted device for any financial transaction.

FIDO2 includes FIDO Protocols that are built using public key cryptography (also known as public-key encryption or asymmetric encryption) device techniques to provide strong authentication. This technology, which provides the utmost security and privacy was (and is currently being used) in security tokens, has been extended to mobile devices. It uses a pair of keys known as a public key and a private key (a public key-private key pair), which are associated with an organization that needs to authenticate its identity for signing encryption or any transaction done digitally. The public key is published, and the corresponding private key is kept undisclosed. The public key validates messages that could only be generated by the corresponding private key.

The FIDO2-enabled tokens and mobile devices work exactly in the same way providing hardware grade security. Moreover, using mobile devices with a base minimum configuration as an authenticator works perfectly well for any user, allowing reduced friction and increased security [5].

4.3 Alternative On-Device Authentication Other Than SMS-OTP

By far, SMS OTP was and is the most widely accepted and fastest method of second-factor authentication, resulting in considerable reduction of cyber frauds. Although OTP is one of the strongest methods of authentication to protect against account thefts, hacking methods have evolved and caused SMS OTP breaches in recent times. The most common of such frauds are SIM SWAP and SS7 attacks. SIM SWAP attacks result in the victim's telephone number being hijacked by an attacker, while SS7 attacks result in the victim's SMS being intercepted. These attacks rely on limited methods of access control to the SS7 network and vulnerabilities in SS7 MAP methods.

FIDO2 enables users to have complete control over common devices and use them to authenticate themselves for online services through web and mobile environments. By enabling device binding, the need for SMS OTPs are eliminated, thus eliminating all attacks of SIM SWAP, password theft and replay attacks [5].

4.4 Multiple Forms of Authentication

FIDO works across all accepted form of biometric authentication, as well as PIN and pattern-based authentication, providing consumers with choice. For strong consumer authentication, FIDO recommends biometric authentication, as it has proven to be more secure [6].

4.5 Ubiquity of FIDO[2]

There are 900+ FIDO-certified devices. All major device manufacturers, including Google, Apple, Samsung, Lenovo, are members of FIDO alliance.

All major browsers—Chrome, Safari, Edge, Firefox, Opera—are FIDO compliant.

Major OS manufacturers—Apple, Microsoft, Google—are FIDO certified.

Security key manufacturers—Ensurity, Yubico, ATKey, Giesecke + Devrient, RSA, OneSpan —manufacture FIDO certified devices.

Major IT and network security providers—RSA, Thales, TrustKey—utilize FIDO.

Chipset manufacturers, like Intel, Infineon, and Qualcomm are also relying on FIDO to provide high scale security.

Major financial organizations and solution providers such as Visa, Giesecke+Devrient, Mastercard, and Bank of America, chose FIDO as a preferred mode of authentication.

5. FIDO More Secure than SMS OTP

FIDO provides a higher level of security compared to SMS OTP. Below we detail how FIDO is enabled to counter particular threats compared to OTP.

5.1 SIM-Swapping Attack

[2] A list of FIDO members can be found at https://fidoalliance.org/members/

SIM-swapping attacks are executed through social engineering, where criminals use identity data from the victim to acquire a duplicate SIM with same number as the victim. SMSs are routed to the new number, which makes financial fraud possible [5].

As FIDO relies heavily on biometrics, which are harder to forge, it can prevent similar attacks.

5.2 Real-Time Phishing (MITM) Attack

MITM attacks are often carried out by fraudulent sites that mimic the original site to steal users' authentication information, such as OTP/passwords. The information is then used to carry out financial transactions [7]

As FIDO key pairs are different for each relying party (here merchant or merchant processor), a fraudulent site would not be able to complete a challenge/response mechanism. Hence, the attack will fail.

6. FIDO Adoptions and Case Studies in India[3]

6.1 – Government of India

The Government of India's Ministry of Finance, the agency for distribution of citizens' benefits, has been conducting POC under the Aegis of National Informatics Center for the deployment of two-factor authentication using biometric FIDO2 devices. The solution has been adapted so that it works with their application, and it also satisfies all audit requirements. After the successful POC, the paid field trials commenced in the first quarter of 2022, after which a decision will be made to deploy the solution throughout India across account offices.

6.2 – A Defense Research Organization

A sensitive defense research organization of India had conducted trials of FIDO2 biometric devices for a strong two-factor authentication on RHEL for PC login to ensure access to the data is restricted only to an authorized user. After successful testing, commercial deployment has started.

7. FIDO Bank Use Case – Middle East

A leading bank in the Middle East wanted to strengthen the security of its various banking applications. It has started implementing a strong two-factor authentication using FIDO2 biometric security keys. The first implementation is for core banking application; subsequently, other applications will also be integrated with FIDO authentication. For ease of use and manageability, a single console solution has also been developed and deployed to manage the large number of keys being deployed across SBUs and geographies.

[3] More case studies can be found at https://fidoalliance.org/content/case-study/.

8. FIDO Resources for Public Policy Discussion[4]

FIDO Alliance works very closely with multiple governments and public policy organizations. Many government ministries/departments are part of FIDO and increasingly influence standards and adoption. (Source : https://fidoalliance.org/members/). In multiple other countries, FIDO is actively working with organizations managing identity solutions, like UIDAI in India, to enhance consumer security and simplify the consumer experience, while protecting consumer data.

FIDO Alliance publicly provides the following resources for policy makers to consider as part of their decision-making process:

a. white papers
b. deployment showcases
c. technical presentations
d. research papers.

9. About FIDO Alliance

"The FIDO (Fast IDentity Online) Alliance was formed in July 2012 to address the lack of interoperability among strong authentication technologies and remedy the problems users face with creating and remembering multiple usernames and passwords. The FIDO Alliance is changing the nature of authentication with standards for simpler, stronger authentication that define an open, scalable, interoperable set of mechanisms that reduce reliance on passwords. FIDO Authentication is stronger, private, and easier to use when authenticating to online services" [8]. The FIDO Alliance is a multi-stakeholder, public-private, industry standards development organization comprised of more than 250 companies and government agencies from around the world dedicated to the creation of standards for multi-factor authentication.

10. Acknowledgments

We would like to thank all FIDO Alliance members and staff who participated in the group discussions or took the time to review this paper and provide input, specifically:

- Arshad Noor, StrongKey
- Mamta Abichandani, Infineon
- Andrew Shikiar, FIDO Alliance
- Joon Hyuk Lee, FIDO Alliance

[4] To learn more about FIDO Alliance's partnership with governments across the globe, including usability in GDPR and CCPA, visit https://fidoalliance.org/fido-government-deployments-and-recognitions/

11. References

[1] "The Reserve Bank of India (Digital Payment Security Controls) Directions 2020-21." Reserve Bank of India. February 18, 2021. https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12032&Mode=0#MD.

[2] "Press Releases." Reserve Bank of India. Accessed August 12, 2022. https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?

[3] "All You Wanted to Know About NBFCs." January 10, 2017. Reserve Bank of India. https://www.rbi.org.in/commonperson/English/Scripts/FAQs.aspx?Id=1167.

[4] "Internet of Things (IoT)." FIDO Alliance. Accessed May 19, 2022. https://fidoalliance.org/internet-of-things/.

[5] P. Suraksha and Surabhi Agarwal. *Economic Times*. "Replace SMS Alerts for Customers' Bank Transactions with App Notifications: Industry Lobbies." June 9, 2022. https://m-economictimes-com.cdn.ampproject.org/c/s/m.economictimes.com/tech/technology/replace-sms-alerts-for-customers-bank-transactions-with-app-notifications-industry lobbies/amp_articleshow/92090339.cms.

[6] Brodsky, Sascha. Lifewire "SIM Swapping Attacks Are Soaring and You Need to Be on Guard." February 14, 2022. https://www.lifewire.com/sim-swapping-attacks-are-soaring-and-you-need-to-be-on-guard-5219003.

[7] Ulqinaku, Enis, Hala Assal, AbdelRahman Abdou, Sonia Chiasson, and Srdjan Capkun. "Is Real-time Phishing Eliminated with FIDO? Social Engineering Downgrade Attacks against FIDO Protocols." Accessed August 12, 2022. https://fidoalliance.org/fido-alliance-announces-asia-pacific-authenticate-virtual-summit-to-drive-further-adoption-of-modern-user-authentication/.

[8] "About the FIDO Alliance." FIDO Alliance. September 5, 2021. https://fidoalliance.org/fido-alliance-announces-asia-pacific-authenticate-virtual-summit-to-drive-further-adoption-of-modern-user-authentication/.

12. Other Readings

"April 2022 Seminar: FIDO & Authentication Technologies." FIDO Alliance. April 7, 2022. https://fidoalliance.org/event/april-2022-seminar-fido-authentication-technologies/.

"Device Binding for Visa Tokenization Services." OpenWay (blog), August 27, 2020.

https://www.openwaygroup.com/way4-release-news-blog/2020/8/27/device-binding-for-visa-tokenization-services.

"FIDO Authentication and the General Data Protection Regulation (GDPR)." FIDO Alliance. May 2018. https://fidoalliance.org/wpcontent/uploads/FIDO_Authentication_and_GDPR_White_Paper_May2018-1.pdf.

"FIDO Authentication: A Passwordless Vision." FIDO Alliance. Accessed May 19, 2022. https://fidoalliance.org/fido2/.

Findon, Marc, Bernard Joly, and Alain Martin. "FIDO Alliance White Paper: PSD2 Support: Why Change to FIDO." June 2020. https://media.fidoalliance.org/wp-content/uploads/2020/06/PSD2-Support-Why-Change-to-FIDO-White-Paper.pdf.

"Identity Verification & Binding." FIDO Alliance. Accessed May 19, 2022. https://fidoalliance.org/identity-verification-binding/.

"Internet Banking Facility for Customers of Cooperative Banks." Reserve Bank of India. November 5, 2015. https://www.rbi.org.in/scripts/BS_CircularIndexDisplay.aspx?Id=10111.

Mueller, Manfred. "In Government, Access Control Means Cybersecurity." Last modified January 14, 2022. https://www.securityinfowatch.com/government/article/21251362/access-control-means-cybersecurity.

Reserve Bank of India. "Master Direction on Digital Payment Security Controls." February 18, 2021. https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032.

"Reserve Bank of India Announces Digital Payments Index (RBI-DPI) for March 2021." Reserve Bank of India. July 28, 2021. https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=51962.

"U.S. General Services Administration's Rollout of FIDO2 on Login.gov." FIDO Alliance. Accessed, May 19, 2022. https://fidoalliance.org/u-s-general-services-administrations-rollout-of-fido2-on-login-gov/

"What is a Man-in-the-Middle (MiTM) Attack?" Yubico. Accessed May 19, 2022. https://www.yubico.com/resources/glossary/man-in-the-middle/.

"What Makes FIDO Different?" FIDO Alliance. Accessed May 19, 2022. https://fidoalliance.org/key-differentiators/.