FOCUS NOTE

CUSTOMER AUTHENTICATION 2.0: APPROACHES AND CHALLENGES IN FAST PAYMENTS

PROJECT FASTT

FRICTIONLESS • AFFORDABLE • SAFE • TIMELY • TRANSACTIONS

AUGUST 2023

WORLD BANK GROUP

FINANCE, COMPETITIVENESS & INNOVATION GLOBAL PRACTICE
Payment Systems Development Group

1818 H Street NW
Washington DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

This volume is a product of the staff of the World Bank. The findings, interpretations, and conclusions expressed in this volume do not necessarily reflect the views of the Executive Directors of the World Bank or the governments they represent.

The World Bank does not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of the World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

CONTENTS

1. SETTING THE CONTEXT 1

2. BACKGROUND 2

3. WEIGHING AUTHENTICATION APPROACHES IN AN FPS CONTEXT 4

3.1 Factor-based authentication 4

3.1.1 One-Time Passwords (OTP) 6

3.1.2 Biometric authentication 7

3.1.3 Device binding 8

3.2 Digital identity-based authentication 8

3.3 Risk-based authentication 10

3.4 Comparison of different authentication approaches 11

4. BEST PRACTICES AND CONSIDERATIONS 12

4.1. Inclusion (digital literacy, feature phone users, elderly population, health conditions) 12

4.2. User experience 12

4.3. Privacy concerns 13

4.4. Ease of implementation 13

4.5. Role of the payment system operator and other ecosystem actors 13

5. COUNTRY EXAMPLES 15

5.1. Brazil 15

5.2. Mexico 15

5.3. Pakistan 15

5.4. Thailand 16

6. CONCLUSION 17

7. ACKNOWLEDGMENTS 18

NOTES 19

1 SETTING THE CONTEXT

The World Bank has been monitoring closely the development of fast payment systems (FPS) by central banks and private-sector players across the globe. This comprehensive study of FPS implementations has resulted in a policy toolkit. The toolkit was designed to guide countries and regions on the likely alternatives and models that could assist them in their policy and implementation choices when they embark on their FPS journeys. Work on the FPS Toolkit was supported by the Bill & Melinda Gates Foundation under Project FASTT (Frictionless Affordable Safe Timely Transactions). The toolkit and other relevant resources of Project FASTT can be found at fastpayments.worldbank.org and consists of the following components:

1. The main report *Considerations and Lessons for the Development and Implementation of Fast Payment Systems*
2. Case studies of countries that have already implemented fast payments
3. A set of short focus notes on specific technical topics related to fast payments

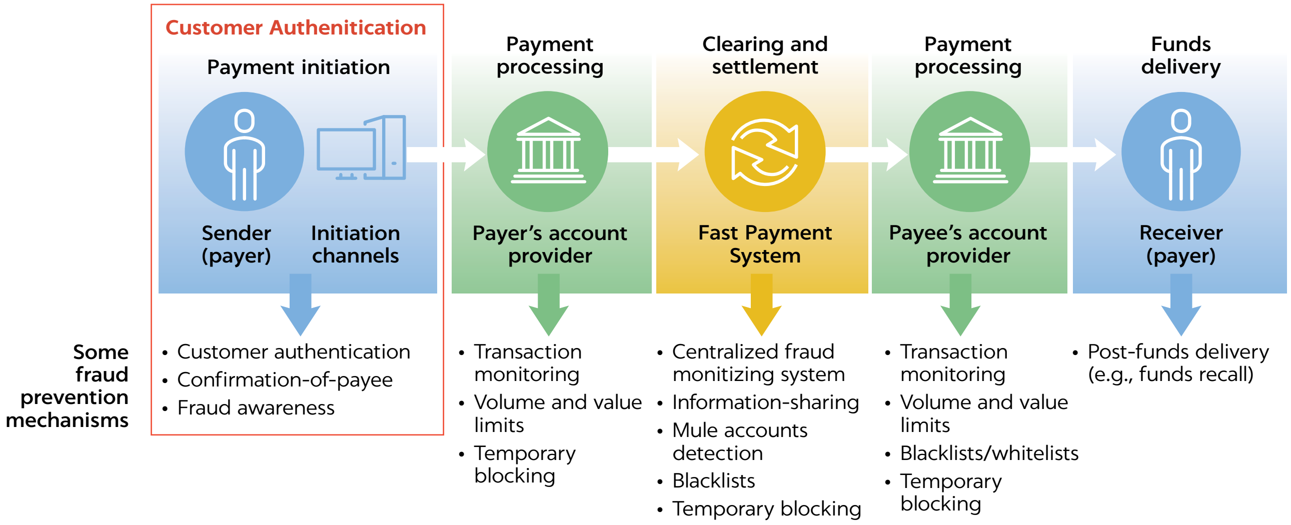
This note is part of the third component of the toolkit. It supplements the first note on customer authentication (published in September 2021) and aims to provide details on customer authentication approaches used in the context of fast payments (that is, factor-based, risk-based, and digital ID–based); outline the implementation challenges and considerations; and extract best practices and lessons learned from several country case studies.

2 BACKGROUND

Fast payment fraud can occur at any point during payment execution and affects the entire payment value chain. Fraud mitigation for fast payments therefore generally requires a holistic approach that covers payment initiation, payment processing, clearing, settlement, and post-funds delivery support.

Preventing fast payment fraud at the time of payment initiation and when accessing the associated transaction account has received particular attention in recent years, as fraudsters have become more adept at exploiting end users. The fact that end-to-end execution occurs within seconds makes it even more challenging to prevent fraud, compared to other payment methods. Industry actors also generally have less experience with detecting fast payment fraud compared to other payment methods that have been around longer, such as cards. For these reasons, account providers and system operators must have a clear strategy for implementing robust customer authentication as a fraud-prevention tool, both when authorizing payments and when providing access to payment accounts.

FIGURE 1 **Layers of Fraud Prevention along the Payment Value Chain**



Source: World Bank.

The World Bank previously published a technical focus note on trends in customer authentication that covered approaches used across the entire payment landscape. This new note provides an overview of authentication approaches that can be used in a fast payment context and weighs their benefits and disadvantages. It also develops a set of best practices for relevant actors with consideration given to security, inclusion, ease of implementation, user experience, and other aspects. Building on the previous note, it concludes with four additional country examples that show how customer authentication approaches for fast payments have been implemented in practice.

3 WEIGHING AUTHENTICATION APPROACHES IN A FAST PAYMENT CONTEXT

As online payment fraud has become more widespread, customer authentication methods have become increasingly sophisticated. Authentication methods are now generally tailored toward the channel being used for payment initiation and often vary with the type of payment instrument and the perceived riskiness of the transaction. There has also been a shift away from relying on rule-based approaches focused on a transaction's characteristics (for example, time of the day, value, location), with the industry moving toward more dynamic approaches that consider the user's characteristics and behavior. User-centric authentication methods often require additional data, factors, or elements to verify the user's identity more accurately; this must be balanced with maintaining the user's payment experience. A high level of friction at the time of payment can slow processing and lead the customer to abandon the transaction and perhaps future transactions with that payment method, service provider, or merchant.

The three main types of authentication approaches that can be considered in a fast payment context are **factor-based**, **risk-based**, and **digital identity-based authentication**. An overview of the three main approaches and their characteristics is presented in figure 2.

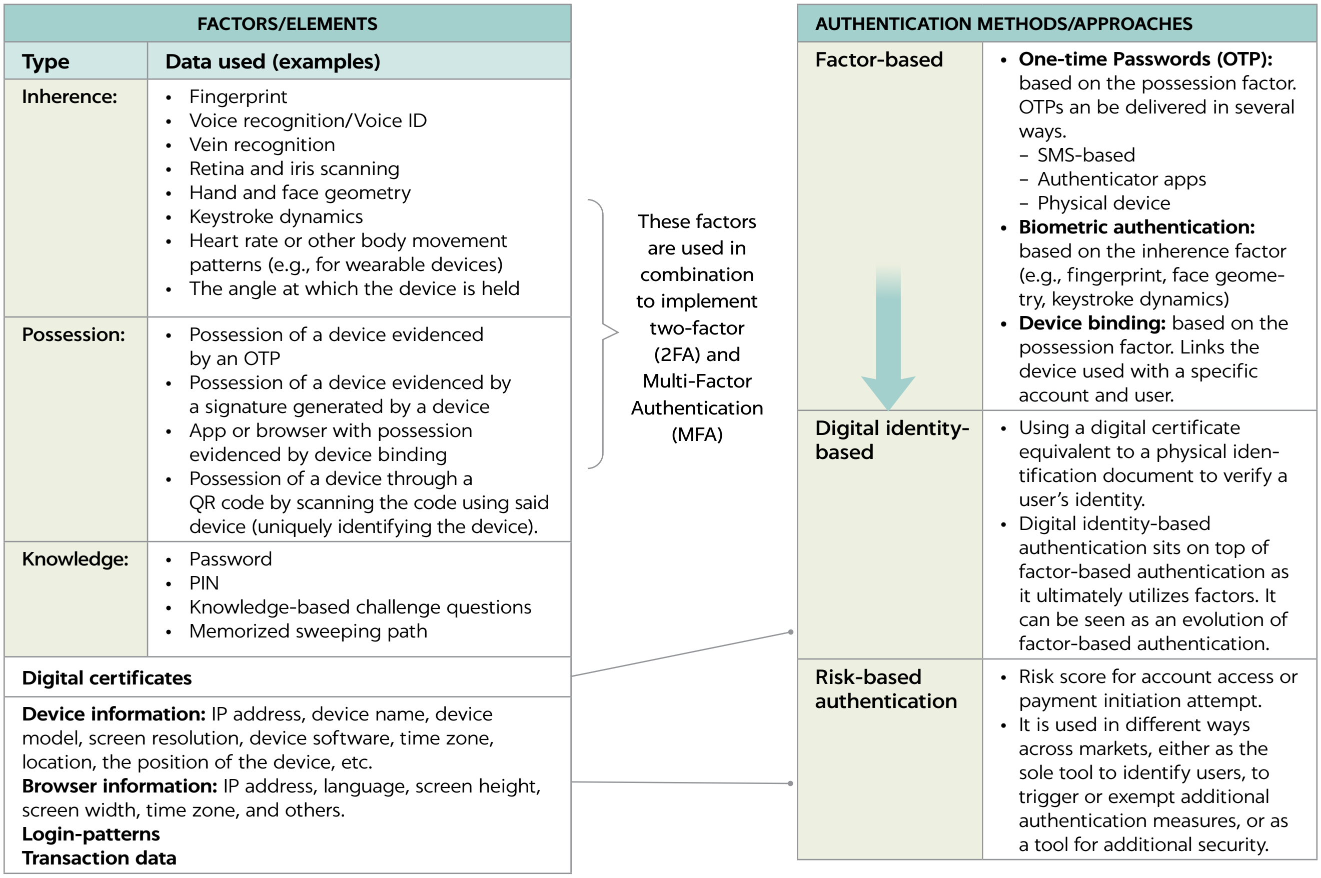
3.1 FACTOR-BASED AUTHENTICATION

Data elements used in factor-based customer authentication rely on factors provided by and/or about the end user to authorize the transaction. Such factors can include something the customer is (inherence), something the customer has (possession), and something the customer knows (knowledge). Different types of factors are often used in combination for increased security.

By combining multiple factors—that is, two-factor authentication (2FA) and multifactor authentication (MFA), wherein the breach of one does not compromise the reliability of the others—the risk of fraudulent activity is reduced. While any authentication approach that uses more than one factor increases security, it is thought that 2FA and MFA, which utilize factors from different and unrelated categories, provide a more secure system than a multilayered approach (where several factors from the same category are used—for example, password + PIN + knowledge-based challenge question). Many regulators and system operators consider implementing MFA to be a best practice for customer authentication in online banking and increasingly for fast payments.

Factors that are often used to authenticate fast payment users include one-time passwords, biometric factors, such as a fingerprint or facial recognition, and device binding. The advantages and disadvantages of each are discussed in detail below.

FIGURE 2 Taxonomy for Customer Authentication Approaches in Fast Payments



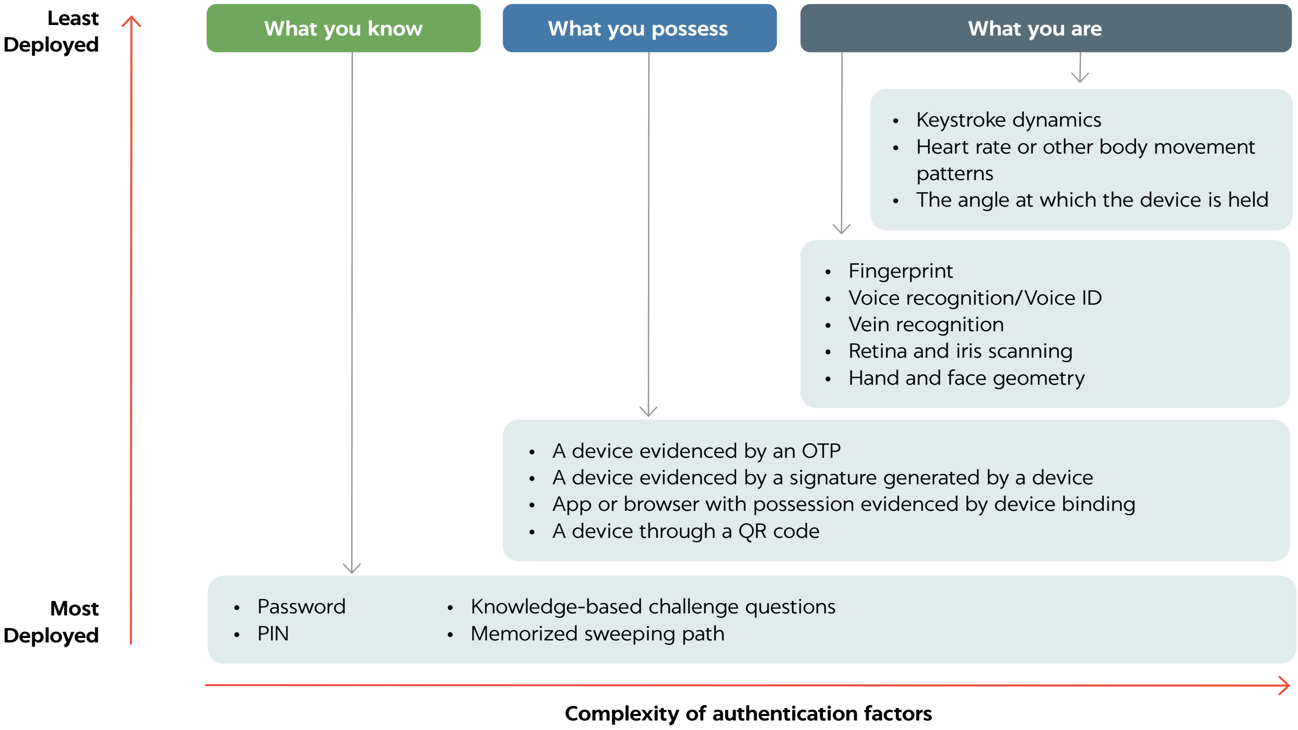
FACTORS/ELEMENTS	
Type	**Data used (examples)**
Inherence:	• Fingerprint • Voice recognition/Voice ID • Vein recognition • Retina and iris scanning • Hand and face geometry • Keystroke dynamics • Heart rate or other body movement patterns (e.g., for wearable devices) • The angle at which the device is held
Possession:	• Possession of a device evidenced by an OTP • Possession of a device evidenced by a signature generated by a device • App or browser with possession evidenced by device binding • Possession of a device through a QR code by scanning the code using said device (uniquely identifying the device).
Knowledge:	• Password • PIN • Knowledge-based challenge questions • Memorized sweeping path
Digital certificates	
Device information: IP address, device name, device model, screen resolution, device software, time zone, location, the position of the device, etc. **Browser information:** IP address, language, screen height, screen width, time zone, and others. **Login-patterns** **Transaction data**	

These factors are used in combination to implement two-factor (2FA) and Multi-Factor Authentication (MFA)

AUTHENTICATION METHODS/APPROACHES	
Factor-based	• **One-time Passwords (OTP):** based on the possession factor. OTPs an be delivered in several ways. – SMS-based – Authenticator apps – Physical device • **Biometric authentication:** based on the inherence factor (e.g., fingerprint, face geometry, keystroke dynamics) • **Device binding:** based on the possession factor. Links the device used with a specific account and user.
Digital identity-based	• Using a digital certificate equivalent to a physical identification document to verify a user's identity. • Digital identity-based authentication sits on top of factor-based authentication as it ultimately utilizes factors. It can be seen as an evolution of factor-based authentication.
Risk-based authentication	• Risk score for account access or payment initiation attempt. • It is used in different ways across markets, either as the sole tool to identify users, to trigger or exempt additional authentication measures, or as a tool for additional security.

Source: World Bank.

FIGURE 3 Overview of Factors Used for MFA



- Keystroke dynamics
- Heart rate or other body movement patterns
- The angle at which the device is held

- Fingerprint
- Voice recognition/Voice ID
- Vein recognition
- Retina and iris scanning
- Hand and face geometry

- A device evidenced by an OTP
- A device evidenced by a signature generated by a device
- App or browser with possession evidenced by device binding
- A device through a QR code

- Password
- PIN
- Knowledge-based challenge questions
- Memorized sweeping path

3.1.1 One-Time Passwords

A one-time password (OTP) is valid for a single account login or transaction. The benefit of using OTPs is that they are user-friendly and have been used outside the payments space for many years. Moreover, they are highly inclusive, as they can be delivered by SMS to users of feature phones. Authenticator apps, paper-based transaction authentication numbers, display cards, voice delivery, and other physical devices can also be used for this purpose. A best practice is to enable users to choose the delivery method for OTPs according to their needs.

While there are advantages of OTPs from the perspective of inclusion and user-friendliness, the use of OTPs is often thought of as less secure than other factors. This is because OTPs can be more vulnerable to "man in the middle" attacks, in which fraudsters intercept the OTP (via social engineering or other means) and manage to authorize transactions successfully. Combining an OTP with another factor can help reduce this risk. Another option is to minimize the time window over which the OTP is valid, because the shorter its time validity, the lower the risk of misuse. Nonetheless, the risk still exists.

BOX 1 AN ASSESSMENT OF OTP DELIVERY METHODS

SMS

In fast payments, SMS-based OTPs may be used as the second factor to authenticate users together with a password or other knowledge-based factor. As an example, in Pakistan's FPS Raast, users typically enter a six-digit OTP received on their registered mobile number to confirm and authorize a fast payment.[1] Besides being used to authenticate each individual transaction, SMS-based OTPs are often used to enroll users in mobile-based fast payment solutions.

One of the main reasons to use SMS-based OTPs is to promote inclusion, as they are not dependent on the type of phone used. However, SMS-based OTPs have become a less secure authentication method in recent years, as fraudsters have developed techniques to intercept OTPs delivered over mobile networks. In particular, SIM swapping has become prevalent in both advanced and developing economies. It involves an attacker fraudulently transferring a victim's phone number to their own SIM card, which can then be used to gain access to messages being sent to it. In addition to the user, other vulnerable elements in the payment value chain can be compromised, such as the telecom operator. This is not the case for other OTP delivery methods.

A best practice is to issue SMS OTPs with an expiration time, to increase security. In some markets, the regulator provides guidelines regarding the time validity of an SMS-based OTP.

Authenticator Apps

Authenticator apps work in a manner similar to an OTP delivered via SMS. The smartphone-based app generates a one-time code that can be used in conjunction with other factors to make a payment. The user must "pair" the app with their account in order for it to work. If the device is lost, the process must be repeated. Authenticator apps' OTPs are considered a proof of possession by the payer of the device on which the OTP was received or generated.

The benefit of authenticator apps is that the OTPs generated usually expire more quickly (in 30–60 seconds) than those delivered by SMS. Moreover, because the codes are not delivered over the mobile network, fraudsters cannot intercept them via techniques such as SIM swapping. However, it does require the sender of the payment to be a smartphone user and often requires account providers to rely on a third party for the generation of the code/OTPs.[2]

Physical Devices

OTPs delivered through paper-based transaction authentication numbers, display cards, or other physical devices have the advantage of being highly inclusive, as they are self-contained and do not require a mobile or smartphone. However, users must have the device on hand for authorizing transactions, and there is the risk of lost devices. Also, in some cases, they may have an expiration date after which they must be replaced. The cost and management of the tokens[3] may discourage banks and other payment service providers from considering this method. As with other forms of OTPs, the risks of successful fraudulent transactions are reduced if physical-device OTPs are implemented together with other types of authentication factors, such as those proving knowledge or inherence

TABLE 1 **Key Takeaways of OTPs**

OTP Delivery method	Benefits	Disadvantages
Benefits	• Inclusiveness, as it is not dependent on the type of phone. • Easy to use and generally, users are already familiar with the method.	• Fraudsters have developed techniques to intercept SMS-based OTPs.
Disadvantages	• OTPs usually expire more quickly than those delivered by SMS. • Fraudsters cannot intercept them via SIM swapping. • Cost efficient	• Potential user exclusion as its delivery is smartphone-based. • Benefit of the authenticator app depends on how the app is designed, and the binding of SIM and handset unique number.
Physical device	• Highly inclusive as they are self-contained and not dependent on a mobile or smartphone.	• Risks of the device being lost. • Hard-tokens often have an expiration date. • More expensive to manage and maintain than soft tokens.

Best practices for OTP implementations

Allow users to decide how to receive OTPs according to their needs

Reinforce OTPs with another type of factor

Minimize the time window over which OTPs are valid

Source: World Bank.

3.1.2 Biometric Authentication

Biometric authentication is based on the physical features of the user (for example, a fingerprint, the retina, voice, and so on), although it can also be performed based on an analysis of the user's behavioral characteristics (referred to as behavioral biometrics) . In jurisdictions that mandate the use of 2FA or MFA, behavioral biometrics are used to feed the scoring algorithms of authentication and fraud-prevention systems but are not legally recognized as an authentication factor per se. Despite this, the significance of behavioral biometrics is on the rise, as it is associated with enhanced user experience.

As described in the previous technical focus note on this topic (World Bank 2021b), the use of biometric authentication in payments is gaining traction in certain parts of the world due to the convenience, security, and accessibility associated with it. It allows a payment to be associated with a single identity, therefore reducing the possibility of contactless fraud and preventing users from transferring or delegating usage of banking services. Embedded fingerprint sensors have had increased use in the last few years, and most smartphones contain a camera and microphone that make biometric authentication convenient for smartphone users. Biometric authentication is quickly evolving, and innovative approaches are continuously entering the market. As an example, the banking industry in Australia has started to use voice recognition/voice ID for authentication in fast payments.[4]

Potential challenges of biometric authentication include privacy concerns related to criminal or commercial exploitation of user data (Federal Reserve 2021b), guaranteeing security for data handling, and ensuring that the user's enrollment process is accurate and that the data is reliable, including risks of forgery associated with deepfakes and AI technology. Regarding the latter point, obtaining high-quality fingerprints from certain population groups (for example, the elderly) may be difficult due to damaged fingerprint characteristics. In terms of behavioral biometrics, one concern is that fraudsters may be able to harvest biometric behavior data through nonpayment apps, with which (combined with personal information obtained through social engineering or data breaches) they can replicate a user's behavior in financial apps. Robust cybersecurity controls should therefore also be used to mitigate risks for biometric approaches, as they are used in other authentication approaches.

Other considerations with respect to the use of biometrics include the fact that the match between the stored template value and the live template value provided by the user at the time of authentication rarely achieves 100 percent due to differences in lighting conditions, angles of the biometric measurement, or differences between readers, to name a few. This means that biometric authentication uses a "score" to determine an acceptable accuracy level. This is distinctly different from authentication based on knowledge—for example, where, if there is no exact match of the password, PIN, or security question, the authorization request is rejected.

3.1.3 Device Binding

Linking a device with a bank account (that is, device binding) is an authentication method that is often used in cases where users have registered their phone numbers with account providers for alias-based fast payment services. In this instance, an OTP is delivered by SMS to the phone number registered with the account provider. At the time of payment initiation, the directory or alias service confirms that the user is utilizing the same device as the one it used to register with the service.

Device binding is commonly used as the possession factor together with either a knowledge or inherence factor. In India, when a Unified Payment Interface (UPI) transaction is initiated using a smartphone, the device fingerprint, such as the International Mobile Equipment Identity number or other unique technical detail, is considered as the first factor of authentication. The second factor (knowledge factor) is the UPI PIN, which must be provided manually by the user (NPCI, n.d.). In Mexico, account providers of the overlay service Codi must authenticate users and their device before submitting payments to SPEI, the country's Fast Payment System (FPS).

3.2 DIGITAL ID-BASED AUTHENTICATION

A digital ID can be defined as a set of electronically captured and stored attributes, factors, and/or credentials that uniquely identify a person (World Bank 2018). The attributes and authentication factors used in a digital ID may vary with the type of identity system. As an example, a digital ID may be composed of biographic data (for example, name, age, address), biometric data, or other attributes.

The development of various digital ID systems is being facilitated by rapidly evolving digital ID technologies.[5] Digital ID systems that meet high technological, organizational, and governance standards have the potential to improve trustworthiness, security, privacy, and convenience in multiple contexts, including for financial services. There is a wide spectrum of applications of digital IDs within financial services, from account-opening and customer due diligence processes to identity authentication for financial transactions. In this context, digital ID-based authentication is increasingly being used for user authentication in FPS. One example is in Sweden, where the widespread use of the alias-based overlay service Swish uses BankID to authenticate users prior to initiating real-time payments. See table 2 for additional examples.

Digital IDs can differ in the way they are implemented and may rely on different models, standards, and technologies. For example, they can be either centralized, such as the government-provided Aadhaar in India and the Authentication and Identity Verification System (SAVI) in Mexico (currently under development), or federated, such as those developed by the private sector in the Nordic countries (that is, by a consortium of account providers). Finland's Bank eID, Norway's BankID, Denmark's NemID, and Sweden's BankID are examples of digital IDs built through the cooperation of account providers (that is, bank consortiums).

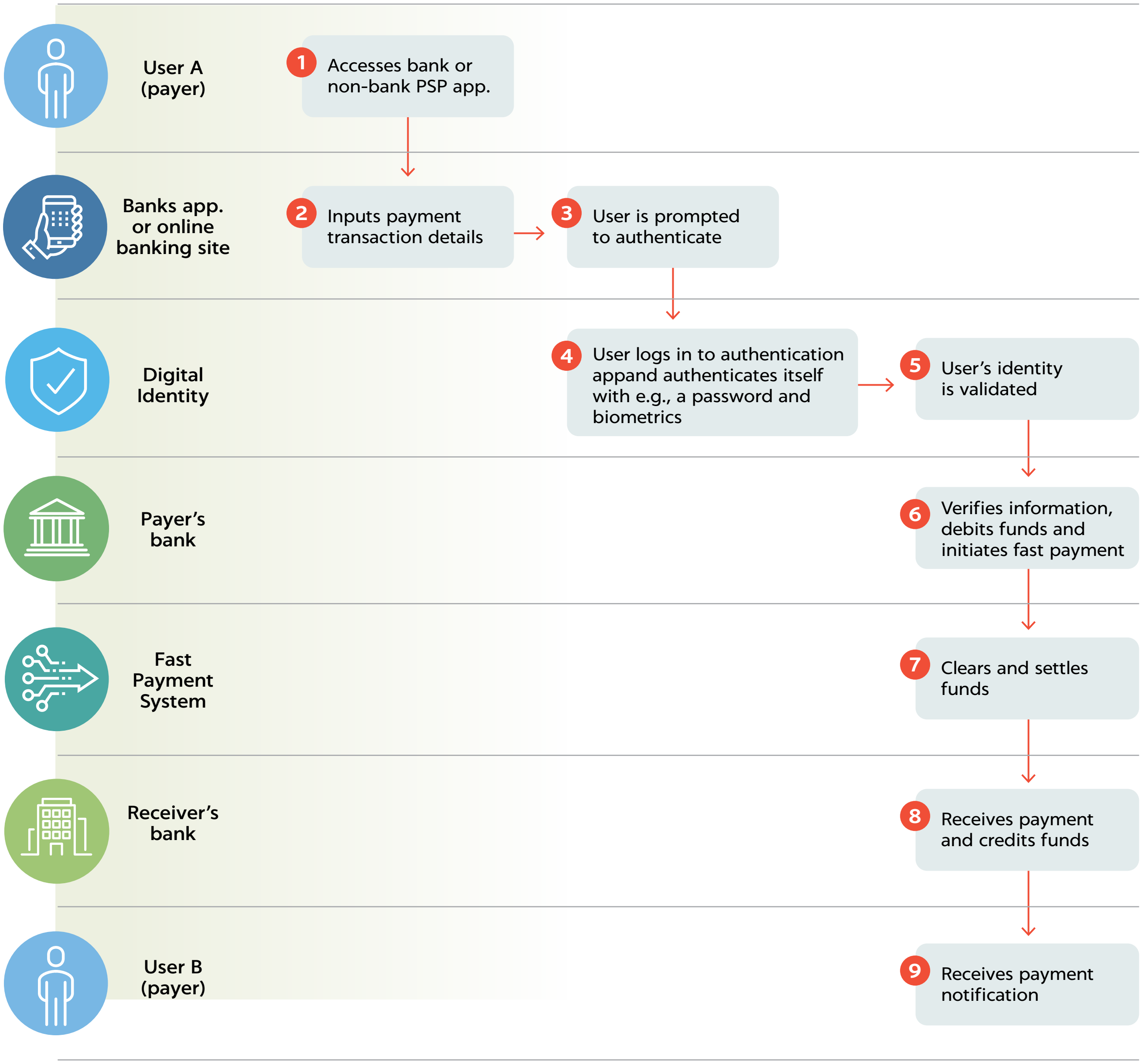
Digital ID-based authentication can be seen as an evolution of factor-based authentication, as it provides an additional layer of security and offers greater convenience, compared to 2FA and MFA.

While there are numerous benefits of using digital IDs for user authentication, implementation challenges and risks need to be addressed, such as the risk of excluding populations without smartphone access or network connectivity, privacy and data protection, and cost challenges for service providers associated with its implementation. If risk factors are not considered and suitable technology-based safeguards are not implemented together with effective governance and accountability measures, digital ID systems may be vulnerable to abuse by fraudsters, who could use them to create sham identities or exploit authenticators linked to legitimate identities.

Regulators are increasingly prioritizing data-privacy legislation in response to ongoing concerns about how identity-related information is processed and used amid increased digitalization. Digital ID systems must be backed by policies and regulations that prioritize data privacy and security and hold providers accountable. As an example, Europe's Electronic Identification, Authentication and Trust Services Regulation is currently being updated to provide access to secure digital ID solutions that can be used across borders, meeting user expectations and market demand. The regulation also seeks to establish a pan-European digital ID wallet.

There are many issues to consider when creating a new digital ID system. These include the type of entities involved (for example, governments, regulators, account providers, and consumer groups), the business model, the governance structure, the technology platform, and user education, to name a few. Regardless of the type of actor setting the digital ID scheme and the technology used, the scheme should be implemented based on user consent, and it should be transparent in the way that data is stored, shared, and verified. As with other authentication approaches, it is crucial for a digital ID system to possess robust security protocols and authentication mechanisms. These measures are necessary to guarantee that only the owner of the digital ID can gain access to it and to prevent misuse of personal information.

FIGURE 4 Example of Customer Authentication for Fast Payments with Digital ID


User A (payer)
Banks app. or online banking site
Digital Identity
Payer’s bank
Fast Payment System
Receiver’s bank
User B (payer)
1 Accesses bank or non-bank PSP app.
2 Inputs payment transaction details
3 User is prompted to authenticate
4 User logs in to authentication appand authenticates itself with e.g., a password and biometrics
5 User’s identity is validated
6 Verifies information, debits funds and initiates fast payment
7 Clears and settles funds
8 Receives payment and credits funds
9 Receives payment notification

Source: Adapted from Banxico 2021.

TABLE 2 Examples of Digital ID Solutions Used in Fast Payments

BELGIUM: **Itsme**	Itsme is a private-sector digital ID led by a consortium of Belgian account providers and mobile network operators. Itsme provides mobile-based authentication of identities that are linked to an eCard[6] and a specific mobile phone and SIM card. The service is being used by more than six million Belgians,[7] and its activation is tied to the ownership of a Belgian eID card, to assure proof of identity. For fast payments, customers can use Itsme to log in to their accounts and conduct transactions.
INDIA: **Aadhaar**	The government-implemented Aadhaar is the largest biometrics-based ID system in the world (Smart Payment Association 2018); more than one billion individuals are enrolled. Aadhaar is a 12-digit random number issued to the residents of India who satisfy the verification process laid down by the issuing authority. Aadhaar has many applications, but its use in the context of FPS is related to enrollment with UPI. To set up UPI, users need a bank account and a mobile number to link the account, as well as a debit card. If users have no debit card, they can also use their Aadhaar card for registering. In this case, the user's data is retrieved from the Unique Identification Authority of India once the user provides the Aadhaar number at the time of registration. Then the user will receive an OTP at the phone number registered with Aadhaar, which must be the same one used to register with the account provider. After successful verification, users can create their virtual payment address, which they use to make payments via UPI.
MEXICO: **SAVI**	Banxico, Mexico's central bank and operator of its FPS, SPEI, is developing and will operate the Authentication and Identity Verification System (SAVI). SAVI is being developed partly in response to increased rates of financial fraud and in anticipation of third-party payment initiation through SPEI. SAVI is envisioned as a centralized registry of end users' personal information (including biometrics, national ID documents, contact details, and others) and transactional information. For fast payments, SAVI will enable identity verification for payments initiated by third parties prior to payment submission to SPEI through the user's biometrics.
SWEDEN: **BankID**	BankID, a digital ID-management system developed by the Swedish banking community, currently holds more than eight million users.[8] BankID is based on the issuance of a digital certificate also known as a public key certificate. The associated mobile app stores a cryptographic key that acts to verify the user's identity when making a Swish payment. A digital certificate is a cryptographic tool used to link a public key to its owner. Using a digital certificate has the benefit of being highly secure and convenient. BankID's use for fast payments relates to customer authentication when using Swish. Swish requires users to log in to the BankID app (with their biometrics) to make and receive payments.

3.3 RISK-BASED AUTHENTICATION

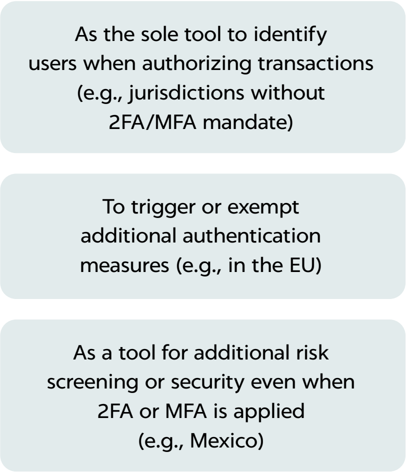
Risk-based authentication (RBA) relies on transactional data (for example, location, device, user profile, log-in patterns, and others) to authenticate the user. The data serves as an input for assigning a risk score that can be used to identify risky or low-risk transactions and trigger additional authentication measures, if needed.

RBA is common in markets without a nationwide regulatory mandate to implement 2FA or MFA for online banking. However, relying only on RBA may pose risks. For example, sophisticated fraudsters may be able to detect how systems calculate risk scores and then attempt to manipulate data elements to keep the score low.

Another consideration is that the thresholds for declining transactions may vary by account provider, leading to inconsistencies in the level of security and user experience. There may also be privacy concerns related to the exploitation of the user's data for commercial purposes.

In markets where 2FA or MFA is mandated, RBA is used as a tool for additional screening or security. In Mexico, the regulator has mandated that account providers consider the user's geolocation for allowing access to online banking services, while in the European Union, risk analysis (known as transaction risk analysis) is used as an input when deciding whether to apply strong customer authentication (SCA)—that is, it is used to trigger an exemption for SCA.[9]

FIGURE 5 Uses of Risk-Based Authentication



As the sole tool to identify users when authorizing transactions (e.g., jurisdictions without 2FA/MFA mandate)

To trigger or exempt additional authentication measures (e.g., in the EU)

As a tool for additional risk screening or security even when 2FA or MFA is applied (e.g., Mexico)

Source: World Bank.

3.4 COMPARISON OF DIFFERENT AUTHENTICATION APPROACHES

Each authentication approach described above has benefits and disadvantages that should be considered in terms of security, ease of implementation, and user experience. Factor-based authentication, specifically 2FA or MFA, is highly secure since the factors utilized are unrelated and from different categories. However, the ease of implementation and user experience can vary greatly. As an example, MFA that requires the user to provide a knowledge factor, such as a password, in addition to an OTP delivered via SMS may affect user experience, as both of those factors must be provided by the user manually. On the other hand, utilizing biometrics together with device binding requires no data input from the end user. When it comes to ease of implementation, clear regulatory guidance, the availability of proper technology, account provider and merchant readiness, and clear communication to the end user are all needed to help the industry prepare and implement MFA.

RBA is often less secure than other approaches when implemented alone to authorize transactions, as it relies more on characteristics of the device used and the transaction details than on a combination of the user's characteristics, behavior, knowledge factors, and so on. However, user experience is regarded as positive, as RBA requires less interaction from the end user and is less perceptible throughout the authorization process.

Digital ID-based authentication is perceived as the approach with the highest implementation complexity, given the number of actors and systems likely to be involved, the possibility that regulation will need to be updated or created, and the likely costs associated with securely collecting and maintaining user's attributes. Nonetheless, this method is generally considered the most secure and provides a positive user experience.

TABLE 3 **Comparison Matrix of Authentication Approaches**

Authentication methods/ approaches	Country examples	Security	Complexity of implementation	User experience
Factor-based (specifically, 2FA or MFA)	EU UK Mexico India Pakistan	Medium to High (depending on the type of factors used)	Can vary depending on whether there is clear regulatory guidance, technology availability, account provider and merchant readiness, and user awareness.	Can vary depending on the factors employed. Knowledge-based factors may result in increased user friction, while biometric factors often offer a more positive experience.
Digital identity-based	Sweden Norway Belgium	High	High	Positive
Risk-based authentication	US* Canada	Low (when implemented alone as the sole authentication approach)	Low	Positive

Source: World Bank.

*Participants in the Clearing House's real-time payment system are mandated to implement MFA to authenticate their customers, though not explicitly for every transaction. See TCH 2017.

4 BEST PRACTICES AND CONSIDERATIONS

When deciding on the types of authentication approaches to use in a fast payment context, it is important to consider issues related to inclusion, user experience, privacy, ease of implementation, and the degree of support required from various ecosystem actors. This section details considerations that regulators, central banks, payment system operators, account providers, merchants, and technology providers should keep in mind when implementing customer authentication approaches for fast payments. There is no "right" authentication approach, and trade-offs must occur. Ultimately, choices will vary by market.

4.1. INCLUSION (DIGITAL LITERACY, FEATURE PHONE USERS, ELDERLY POPULATION, HEALTH CONDITIONS)

The approaches used for customer authentication can pose challenges to customers who lack digital literacy or familiarity with certain technologies. In some markets, the exclusion of the less tech savvy and/or elderly populations can occur through the sole use of authentication approaches based on smartphones and inherence factors.

Inclusion has been a key topic of discussion among markets that have already implemented MFA, such as the United Kingdom and European Union.[10] UK Finance (the United Kingdom's trade association for the banking and financial services sector) provides recommendations for authentication options that are suited for users with certain conditions. As an example, knowledge-based factors may not be the most appropriate for users with cognitive issues.[11] In the European Union, the European Banking Authority proposes to introduce a general provision requiring bank and nonbank payment service providers (PSPs) to consider the needs of different groups, including vulnerable groups, in the provision of authentication solutions, and to enhance awareness of authentication solutions. All actors in the payment value chain should offer a range of options for customers to authenticate themselves that address a variety of user conditions and population groups, regardless of age, disability, health condition, the type of device used (smartphone versus feature phone), and financial education, to name a few.

4.2. USER EXPERIENCE

Studies have shown that non-adoption of MFA by users (when given the choice) stems from a lack of clear instructions and tool knowledge, inaccurate risk perception, and user overconfidence when it comes to security risks. If a transaction is too security driven, it may deter customers from completing the transaction and, when implemented in the consumer-to-business context, decrease conversion rates. In some markets (such as the European Union), delegated authentication, wherein authentication is performed by the merchant/business (that is, the payee), is being adopted to improve the user experience for consumer-to-business transactions.

In the context of fast payments, user convenience may be hampered if overly onerous customer authentication measures are implemented. For this reason, it is critical for organizations to strengthen authentication mechanisms while paying adequate attention to maintaining the customer experience.

Implementation of MFA approaches should be accompanied by clear communication to end users; low-friction authentication such as biometrics should be utilized when appropriate; complex authentication methods or those that rely on a knowledge factor that can be forgotten should be avoided; and users' contact information should be kept up to date.

4.3. PRIVACY CONCERNS

Consumers value their privacy and are aware of the risk that their personal data may be compromised in the digital environment. When it comes to utilizing personal information of any kind for customer authentication, having a strong privacy framework is a prerequisite. When designing and implementing customer authentication approaches, privacy and data protection should be considered at every stage. This involves, among other things, limiting the collection, use, and storage of data to the minimum necessary for secure and successful authentication. When notice is provided to users, it should be clear, accurate, and unambiguous.

Approaches relying on inherence factors (for example, biometrics) may increase data-privacy concerns, as some users may not be comfortable due to the lack of national data-privacy regulations. For example, unlike passwords, which can be changed after hacking, inherence factors generally cannot be changed. To alleviate users' concerns regarding the use of their biometric data and their privacy, the following measures can be taken: ensuring transparency throughout the enrollment and operational processes, providing users with control over their data, ensuring that biometrics are used only for the purpose of authentication, implementing proper security controls to prevent unauthorized access, and raising awareness of the advantages of biometric authentication.

4.4. EASE OF IMPLEMENTATION

In some markets, access to online banking and online payment initiation is permitted by regulatory mandate or guidance only after the application of MFA. The general objectives are to improve cybersecurity and reduce the risk of fraud by mandating and standardizing the application of "strong customer authentication" approaches. Countries such as Bahrain, India, Mexico, Pakistan, Thailand, and the United Kingdom, and countries that are part of the European Union, to name a few, all mandate some form of MFA. Markets without a regulatory mandate to implement MFA may experience an uneven adoption of authentication approaches and a varying degree of authentication security among PSPs. This may ultimately affect the perceived security of fast payments.

MFA mandates bring about benefits in terms of homogenous and widespread use of authentication approaches, but there are implementation challenges related to a lack of clear guidance from regulators, merchant onboarding, technology requirements, costs, and end-user education. Both the United Kingdom and European Union extended the deadline for implementing SCA due to, among other reasons, regulatory uncertainty and concerns about merchant readiness (mostly related to card transactions). Clear regulatory direction, including guidance about specific elements that could be used within the knowledge, inherence, and possession factors, can help ease implementation issues. Promoting user awareness and making sure that the required technology is available to support implementation is also important. In a cross-border context, there may also be challenges due to the lack of harmonization of authentication standards across different markets.

Markets with successful implementations of MFA at a national level have followed migration plans set in collaboration with the banking industry to ensure that key milestones are met and specific metrics are used when reviewing the implementation progress. As an example, UK Finance led the United Kingdom's SCA migration plan and developed the specific metrics to use when reviewing implementation progress. Similarly, the Dutch Payments Association proved helpful in coordinating activities across ecosystem actors in the Netherlands, developing messaging and communications and resolving industry-wide issues.

4.5. ROLE OF THE PAYMENT SYSTEM OPERATOR AND OTHER ECOSYSTEM ACTORS

Account providers can implement customer authentication approaches as required by regulation or the payment system operator, either independently or with the use of tools and solutions provided by governments, central banks, or private-sector entities. As previously described, Banxico plays a great role in providing identity-verification solutions, which account providers can leverage to conduct customer authentication processes. In other markets, such as in Sweden and Belgium, a consortium of account providers developed a solution to enable customer authentication with digital IDs. That said, in most markets, account providers alone carry out all aspects of customer authentication without the support of central bank–, government-, or consortium-developed tools/solutions.

Banxico's SAVI (currently under development) shows a model in which the central bank as the payment system operator is involved in facilitating customer authentication through a centrally held biometrics database, leveraging its central position in the payment value chain and as a trusted authority in assuming data-protection responsibilities. However, all markets have different payment ecosystem arrangements, where the central bank may play no role in payment system operation. In other markets, cooperation within the banking sector plays a relevant role in providing industry-wide solutions that all actors can leverage.

BOX 2 CUSTOMER AUTHENTICATION AND LIABILITY

In some jurisdictions, the application of 2FA or MFA is also relevant for determining liability for fraudulent transactions. In the European Union, the Revised Payment Services Directive (PSD2) states that, in the case of an unauthorized payment, the payer's PSP refunds the payer the amount of such transaction. According to the PSD2, where the payer's PSP does not require SCA, the payer shall not bear any financial losses unless the payer acted fraudulently. Where the payee or the PSP of the payee fails to accept SCA, it must refund the financial damage caused to the payer's PSP.

In this context, unless the payer acted fraudulently, the payer's PSP is liable to the payer for transactions carried out without SCA. If the PSP of the payee triggers an SCA exemption and the transaction is carried out without an SCA, the payee's PSP will be liable to the payer's PSP for the financial damage caused. Regardless of the liability shift between the payer's PSP and the payee's PSP, the payer is not held liable whenever SCA is not used and there is a case of fraud. Similarly, account providers in Mexico are obliged to reimburse consumers for the losses of a fraudulent transaction when 2FA (as mandated by the financial regulator) is not implemented.

5 COUNTRY EXAMPLES

5.1. BRAZIL

The Central Bank of Brazil is one of the four regulators within the Brazilian financial sector, as well as the scheme operator and regulator of the country's FPS, Pix. Each participant in Pix is responsible for ensuring secure customer authentication. Nonetheless, the central bank recommends (but does not mandate) the use of MFA mechanisms, including biometrics.[12]

In this context, each Pix participant is responsible for choosing the specific customer authentication methods for Pix transactions. The lack of a mandate has created flexibility in terms of implementation but has also led to a lack of clarity among participants. Moreover, small institutions may lack the knowledge or ability to implement robust customer authentication methods, in comparison to larger and more established institutions.

5.2. MEXICO

Mexico's financial-sector regulator, the Comisión Nacional Bancaria y de Valores (CNBV), mandated financial institutions to implement 2FA for accessing and authorizing electronic transactions (not only fast payments but also other types of payments). Starting in 2021, users of online banking services were required to allow banks to access their geolocation data in order to use online banking services.

CNBV is prescriptive about what elements and factors can be used to authenticate users and provides details, such as the maximum time that an OTP can be considered valid, restrictions on the length and content of user's passwords, and the mandatory use of either OTPs or a biometric factor for authorizing payments, among other specifications.[13] In addition, within the FPS's participation rules (that is, SPEI), the system operator Banxico reinforced such regulation by calling for all participating entities submitting payments to SPEI to implement 2FA prior to payment submission.

Banxico plays a crucial role in the payment ecosystem, as it regulates and operates the FPS. To this end, Banxico is working on developing new functionalities to support the growth and security of fast payments. One example is SAVI (defined as a central registry of users' biometric, biographic, and transactional data), which will help account providers conduct biometric validation prior to payment initiation in SPEI. The data held within SAVI will include biometrics, social security numbers, and other biographic data (for example, name, gender, birth date, and so on), users' IDs, and contact details. With SAVI, account providers will be able to validate their users' biometrical information against the information stored in SAVI.

5.3. PAKISTAN

The State Bank of Pakistan fulfills multiple roles, including that of regulator and payment system operator. It is the owner and operator of the recently launched[14] FPS, Raast. The bank mandated the use of MFA for clients accessing banking products, and biometrics are mandatory in some cases (such as for fund withdrawals) . When it comes to fast payments, account providers verify the user's identity prior to initiating payments through a six-digit OTP delivered via SMS. In addition, customer authentication via mobile phone verifies the validity of an end user using the International Mobile Equipment Identity number. Account providers were advised by the State Bank of Pakistan to take all necessary measures to protect customer transactions while ensuring that the user experience remains smooth, with minimum hassle, to encourage the adoption of Raast. In this regard, account providers were encouraged to use more proactive and user-friendly measures, instead of cumbersome techniques, such as requiring passwords received via multiple channels at the time of the transaction.

5.4. THAILAND

The Bank of Thailand[15] mandates MFA for all electronic payments, including fast payments (that is, PromptPay transactions). The use of biometrics will become mandatory[16] for transactions above B 50,000. For PromptPay, account providers typically use a combination of OTPs and fingerprint/facial recognition for authenticating their users.

When it comes to the use of biometrics, the Bank of Thailand issued guidelines (specifically relevant to facial-recognition technology) allowing financial institutions to test their solutions safely in the bank's regulatory sandbox. In parallel, the Thailand Revenue Department, together with the bank, commercial banks, and the National Digital ID Company Ltd., developed a digital ID system called the NDID Platform.[17] However, the key use case for NDID is the opening of bank accounts, though its use cases have been expanding.

TABLE 4 Comparison Matrix of Customer Authentication Approaches in Selected Countries

	What Method(s) Are Used?	Is MFA Mandated?	What Is the Role of the System Operator?	Is an Ancillary Authentication Service Used?
Brazil	MFA	No	Endorses MFA as the most secure method but is not prescriptive	No
Mexico	2FA/MFA, geolocation, and digital ID (under development)	Yes. Scheme operator also mandates its implementation for all FPS participants.	Mandates 2FA and is currently developing tools for identity validation	Yes (SAVI)
Pakistan	MFA with SMS-based OTP	Yes. Scheme operator also mandates its implementation for all FPS participants.	Mandates 2FA/MFA and relies on account providers to comply	No
Thailand	MFA	Yes	Mandates 2FA/MFA and relies on account providers to comply	No

Source: World Bank.

6 CONCLUSION

Regulators and system operators widely recognize the implementation of MFA as a best practice for authenticating customers in online banking and, increasingly, for FPS. OTPs are commonly used as an authentication factor because they are highly inclusive, cost-efficient, and user-friendly, but they are proven to be less secure, as fraudsters have learned to intercept them, especially when delivered via SMS. Combining OTPs with another factor, enabling users to decide how to receive OTPs, and minimizing the validity of OTPs are all best practices. The use of biometric authentication is growing due to the convenience, security, and accessibility associated with it. Digital IDs may be seen as an evolution of factor-based authentication and have the potential to improve trustworthiness, privacy, security, and convenience.

While in many markets, account providers alone carry out all aspects of customer authentication, there are also jurisdictions where the central bank, government, or an industry consortium develops tools and solutions to help account providers conduct robust customer authentication. Such tools have the potential to harmonize the security and user experience associated with customer authentication by enabling account providers access to the same technology.

When implementing customer authentication approaches, all actors in the payment value chain should address a variety of user conditions and population groups; pay adequate attention to maintaining the customer experience; and accompany the implementation of MFA with clear communication to end users, an industry implementation plan, and a strong security and privacy framework. The advantages and disadvantages of each authentication approach must be weighed. Ultimately, each market needs to adopt a tailored approach that works for its market.

7 ACKNOWLEDGMENTS

Organization	Contributor
Lipis Advisors	Lipis Advisors
World Bank	Harish Natarajan
	Holti Banka
	Nilima Ramteke
	Thomas Piveteau
	Andrea Monteleone

NOTES

1. Bank of Punjab, Habib Bank, Standard Charter, and Dubai Islamic Bank have all implemented OTPs for Raast users.
2. As an example, Deutsche Bank developed its own "Secure Authenticator."
3. They require a token-management system with appropriate levels of controls and administration (Federal Reserve Bank of Atlanta 2015).
4. Such as the Australia and New Zealand Banking Group Ltd.
5. A digital ID system refers to the systems and processes that manage the life cycle of individual digital identities (World Bank 2018).
6. The eID is the electronic ID card issued to all Belgians over the age of 12.
7. Itsme.
8. BankID.
9. For more details on the European Union's SCA and the available exemptions. see World Bank, 2021. See the previous note on customer authentication for further explanation of SCA and its application of RBA.
10. For the European Union, see EBA 2022.
11. For more details, see UK Finance 2020.
12. The Central Bank of Brazil has decided not to regulate the use of particular authentication measures, as it deemed that ecosystem participants already carry out relatively effective user authentication.
13. See CNBV 2023 for the specific authenticator factors considered as valid by the regulator.
14. Launched in 2022.
15. Which regulates PromptPay.
16. Starting June 2023.
17. NDID, National Identity for All, https://www.ndid.co.th/.

WORLD BANK GROUP