FOCUS NOTE

CUSTOMER AUTHENTICATION IN PAYMENTS

Part of the World Bank Fast Payments Toolkit

SEPTEMBER 2021

WORLD BANK GROUP

CONTENTS

FINANCE, COMPETITIVENESS & INNOVATION GLOBAL PRACTICE

Payment Systems Development Group

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

1 SETTING THE CONTEXT

The World Bank has been monitoring closely the developments of fast payment systems (FPS) by central banks and private players across the globe.[1] 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 and Melinda Gates Foundation. The toolkit 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 and aims to provide inputs on customer authentication. As the use of digital payments increases around the globe, safe and reliable authentication mechanisms to enhance security and prevent fraud have been increasing in importance. The set of features covered in this note are present across the entire payments landscape, including card and online transactions.

2 BACKGROUND

Authentication is the means to recognize a customer's identity. It is the process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.[2] For example, each time we use a key to open a door, we authenticate ourselves to the space we are entering through possession of the key. Individuals authenticate themselves multiple times every day. The use of a password is the most common form of authentication, but only a limited number of individuals have separate passwords for different accounts, while others often use two to three passwords among their multiple accounts. This has led to concerns that a miscreant might gain access to one password and then log in to multiple different accounts. In banking, authentication is the process that a bank or payment service provider (PSP) uses to establish that people really are who they say they are. It aims to make sure that the person requesting access to an account, or trying to make a payment, is either the account owner or someone to whom the account owner has given consent.

There are many different types of customer authentication,[3] including the use of an authentication code (an identifier used to verify identity or validate the authenticity of data), data authentication (the process of confirming the origin and integrity of data), multifactor authentication (the process of verifying identity using at least two independent factors, such as a personal ID number, password, or security tokens), digital identity (a number, code, or collection of attributes used by information technologies to identify entities), and strong password, among others. The use of multifactor authentication has been enabled by the proliferation of smartphones that produce both biometric and possession factors. Multifactor authentication increases the reliability of the authentication process.

There is an inherent trade-off between customer authentication and customer convenience. For example, one of the main issues with respect to customer authentication in the context of e-commerce transactions is shopping-cart abandonment, where the consumer stops purchasing goods when it comes to the authentication stage of a purchase because the process is too long, complex, or cumbersome or the customer is not sure what needs to be done. Hence, it is essential to strike a balance between security and usability. The effectiveness and reliability of authentication credentials depend on their ability to withstand data breaches from cyberattacks or other means, man-in-the-middle attacks, and social-engineering attacks, among others. Strong customer authentication (SCA)[4] (authentication standards using multiple factors) is increasingly becoming a critical requirement for financial transactions and notably for fast payment services.

In addition to multifactor authentication, risk-based authentication (RBA)[5] is also prevalent, where the associated risk of a transaction is assessed based on factors such as the amount of the transaction, location, and type of operation, and the level of authentication needed is determined accordingly.

As more third-party providers centralize their account information and payment options on a single device, the need for a general-purpose authentication mechanism that is not tied to a particular banking or payment relationship is gaining attention.

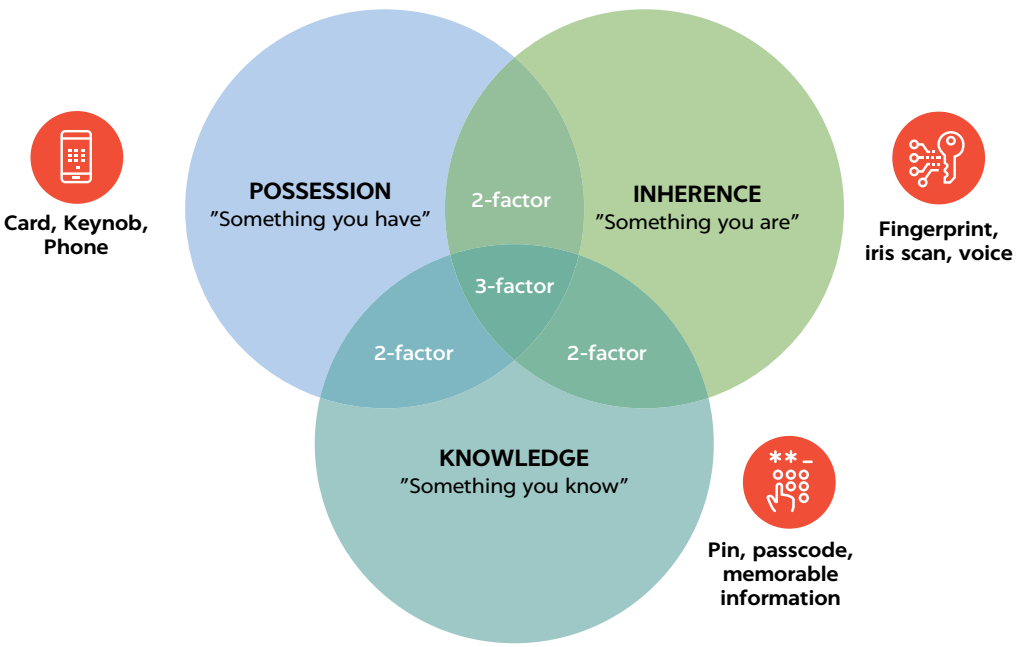
3 CUSTOMER AUTHENTICATION IN FAST PAYMENTS

In a fast payment context, payment authentication and authorization include the steps of a transaction where customers confirm who they claim to be (authentication) and are granted permission for the transfer (authorization).[6] Given that most fast payment systems have settlement finality and that, once processed, a transaction cannot be reversed, customer authentication becomes critical. Typically, fast payments include two-factor authentication, wherein the two factors are typically a combination of the three factors described in the European Union's SCA.

The use of biometrics[7] in sender authentication is also becoming increasingly common. Whether a transaction is initiated by the payer or the payee, authentication typically takes place at the payer's end. This has been depicted in the transaction flows mapped in figure 2.

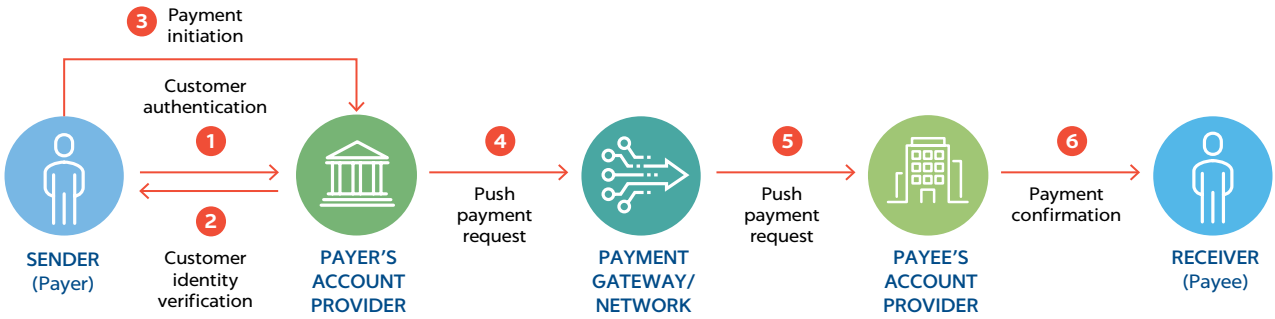
For a typical push payment, the customer uses one or more factors of authentication, after which the payment is initiated. The critical elements that identify the payer travel to the payer's institution for authentication of the payer, followed by authorization of the payment transaction.

FIGURE 1 **Factors of Strong Customer Authentication**



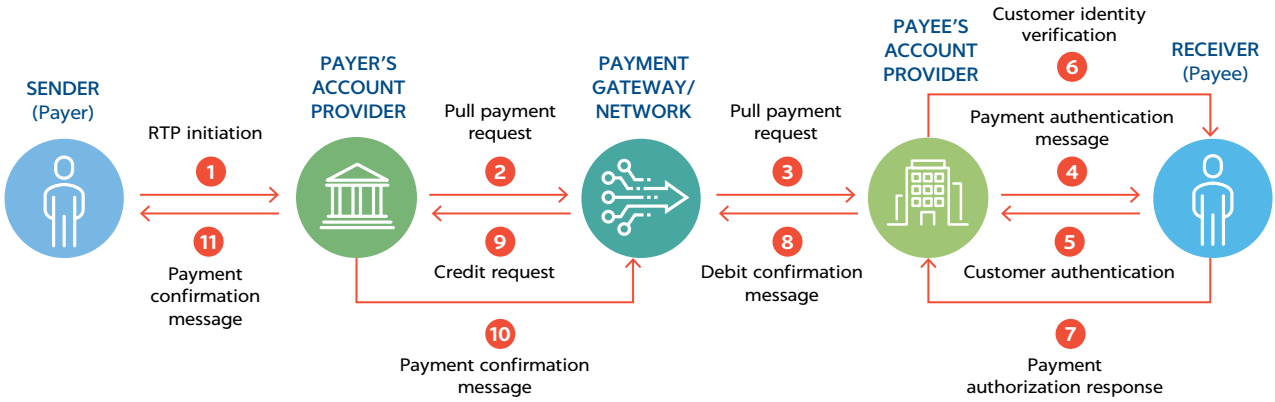
Source: Own elaboration

FIGURE 2 **Customer Authentication in a Typical Push Transaction**



Source: Own elaboration

FIGURE 3 **Customer Authentication in a Typical Pull Transaction**



Source: Own elaboration

Following this, the authorized payment request flows from the payer's account provider, through the payment gateway/network, to the payee's account provider, which goes on to credit the payee's account.

For a typical pull payment—request to pay, in this case—the initiator of the payment (payee) does not authenticate itself, and the customer authentication takes place at the payer's end using one or more factors of authentication. Here, after the payee initiates the request to pay, the pull payment request flows from the payee's account provider, through the payment gateway/network, to the payer's account provider, which goes on to debit the payer's account after authenticating the payer. Following this, the payer's account provider sends the debit confirmation message to the payment gateway/network, which sends the credit request to the payee's account provider. Once the payee's account provider credits the payee's account, a confirmation message is sent back to the payment gateway/network and the payee. There are instances where third-party application providers are also involved from the payer and/or payee perspective.

4 NEW TRENDS IN AUTHENTICATION

There are multiple innovations in the authentication space, including the consumer device cardholder-verification method (CDCVM), FIDO Standards, GSMA's Mobile Connect, OAuth 2.0, and OpenID Connect. While these new trends are not being used in fast payments, they might be relevant as fast payments evolve.

4.1 CONSUMER DEVICE CARDHOLDER-VERIFICATION METHOD

The cardholder-verification method (CVM) is used to evaluate whether the person presenting a payment instrument, such as a payment card, is the legitimate cardholder. As mobile devices are used more and more to make payment transactions, consumer authentication is being performed on the consumer's own device via passcodes, passwords, patterns, and biometrics, such as fingerprints, iris scans, and voice and face recognition. This type of authentication on a consumer device, which is an enhancement of CVM, is known as CDCVM (for consumer device CVM). Additionally, when multiple payment applications on the device share the same CDCVM and the associated result, it is referred to as shared CDCVM.

CDCVM was not initially considered as a CVM because issuing banks or PSPs had no way to confirm that the authentication process on the cardholder's device was secure. CDCVM can be supported using biometrics in the following three ways:

- Biometric validation at the point-of-sale level (biometric at POS),[8] wherein biometrics are captured at the point of sale and verified against the previously captured biometric template stored on the card's chip or transmitted as part of a payment-authorization message for verification by the issuer. EMVCo has updated its contact specifications to support it.
- Biometric validation, where authentication is carried out at the level of the cardholder's phone and is supported by the phone operating system and hardware (known as CDCVM). EMVCo has developed a process to evaluate software-based mobile-phone security (which includes the security of CDCVM). In addition, it has defined industry best practices to address functional and performance considerations and is creating a central mechanism to identify a CDCVM solution. EMVCo also works closely with the FIDO Alliance on CDCVM functional evaluation.
- Biometric validation on card, which is not addressed by this document.

According to the Apple website, for contactless Apple Pay EMV® transactions, CDCVM is performed and verified entirely on the iOS device or on an Apple Watch. CDCVM is SCA compliant.

4.2 FIDO STANDARDS

The FIDO (Fast Identity Online) Alliance is an open industry association working toward promoting authentication standards that allow for passwords to be replaced by interoper-

able, secure, and fast authentication methods and eliminate friction for consumers.

From a security perspective, FIDO standards are based on public-key cryptography and require no shared secrets. In other words, all sensitive data remains on the consumer's device, so if there is a data breach in the issuer's system, there is no authentication-related information to steal. Details on the FIDO specifications have been included below.

- **FIDO Universal Authentication Framework:** A whole solution to enable a consumer's device to become an authentication mechanism. Consumers can register their device to a service and use the relaying party's selected authentication method to access services or make a payment.
- **Universal Second-Factor Authentication (U2F):** Designed to improve a user's existing authentication flow by adding a strong second factor (for example, the use of a USB dongle for authentication, in addition to a password). The U2F specification is now part of FIDO2.
- **FIDO2:** Consists of W3C's WebAuthn API, which is built into platforms and browsers, and CTAP (client-to-authenticator protocol), which enables external authenticators, such as USB keys or mobile phones, to create a password-less or multifactor experience using USB, Bluetooth Low Energy, or near-field communication.

FIDO standardizes device-server authentication by converting user devices into a means of authentication. Users initiate an authentication session by presenting their device and may be required to enter some form of verification (for example, a PIN or biometrics) to unlock the user's device. A different public and private key are created for each combination of service provider (online service), device, and user account with the online service. The public key is stored in the online service, and the private key is stored in the user's device. Authentication is performed by a challenge-response mechanism wherein the online service generates a challenge, and the device applies the relevant private key to sign the challenge for validation, using the user's public key for the device service registered with the service provider. That makes the server independent from the local device and reduces the risk of phishing and that passwords may be hacked from the server. FIDO can be used across various industries, such as enterprise, banking, e-government, health care, and insurance.

4.3 EMV 3-D SECURE

EMV 3-D Secure (3DS) is a messaging protocol that enables frictionless cardholder authentication when carrying out card-not-present e-commerce transactions.[9] It allows cardholders to authenticate themselves with their card issuers if cardholder verification is needed. To reflect current and future market requirements, the payments industry recognized the need to create a new 3DS specification that would support app-based authentication and integration with digital wallets as well as traditional browser-based e-commerce transactions. This led to the development and publication of the EMV 3-D Secure Protocol and Core Functions Specification.[10]

A merchant needs to perform the following two steps when using EMV 3DS:[11]

1. **Authentication:** The consumer's ownership of a card is confirmed through the merchant's 3DS authentication solution. As proof of this confirmation, the issuer returns a unique identifier to the merchant.
2. **Authorization:** Authorization confirms the issuer's approval of the transaction. After successful authentication, the merchant sends to the issuer the authorization request, along with the authentication identifier returned in step 1. Once authorized, the merchant can proceed to a settlement request.

The EMV 3DS specification is based on the use of a primary account number. 3DS specification is optimized for authentication using card data. EMV 3DS can be used in the FPS world if the primary account number can be mapped to an International Bank Account Number by the payer's PSP. While 3DS specifications may be applied for FPS, this is not the objective of the specification, as FPS is out of the scope of EMVCo.

As per a statement from the European Banking Authority (EBA), EMV 3DS facilitates the support of SCA[12] and its requirements. The statement also mentions that the authority recommends the use of EMV 3DS for SCA. EMV 3DS is recognized as a good technology for SCA and for the revised European Payment Services Directive (PSD2).

Cardholder authentication holds various benefits. One benefit is that the exchange of 3DS data between the merchant and card issuer can increase authorization-approval rates.[13] Another pertains to reducing the risk of fraud for issuers, acquirers, and merchants.

EMV 3DS protocol's Version 2.1.0 was first released in October 2017 and includes enhancements to encourage secure, consistent cardholder e-commerce transactions across

BOX1 FIDO ALLIANCE PROCESSES

The FIDO registration process involves the following steps, based on the FIDO website:

- User is prompted to choose an available FIDO authenticator that matches the online service's acceptance policy.
- User unlocks the FIDO authenticator using a fingerprint reader, a button on a second–factor device, a securely entered PIN, or another method.
- User's device creates a new public/private-key pair unique for the local device, online service, and user's account.
- Public key is sent to the online service and associated with the user's account. The private key and any information about the local authentication method (such as biometric measurements or templates) never leave the local device.

Similarly, as per the FIDO Alliance website, the FIDO log-in process involves the following steps:

- Online service challenges the user to log in with a previously registered device that matches the service's acceptance policy.
- User unlocks the FIDO authenticator using the same method as at registration time.
- Device uses the user's account identifier provided by the service to select the correct key and sign the service's challenge.
- Client device sends the signed challenge back to the service, which verifies it with the stored public key and logs in the user.

- The FIDO2 stack consists of two specifications: CTAP (published by FIDO) and Web Authentication (or WebAuthn, published by W3C). Several companies participate in those efforts, including Google, Apple, Microsoft, Yubico, and PayPal.
- With WebAuthn, a site authenticates a user with public-key cryptography instead of a password. WebAuthn is for more than just payments, although there are many use cases of WebAuthn even in the payments context. WebAuthn involves two ceremonies: registration of authentication credentials with a relying party, and authentication (for example, during a subsequent payment transaction).
- WebAuthn can be initiated from different places depending on whom the user is interacting with (merchant website customer log-in, bank, or access control server—acting on behalf of the bank as the cardholder); the goal is to make authentication smooth and secure. WebAuthn is supported by all major browsers on desktop and mobile devices and can be used with authenticators (which manage the custody of the user keys and can assert them when required as part of the WebAuthn authentication process) already available to millions of users on current mobile devices and laptops. W3C, FIDO, and EMVCo are actively collaborating to support the use of WebAuthn in EMV 3D Secure flows and to fulfill dynamic linking requirements of the revised European Payment Services Directive.

Source: FIDO Alliance

all channels and connected devices while enhancing the cardholder's experience. The latest specification document, *Version 2.2.0 of EMV 3-D Secure Protocol and Core Functions Specification,* was released in December 2018.

4.4 INDUSTRY-BODY COLLABORATIONS

The FIDO Alliance, W3C, and EMVCo have established the Web Payment Security Interest Group,[14] whose overarching objective is to enhance the security, interoperability, and convenience of web payments. Individuals from all three industry bodies come together in this forum to discuss the various specifications that are in development and to make sure that the bodies work together from a security and user-experience perspective. Key areas of collaboration include the following:

- Providing a standard way for mobile-wallet providers and payment application developers to support on-device cardholder verification (CDCVM) using FIDO data
- Developing a process to evaluate the security of CDCVM, defining industry best practices to address functional and performance considerations, and creating a central mechanism to identify a CDCVM solution

- Ensuring that FIDO authentication information can be transmitted in an EMV 3DS authentication flow to give the issuing bank additional information that, in turn, facilitates a more informed and secure authorization decision

EMVCo relies on the FIDO Functional Evaluation for testing. On the security side, the company promotes the use of the Software-Based Mobile Payment (SBMP) Evaluation Process, which evaluates the security of implementations of such solutions. EMVCo is also working on building a database of both solution providers and associated solutions that will provide issuers with all information on security and functional results, in order to include this processing/verification during an authorization request.

4.5 GSMA'S MOBILE CONNECT

Mobile Connect is an identity service supported by mobile telephony operators. It enables authentication, authorization, and identity verification. Since its inception in 2014, Mobile Connect has been launched by more than 70 mobile operators around the world, reaching over four million end users. By matching end users to their mobile phone numbers, Mobile Connect empowers users to confirm their identity online and authorize transactions such as payments, sharing only essential personal data for transaction completion. The Mobile Connect product portfolio is delivered through the Mobile Connect API using the OpenID Connect standard. The service provider's application invokes the API to request the desired functionality from an operator, such as authenticating an end user or requesting an end user to authorize a transaction. The operator engages with the end user to fulfill the request and provide a response back to the application.[15] Mobile Connect's product portfolio, as per their website,[16] consists of the following:

- **Authentication:** Simple, secure log-in and two-factor authentication for the user when a PIN or fingerprint is requested for extra security
- **Authorization:** Allowing end users to authorize requests from service providers—such as payments and permissions—directly from their mobile phone
- **Identity:** Enabling end users to confirm or share their personal data with digital services quickly and securely
- **Attributes:** Utilizing device and network information for identity verification and fraud prevention

OAUTH 2.0 AND OPENID CONNECT[17]

OAuth 2.0 provides authorization workflows for diverse applications, such as web applications, desktop applications, mobile phones, and home-automation devices, while providing a simple platform for developers to harness. In an OAuth-based authorization, a consumer requests access to resources under the control of a resource owner. To access these resources, the consumer is provided a different set of credentials. This can be used for accessing the APIs from multiple devices, including mobile apps and desktops.

OpenID Connect is an interoperable authentication protocol based on the OAuth 2.0 family of specifications. It uses straightforward REST/JSON message flows with a design goal of simplifying things, and it works over the existing HTTP standard. OpenID Connect enables developers to create an authentication mechanism across websites and applications without creating a separate username/password file combination of their own. OpenID has the capability to manage multiple types of clients, including browser-based JavaScript and native mobile applications. Apps designed using OpenID can utilize sign-in workflows and receive confirmable assertions about the identity of the user (identity authentication + OAuth 2.0 = OpenID Connect). This can be used to access the APIs from multiple devices, including mobile apps, desktops, and so on in a manner similar to how Google/Facebook's single sign-on works across other websites.

5 COUNTRY EXAMPLES FOCUSING ON FAST PAYMENTS

Customer authentication in fast payments pertains to the method through which end users authenticate themselves while making a transaction. Select examples have been called out below.

Australia: There are no specific customer-authentication standards for making a fast payment, as these payments are initiated by logging into the internet and the mobile-banking application of a participating financial institution. This means that payments on the New Payments Platform are subject to the same fraud and security protections, including customer-authentication standards, that banks use for all of their internet and mobile-banking transactions—that is, two-factor authentication.

Bahrain: The Central Bank of Bahrain has mandated banks to have SCA and authorization. Customers need to log in to their mobile or internet banking app and enter the 10-digit International Bank Account Number to complete the Fawri+ transaction process. Additionally, transactions through Benefit Pay are processed through multifactor authentication.

Europe: In SEPA Instant Credit Transfer (SCT Inst), SCA guidelines are mandated as part of PSD2. The core principle is to reduce payment fraud with minimal impact on the customer experience—that is, without introducing too much friction into the payment process.[18]

- *The key enabler is two-factor authentication:* Consumers will need to provide two sets of information to prove they are who they say they are: something they own (for example, a mobile phone), something they know (for example, a PIN code), or something they are (for example, a fingerprint).
- *Ensure that your gateway, acquirer, and other third-party technology partners are 3DS ready:* Merchants should ensure that they understand what their partners' plans are for rolling out 3DS and how those plans will affect their own development road map. 3DS 2.1 facilitates a much more user-friendly payment process on mobile devices and complements digital wallets, such as Apple Pay or Google Pay. In addition, it allows the acquirer to send richer transaction data to the issuer, which can lead to higher authentication rates.
- *Some transactions will be exempt from authentication*—for example, low-value transactions, recurring transactions, when a user has "whitelisted" the merchant by indicating they shop there often, and when a user doesn't wish to be authenticated. Merchants will be able to claim some of these exemptions using the next iteration of 3DS.

Hong Kong SAR, China: The Hong Kong Monetary Authority has issued guidelines to banks for customer authentication. Since 2018, all banks and stored-value facilities have had to ensure two-factor authentication. Hong Kong's FPS does not impose any additional customer-authentication measure other than those mandated by the monetary authority.

India: For the Immediate Payment Service, two-factor authentication is carried out, and the factors are the following:

- Mobile number and mobile PIN for mobile transactions
- Card and ATM PIN for ATM channel
- User ID and internet banking password/transaction password for internet banking channel

In the case of the Unified Payments Interface (UPI):

- One-click, two-factor authentication is supported, using mobile (first factor) and UPI PIN (second factor). The mobile number is used for authenticating the first transaction, and the device fingerprint through device binding is used for subsequent transactions. While the system supports biometrics (Aadhaar) as a second factor, it has not been implemented yet.
- Risk is reduced further by dividing authentication requirements between the third-party application provider and issuer bank. The first factor is validated by the PSP, and the second factor is validated by the remitter bank.

Mexico: To send an Interbank Electronic Payment System (SPEI) transfer through electronic channels, end customers must use two-factor authentication, which resembles SCA in the European Union context. All SPEI participants are required to provide secure electronic channels and use two-factor authentication schemes, according to regulatory guidelines from the National Banking and Securities Commission (CNBV) and Banco de México.

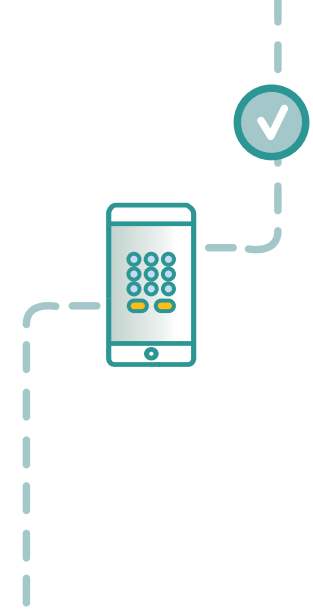
- CNBV has issued guidelines for credit-service institutions regarding customer authentication. These institutions need to adopt two-factor authentication for customer authorization for all services, including SPEI.
- SPEI rules published by Banco de México establish requirements for institutions other than credit-service institutions. Also, SPEI rules reinforce the guidelines for banks and credit-service institutions issued by CNBV.
- CNBV is considering the homogenization of customer-authentication standards, as they currently vary based on the nature of the participant.

United States: PSPs are mandated to establish multifactor authentication and implement a layered security program that includes fraud detection and monitoring, as well as other effective controls. At a minimum, the layered security program needs to include effective processes designed to detect anomalies and react to suspicious or outlier activity pertaining to the initial log-in and customer authentication and the initiation of electronic fund transfers to third parties. For business accounts, the layered security program needs to include advanced controls for system administrators.

It is necessary for PSPs to carry out periodic risk assessments and to adjust customer-authentication controls according to new threats. PSPs should also implement robust controls as the risk associated with a transaction increases.[19] Many countries, such as Bahrain, India, and Mexico, use multifactor authentication techniques for fast payment transactions. The specifications across schemes are based on regulations by central banks. Globally, there is a push toward using SCA to reduce fraud and make online payments more secure. However, it is critical for organizations to pay adequate attention to maintaining customer experience while strengthening authentication mechanisms.

6 CONCLUSION

The authentication measures used in a country depend on such factors as demography, economy, technology standards, and adoption of fast payments. Regulators have also started to define broad guidelines in regions such as Europe. Globally, multifactor authentication has proliferated, given the increasing use of digital payments and heightened need for enhanced security and limited fraud. In fast payments, irrespective of whether a transaction is initiated by the payer or the payee, authentication typically takes place at the payer's end. Third-party application providers can also help map out the key areas of authentication, identity, and trust and create a fast payment system that's stable, efficient, secure, and easy to use for all groups. Additionally, advanced features, such as CDCVM, FIDO Standards, GSMA's Mobile Connect, OAuth 2.0, and OpenID Connect, are emerging and could be useful for fast payments as operators work toward frictionless authentication with limited scope for error while also enhancing customer experience. Going ahead, a need for interoperability among strong authentication methods has also been recognized by industry bodies such as the FIDO Alliance, and further innovations in customer authentication can be expected.



7 ACKNOWLEDGMENTS

Organization	Contributor
Deloitte India	Deloitte India
EMVCo	Bastien Latge
	Simon Kleine
FIDO Alliance	Brett McDowell
	Christina Hulka
	David Turner
GSMA	Bart-Jan Pors
W3C	Ian Jacobs
World Bank	Harish Natarajan
	Nilima Ramteke
	Holti Banka
	Guillermo Galicia Rabadan

8 APPENDIX

8.1 STRONG CUSTOMER AUTHENTICATION

Strong customer authentication (SCA) is an authentication process that validates the identity of the user of a payment service or of the payment transaction. More specifically, SCA indicates whether the use of a payment instrument is authorized.[20] The European Central Bank has developed draft regulatory technical standards[21] specifying the requirements of SCA, the exemptions from the application of SCA, the requirements with which security measures have to comply to protect the confidentiality and integrity of the personalized security credentials of the users of a payment service, and the requirements for common and secure open standards of communication between account-servicing PSPs, payment-initiation service providers, account-information service providers, payers, payees, and other PSPs.[22]

SCA came into force on September 14, 2019. The enforcement deadline for SCA was December 31, 2020. The proposed guidelines are key to achieving the objectives of PSD2 and introduce new requirements for authenticating online payments. PSD2 requires PSPs to apply SCA when a payer initiates an electronic payment transaction. PSPs include banks and other PSPs. SCA applies to all customer-initiated online payments across Europe. The main objectives of SCA are to minimize fraud, create a more secure environment for online payments, protect the confidentiality of the user's financial data, including personal data, and add extra layers of protection by authenticating payments with additional identifying factors.

The SCA check requires authentication using two of the following three factors:

- Something the customer has—for example, a card, token, or phone
- Something the customer knows—for example, a PIN or password
- Something the customer is—for example, biometrics, such as fingerprint or face recognition

The following two additional elements of SCA are also sometimes leveraged for multifactor authentication:

- "Somewhere you are" (location), which is commonly detected by users' Internet Protocol addresses
- "Something you do" (behavior), least commonly used, where actions such as gestures or touches (for example, on a picture) are observed to prove identities

Some European Union member states, such as Belgium, the Netherlands, and Sweden, use SCA for remote electronic payment transactions, be it a card payment or a credit transfer from an online bank. In some other European Union countries, some PSPs apply SCA on a voluntary basis.[23]

8.2 EXEMPTIONS TO STRONG CUSTOMER AUTHENTICATION

Some types of transactions are exempt from SCA. Payment providers such as Stripe, Square, or PayPal can request an exemption on their customers' behalf during payment processing. The cardholder's bank decides whether to grant or reject the exemption. The most common types of exemptions are as follows:[24]

- **Low-value transactions:** Transactions under €30 are exempt. However, SCA is required if the card or payment method has seen more than five exempt transactions, or the total of exempted transactions exceeds €100 in a day.
- **Low-risk transactions:** Payment processors can do a real-time risk analysis to judge whether to apply for SCA. This can be done only if the fraud rates of the payment provider or bank remain low.
- **Subscriptions:** SCA is required for the first payment but may be exempted in subsequent payments if they're for the same amount to the same business. Variable amounts (or metered billing) require SCA every time.
- **Trusted beneficiaries:** Customers can "whitelist" businesses they trust. These businesses get placed on a list of "trusted beneficiaries" maintained by the customer's bank. SCA is required for the first payment to whitelisted business, but not for subsequent payments.
- **Mail-order and telephone-order (MOTO) transactions:** MOTO transactions are not considered "electronic" payments. They are not regulated under SCA.

The main challenge with implementing SCA requirements while maintaining a seamless and consistent user experience is largely determined by the ability of a firm (financial institutions and account-servicing PSPs) to take advantage of all available PSD2 SCA exemptions. In particular, to take advantage of the transaction-risk-analysis exemption, account-servicing PSPs will need to adopt advanced and effective capabilities to detect and report payment fraud that are able to determine, in real time, whether a particular transaction presents a low risk of fraud, and they will consistently need to maintain overall fraud below the predefined levels set by the regulatory technical standards.

In the case of real-time transaction risk analysis that categorizes a payment transaction as low risk, it is appropriate to introduce an exemption for the PSP that does not intend to apply SCA through the adoption of effective and risk-based requirements (that combine the scores of the risk analysis, confirming that no abnormal spending or behavioral pattern of the payer has been identified while accounting for other risk factors, such as the locations of the payer and the payee, with monetary thresholds based on fraud rates calculated for remote payments), which ensure the safety of the payment service user's funds and personal data.[25]

In March 2020, the EBA issued a statement regarding consumer and payment issues in the context of the COVID-19 pandemic. The statement acknowledges the need to adopt appropriate measures to protect consumers and the orderly functioning of payment services across the European Union. According to the statement, PSPs are advised to facilitate the use of payment methods that do not require physical contact. The EBA encourages these providers to apply the exemption for contactless payments from SCA to the fullest extent permitted by the regulatory technical standards on SCA (for example, use the maximum threshold of €50 per transaction). Additionally, intending to alleviate the pressure on the PSPs to implement migration plans to SCA-compliant solutions for e-commerce card-based payment transactions, the EBA removed the national competent authorities' obligation to report by March 31, 2020, the readiness of the payment service providers in this respect.

8.3 CHALLENGES ASSOCIATED WITH STRONG CUSTOMER AUTHENTICATION

The following challenges are associated with SCA:

- While innovating their online payment processes, merchants may need to incur expenses involved with implementing new infrastructure and protection required to comply with SCA.
- Card networks such as Mastercard and Visa utilize 3DS, and the newest version of 3DS is SCA compliant. Merchants may need to partner with and integrate card networks to meet SCA needs, resulting in additional costs.
- SCA may dampen customer experience due to added authentication steps and, thus, more friction.
- According to the EBA's "Opinion of the European Banking Authority on the Elements of SCA under PSD2," released in June 2019, a one-time password generated by or received on a device (hardware or software token generator, SMS OTP) is not PSD2 SCA compliant. According to the EBA, a one-time password contributes to providing evidence of possession but does not constitute a knowledge element for approaches currently observed in the market. Knowledge is an element that should exist prior to the initiation of the payment or the online access; thus, the one-time password does not qualify. As per the revised PSD2, any financial or commercial operation carried out by consumers in the European Union must be authorized using an SCA-compliant mechanism.[26] Select German banks have dropped SMS-based one-time passcodes in response to this development.
- The COVID-19 pandemic has potentially delayed implementation timelines, as merchants are pivoting to cater

to changing customer needs, and staff who would otherwise have been working on SCA-related changes are occupied with such areas as business continuity, customer support, and maintaining their own economic stability. Technical teams are also working remotely, which can serve as an added risk and lead to confusion and disruptions. Additionally, testing for SCA compliance requires coordination between multiple stakeholders (which is critical for a safe implementation).

8.4 RISK-BASED AUTHENTICATION

Risk-based authentication (RBA) is a means of authentication where the risk associated with a transaction is assessed, and the level of security for the transaction is determined based on that risk. RBA may be experienced when an individual accesses a bank account from another country and is asked more than the usual number of security questions. Some common criteria for assessing risks include geographic location, IP address, and the status of antivirus software. The principle of RBA has been around for a while. It started with simply the amount of the transaction (with low amounts implying low risk and larger amounts implying a higher associated risk). Today, in the e-commerce world, there is a lot more data, so RBA is much more sophisticated. With 3DS being implemented, consumers are asked to perform authentication so that they can confirm that they may legitimately perform the transaction.

From a fast payment perspective, RBA involves comparing various parameters relating to each transaction and buyer against a large data set of similar transactions, to determine whether further authentication is necessary. If the information provided indicates normal transactional patterns and low risk, the issuer can decide whether to request for additional authentication information. These parameters include the following:

- Transaction value
- Number of transactions within a specific time frame
- Buyer's transaction history
- Cardholder's browser fingerprint
- Whether the buyer is a new or returning customer
- Information about the buyer's location

RBA has the potential to ensure a streamlined customer journey with fewer friction points while minimizing fraud. RBA is also applicable in the e-commerce world, where there is a need to send enough information so that the issuer can decide whether to accept the transaction. RBA has various advantages associated with it when compared with the traditional static-password authentication approach. These benefits include the following:[27]

- Better fraud detection and lowered fraud losses for issuers
- Reduced liability for unauthorized card-not-present transactions
- Lowered cardholder abandonment rates at the point of interaction
- Faster checkout times
- Lowered cardholder authentication interaction at the point of interaction
- Limited call-center inquiries
- Potential elimination of the need for cardholder registration in select applications

RBA is a common way to evaluate risk for transactions. In the four-corner (merchant, acquirer, payment system, and issuer) type of transaction, each entity can perform its own RBA to evaluate the risk of a transaction. For example, when an individual uses a card at the point of sale, based on transaction data elements, such as the amount, whether the transaction is domestic or international, the location of the transaction, and whether the PIN was entered or not, the information is analyzed by the chip card and/or sent to the issuer. During the authorization analysis, the issuer processes all this information, assesses the risk, and accepts or declines the transaction accordingly. In RBA, solutions like that of the FIDO Alliance can play a role with respect to 3DS. When such solutions are used for the authentication step, that information is embedded in the 3DS response to help with risk evaluation. So, in addition to the other data, customers also have the assurance that the authentication was done with a certain level of confidence.

8.5 BIOMETRIC AUTHENTICATION

Biometric features are physical and biological elements that are unique to a person and can be easily compared to authorized features saved in a database.[28] Biometric authentication is a form of security that measures and matches biometric features of an individual to confirm that a person trying to transact via a payment method is authorized to do so. Some common types of biometric authentication include fingerprint scanners, facial recognition, voice identi-

fication, and eye scanners.

Biometric authentication is gaining traction in certain parts of the world due to the convenience, security, and accessibility associated with it. For example, Aadhaar, in India, is the largest biometrics-based identification system in the world;[29] 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-linked cards provide direct benefit transfers to retailers. Biometric authentication is carried out via a fingerprint scanner.

Using biometric authentication enables heightened security. The payment is associated with a single person, removing the possibility of contactless fraud or transferring or delegating usage. The use of biometrics is expected to go up significantly, and their availability is becoming universal today.

EMVCo has several specifications related to biometric authentication, such as the use of biometric authentication on acquired devices and the use of cardholder device authentication (CDCVM). FIDO standards have been developed to accommodate any biometrics. Within the FIDO Alliance, a group is focused on a biometric component certification program. This program tests biometric components that might be implemented in a laptop or phone for false positive, false negative, and presentation attacks. In addition, ISO/IEC JTC SC 37 has incorporated FIDO biometric-testing requirements into their work.

NOTES

1. According to the Committee on Payments and Market Infrastructures, a fast payment can be defined as a payment in which the "transmission of the payment message and the availability of 'final' funds to the payee occur in real time or near-real time on as near to a 24-hour and seven-day (24/7) basis as possible."
2. https://csrc.nist.gov/glossary/term/authentication
3. https://simplicable.com/new/authentication
4. More details on SCA can be found in this note's appendix.
5. More details on RBA can be found in this note's appendix.
6. https://www.cgap.org/sites/default/files/publications/2021_01_Technical_Guide_Building_Faster_Better.pdf
7. More details on biometric authentication can be found in this note's appendix.
8. https://www.emvco.com/wp-content/uploads/2017/03/EMVCo-Website-Content-2.1-Contact-Portal-plus-Biometric-FAQ_v2.pdf
9. https://www.emvco.com/media-centre/emv-3ds-press-kit/
10. https://www.emvco.com/emv-technologies/3d-secure/
11. https://www.jpmorgan.com/content/dam/jpm/merchant-services/documents/JPFEB20_006%20SCA%20Merchant%20Guide%20A4.pdf
12. https://eba.europa.eu/eba-publishes-opinion-on-the-deadline-and-process-for-completing-the-migration-to-strong-customer-authentication-sca-for-e-commerce-card-based-payment
13. https://www.emvco.com/wp-content/uploads/2018/08/EMV-3DS-press-kit-QA_FINAL.pdf
14. https://www.emvco.com/wp-content/uploads/documents/EMVCo-FIDO-Alliance-W3C-Interest-Group-release_FINAL-website-version.pdf
15. https://www.gsma.com/identity/mobile-connect
16. https://mobileconnect.io/
17. https://abs.org.sg/docs/library/abs-api-playbook.pdf
18. https://www.jpmorgan.com/europe/merchant-services/insights/PSD2
19. https://www.theclearinghouse.org/payment-systems/rtp/-/media/73118cf25e8043239672eb-270cf47b9b.ashx
20. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_5555
21. For additional details on regulatory technical standards, please refer to European Banking Authority, Final Report: Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication under Article 98 of Directive 2015/2366 (PSD2), EBA/RTS/2017/02 (EBA, 2017): https://eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf?retry=1
22. https://eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf
23. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_5555
24. https://stripe.com/en-in/guides/strong-customer-authentication
25. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.069.01.0023.01.ENG&toc=OJ:L:2018:069:TOC
26. https://www.zdnet.com/article/german-banks-are-moving-away-from-sms-one-time-passcodes/
27. https://globalrisk.mastercard.com/wp-content/uploads/2015/12/Advantages-of-Risk-Based-Authentication.pdf
28. https://www.iovation.com/topics/biometric-authentication
29. https://uidai.gov.in/my-aadhaar/about-your-aadhaar.html

WORLD BANK GROUP